DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

While NIST and the NCCoE address goals of improving management of cybersecurity and privacy risk through outreach and application of standards and best practices, it is the stakeholder’s responsibility to fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise, and the impact should the threat be realized before adopting cybersecurity measures such as this recommendation.


FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: nccoe-zta-project@list.nist.gov.

Public comment period: August 9, 2022 through September 9, 2022

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov
The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses’ most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology collaborators—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://www.nist.gov.

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

**ABSTRACT**

A zero trust architecture (ZTA) focuses on protecting data and resources. It enables secure authorized access to enterprise resources that are distributed across on-premises and multiple cloud environments, while enabling a hybrid workforce and partners to access resources from anywhere, at any time, from any device in support of the organization’s mission. Each access request is evaluated by verifying the context available at access time, including the requester’s identity and role, the requesting device’s health and credentials, and the sensitivity of the resource. If the enterprise’s defined access policy is met, a secure session is created to protect all information transferred to and from the resource. A real-time and continuous policy-driven, risk-based assessment is performed to establish and maintain the
access. In this project, the NCCoE and its collaborators use commercially available technology to build interoperable, open, standards-based ZTA implementations that align to the concepts and principles in NIST Special Publication (SP) 800-207, Zero Trust Architecture. This NIST Cybersecurity Practice Guide explains how commercially available technology can be integrated and used to build various ZTAs.

**KEYWORDS**

enhanced identity governance (EIG); identity, credential, and access management (ICAM); zero trust; zero trust architecture (ZTA).

**ACKNOWLEDGMENTS**

We are grateful to the following individuals for their generous contributions of expertise and time.

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Michael Friedrich</td>
<td>Appgate</td>
</tr>
<tr>
<td>Adam Rose</td>
<td>Appgate</td>
</tr>
<tr>
<td>Jonathan Roy</td>
<td>Appgate</td>
</tr>
<tr>
<td>Quint Van Deman</td>
<td>Amazon Web Services</td>
</tr>
<tr>
<td>Eric Michael</td>
<td>Broadcom Software</td>
</tr>
<tr>
<td>Ken Andrews</td>
<td>Cisco</td>
</tr>
<tr>
<td>Matthew Hyatt</td>
<td>Cisco</td>
</tr>
<tr>
<td>Leo Lebel</td>
<td>Cisco</td>
</tr>
<tr>
<td>Tom Oast</td>
<td>Cisco</td>
</tr>
<tr>
<td>Peter Romness</td>
<td>Cisco</td>
</tr>
<tr>
<td>Steve Vetter</td>
<td>Cisco</td>
</tr>
<tr>
<td>Daniel Cayer</td>
<td>F5</td>
</tr>
<tr>
<td>Name</td>
<td>Organization</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>David Clark</td>
<td>F5</td>
</tr>
<tr>
<td>Jay Kelley</td>
<td>F5</td>
</tr>
<tr>
<td>Jamie Lozan</td>
<td>F5</td>
</tr>
<tr>
<td>Jason Wilburn</td>
<td>F5</td>
</tr>
<tr>
<td>Tim Jones</td>
<td>Forescout</td>
</tr>
<tr>
<td>Yejin Jang</td>
<td>Forescout</td>
</tr>
<tr>
<td>Andrew Campagna</td>
<td>IBM</td>
</tr>
<tr>
<td>Adam Frank</td>
<td>IBM</td>
</tr>
<tr>
<td>Nalini Kannan</td>
<td>IBM</td>
</tr>
<tr>
<td>Priti Patil</td>
<td>IBM</td>
</tr>
<tr>
<td>Nikhil Shah</td>
<td>IBM</td>
</tr>
<tr>
<td>Mike Spisak</td>
<td>IBM</td>
</tr>
<tr>
<td>Vahid Esfahani</td>
<td>IT Coalition</td>
</tr>
<tr>
<td>Ebadullah Siddiqui</td>
<td>IT Coalition</td>
</tr>
<tr>
<td>Musumani Woods</td>
<td>IT Coalition</td>
</tr>
<tr>
<td>Tyler Croak</td>
<td>Lookout</td>
</tr>
<tr>
<td>Madhu Dodda</td>
<td>Lookout</td>
</tr>
<tr>
<td>Jeff Gilhool</td>
<td>Lookout</td>
</tr>
<tr>
<td>Name</td>
<td>Organization</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Ken Durbin</td>
<td>Mandiant</td>
</tr>
<tr>
<td>Earl Matthews</td>
<td>Mandiant</td>
</tr>
<tr>
<td>Joey Cruz</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Janet Jones</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Carmichael Patton</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Hemma Prafullchandra</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Brandon Stephenson</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Sarah Young</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Spike Dog</td>
<td>MITRE</td>
</tr>
<tr>
<td>Ayayidjin Gabiam</td>
<td>MITRE</td>
</tr>
<tr>
<td>Karri Meldorf</td>
<td>MITRE</td>
</tr>
<tr>
<td>Kenneth Sandlin</td>
<td>MITRE</td>
</tr>
<tr>
<td>Jessica Walton</td>
<td>MITRE</td>
</tr>
<tr>
<td>Mike Bartock</td>
<td>NIST</td>
</tr>
<tr>
<td>Oliver Borchert</td>
<td>NIST</td>
</tr>
<tr>
<td>Gini Khalsa</td>
<td>NIST</td>
</tr>
<tr>
<td>Douglas Montgomery</td>
<td>NIST</td>
</tr>
<tr>
<td>Scott Rose</td>
<td>NIST</td>
</tr>
<tr>
<td>Name</td>
<td>Organization</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Kevin Stine</td>
<td>NIST</td>
</tr>
<tr>
<td>Sean Frazier</td>
<td>Okta</td>
</tr>
<tr>
<td>Kelsey Nelson</td>
<td>Okta</td>
</tr>
<tr>
<td>Shankar Chandrasekhar</td>
<td>Palo Alto Networks</td>
</tr>
<tr>
<td>Sean Morgan</td>
<td>Palo Alto Networks</td>
</tr>
<tr>
<td>Seetal Patel</td>
<td>Palo Alto Networks</td>
</tr>
<tr>
<td>Zack Austin</td>
<td>PC Matic</td>
</tr>
<tr>
<td>Andy Tuch</td>
<td>PC Matic</td>
</tr>
<tr>
<td>Bill Baz</td>
<td>Radiant Logic</td>
</tr>
<tr>
<td>Rusty Deaton</td>
<td>Radiant Logic</td>
</tr>
<tr>
<td>Deborah McGinn</td>
<td>Radiant Logic</td>
</tr>
<tr>
<td>Lauren Selby</td>
<td>Radiant Logic</td>
</tr>
<tr>
<td>Peter Amaral</td>
<td>SailPoint</td>
</tr>
<tr>
<td>Jim Russell</td>
<td>SailPoint</td>
</tr>
<tr>
<td>Esteban Soto</td>
<td>SailPoint</td>
</tr>
<tr>
<td>Jeremiah Stallcup</td>
<td>Tenable</td>
</tr>
<tr>
<td>Andrew Babakian</td>
<td>VMware</td>
</tr>
<tr>
<td>Dennis Moreau</td>
<td>VMware</td>
</tr>
</tbody>
</table>
### Name | Organization
---|---
Jeffrey Adorno | Zscaler
Jeremy James | Zscaler
Lisa Lorenzin | Zscaler
Matt Moulton | Zscaler
Patrick Perry | Zscaler

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

<table>
<thead>
<tr>
<th>Technology Collaborators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appgate</td>
</tr>
<tr>
<td>AWS</td>
</tr>
<tr>
<td>Broadcom Software</td>
</tr>
<tr>
<td>Cisco</td>
</tr>
<tr>
<td>DigiCert</td>
</tr>
<tr>
<td>F5</td>
</tr>
<tr>
<td>Forescout</td>
</tr>
<tr>
<td>Google Cloud</td>
</tr>
</tbody>
</table>

**DOCUMENT CONVENTIONS**

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action permissible within the limits of the publication. The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.
CALL FOR PATENT CLAIMS

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
2. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: nccoe-zta-project@list.nist.gov
# Contents

1 Introduction ........................................................................................ 1
   1.1 How to Use this Guide ................................................................................................... 1
   1.2 Build Overview .............................................................................................................. 3
      1.2.1 EIG Crawl Phase Build Features .................................................................................... 3
      1.2.2 Physical Architecture Overview .................................................................................... 4
   1.3 Typographic Conventions .............................................................................................. 6

2 Enterprise 1 Build 1 (EIG E1B1) Product Guides ................................... 6
   2.1 Okta Identity Cloud ....................................................................................................... 7
      2.1.1 Configuration and Integration ...................................................................................... 7
      2.1.2 Okta Verify App ........................................................................................................... 10
      2.1.3 Okta Access Gateway .................................................................................................. 10
   2.2 Radiant Logic RadiantOne ........................................................................................... 11
      2.2.1 Installation .................................................................................................................. 11
      2.2.2 Configuration .............................................................................................................. 11
      2.2.3 Integration .................................................................................................................. 15
   2.3 SailPoint IdentityIQ ...................................................................................................... 16
      2.3.1 Installation and Configuration .................................................................................... 16
      2.3.2 Integration with Radiant Logic .................................................................................... 26
      2.3.3 Integration with AD ..................................................................................................... 27
      2.3.4 Integration with Okta .................................................................................................. 28
   2.4 Ivanti Neurons for UEM ............................................................................................... 29
      2.4.1 Installation and Configuration .................................................................................... 29
      2.4.2 Integration with Ivanti Connector .............................................................................. 34
      2.4.3 Integration with Okta .................................................................................................. 35
   2.5 Ivanti Sentry .................................................................................................................. 36
      2.5.1 Installation and Configuration .................................................................................... 36
      2.5.2 Ivanti Tunnel Configuration and Deployment ............................................................ 36
   2.6 Ivanti Access ZSO ......................................................................................................... 37
2.6.1 Integration with Ivanti Neurons for UEM ................................................................. 37
2.6.2 Integration with Okta ................................................................................................. 38
2.7 Zimperium Mobile Threat Defense (MTD) ................................................................. 38
2.7.1 Installation, Configuration, and Integration .............................................................. 38
2.8 IBM Cloud Pak for Security ......................................................................................... 42
2.9 IBM Security QRadar XDR ......................................................................................... 43
2.10 Tenable.io .................................................................................................................. 43
  2.10.1 Installation and Configuration ................................................................................. 43
  2.10.2 Integration with QRadar ........................................................................................ 44
2.11 Tenable.ad .................................................................................................................. 45
2.12 Mandiant Security Validation (MSV) ........................................................................ 45
  2.12.1 MSV Director Installation/Configuration ............................................................... 45
  2.12.2 MSV Network Actor Installation/Configuration .................................................... 46
  2.12.3 MSV Endpoint Actor Installation/Configuration .................................................... 46
  2.12.4 MSV Evaluation Configuration .............................................................................. 47
  2.12.5 MSV Evaluation Execution .................................................................................... 48
2.13 DigiCert CertCentral ................................................................................................. 49
2.14 AWS IaaS ................................................................................................................. 49

3  Enterprise 3 Build 1 (EIG E3B1) Product Guides .................................................... 49
  3.1 Microsoft Azure Active Directory (AD) ................................................................. 49
  3.2 Microsoft Endpoint Manager .................................................................................... 50
    3.2.1 Configuration and Integration ............................................................................. 50
  3.3 Microsoft Defender for Endpoint ............................................................................. 55
    3.3.1 Configuration and Integration ............................................................................. 55
    3.3.2 Microsoft Defender Antivirus .......................................................................... 59
  3.4 Microsoft Sentinel ..................................................................................................... 60
  3.5 F5 BIG-IP ................................................................................................................ 60
    3.5.1 Installation, Configuration, and Integration ......................................................... 61
  3.6 Lookout Mobile Endpoint Security (MES) ............................................................... 62
    3.6.1 Configuration and Integration ............................................................................. 62
3.6.2 Create MTD device compliance policy with Intune .................................................... 64
3.7 PC Matic Pro ................................................................................................................ 65
3.8 Tenable.io .................................................................................................................... 66
  3.8.1 Integration with Microsoft Sentinel ............................................................................ 66
3.9 Tenable.ad ................................................................................................................... 66
3.10 Mandiant Security Validation (MSV) ............................................................................ 67
3.11 Forescout eyeSight ..................................................................................................... 67
  3.11.1 Integration with AD ............................................................................................... 67
  3.11.2 Integration with Cisco Switch ..................................................................................... 67
  3.11.3 Integration with Cisco Wireless Controller ................................................................. 67
  3.11.4 Integration with Microsoft Sentinel ............................................................................ 67
  3.11.5 Integration with Palo Alto Networks NGFW ............................................................... 68
  3.11.6 Integration with Tenable.io ........................................................................................ 68
3.12 Palo Alto Next Generation Firewall ............................................................................. 68
3.13 DigiCert CertCentral .................................................................................................... 68

Appendix A  List of Acronyms .......................................................................................... 69

List of Figures

Figure 1-1 Laboratory Infrastructure for the EIG Builds ....................................................... 5
1 Introduction

The following volumes of this guide show information technology (IT) professionals and security engineers how we implemented two example zero trust architecture (ZTA) solutions. We cover all of the products employed in this reference design. We do not recreate the product manufacturers’ documentation, which is presumed to be widely available. Rather, these volumes show how we incorporated the products together in our environment to create two example solutions.

Note: These are not comprehensive tutorials. There are many possible service and security configurations for these products that are out of scope for this reference design.

1.1 How to Use this Guide

This NIST Cybersecurity Practice Guide will help users develop a plan for migrating to ZTA. It demonstrates a standards-based reference design for implementing a ZTA and provides users with the information they need to replicate two different implementations of this reference design. Each of these implementations, which are known as builds, are standards-based and align to the concepts and principles in NIST Special Publication (SP) 800-27, Zero Trust Architecture. The reference design described in this practice guide is modular and can be deployed in whole or in part, enabling organizations to incorporate ZTA into their legacy environments gradually, in a process of continuous improvement that brings them closer and closer to achieving the ZTA goals that they have prioritized based on risk, cost, and resources.

NIST is adopting an agile process to publish this content. Each volume is being made available as soon as possible rather than delaying release until all volumes are completed. Work continues on implementing the example solutions and developing other parts of the content. As a preliminary draft, we will publish at least one additional draft for public comment before it is finalized.

When complete, this guide will contain four volumes:

- NIST SP 1800-35A: Executive Summary – why we wrote this guide, the challenge we address, why it could be important to your organization, and our approach to solving this challenge
- NIST SP 1800-35C: How-To Guides – instructions for building the example implementations, including all the security-relevant details that would allow you to replicate all or parts of this project (you are here)
- NIST SP 1800-35D: Functional Demonstrations – use cases that have been defined to showcase ZTA security capabilities and the results of demonstrating them with each of the example implementations
Depending on your role in your organization, you might use this guide in different ways:

- **Business decision makers**, including chief security and technology officers, will be interested in the Executive Summary, NIST SP 1800-35A, which describes the following topics:
  - challenges that enterprises face in migrating to the use of ZTA
  - example solution built at the National Cybersecurity Center of Excellence (NCCoE)
  - benefits of adopting the example solution

- **Technology or security program managers** who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, NIST SP 1800-35B, which describes what we did and why.

- You might share the Executive Summary, NIST SP 1800-35A, with your leadership team members to help them understand the importance of migrating toward standards-based ZTA implementations that align to the concepts and principles in NIST SP 800-207, Zero Trust Architecture.

- **IT professionals** who want to implement similar solutions will find the whole practice guide useful. You can use the how-to portion of the guide, NIST SP 1800-35C, to replicate all or parts of the builds created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create the product manufacturers’ documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution. Also, you can use Functional Demonstrations, NIST SP 1800-35D, which provides the use cases that have been defined to showcase ZTA security capabilities and the results of demonstrating them with each of the example implementations.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a ZTA. Your organization’s security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices.

A NIST Cybersecurity Practice Guide does not describe “the” solution, but example solutions. This is a preliminary draft guide. As the project progresses, the preliminary draft will be updated, and additional volumes will also be released for comment. We seek feedback on the publication’s contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to nccoe-zta-project@list.nist.gov.
1.2 Build Overview

This NIST Cybersecurity Practice Guide addresses the challenge of using standards-based protocols and available technologies to build a ZTA. In our lab at the NCCoE, we plan to implement and demonstrate a variety of builds that serve as example ZTA solutions, each of which is designed to dynamically and securely manage access to resources across a set of use cases that a medium or large enterprise might typically deploy. Our plan is to implement these builds in a series of phases, starting with a baseline enterprise architecture that represents the typical legacy components that an enterprise might start with when deciding to begin adding zero trust capabilities.

We began with builds for enhanced identity governance (EIG) that were restricted to a limited set of capabilities. We call these EIG crawl phase builds. The central capabilities of these builds are identity, credential, and access management (ICAM) and endpoint protection. In particular, these EIG crawl phase builds do not include the separate, centralized policy engine (PE) or policy administration (PA) components. Instead, these initial EIG crawl phase builds rely upon the PE and PA capabilities provided by their ICAM components. After completing the EIG crawl phase builds, our plan is to gradually enhance these implementations by adding specialized PE and PA components, as well as capabilities such as software defined perimeter and micro-segmentation.

This practice guide provides instructions for reproducing the two EIG crawl phase builds that we have implemented so far: EIG Enterprise 1 Build 1 (E1B1) and EIG Enterprise 3 Build 1 (E3B1). The NCCoE worked with members of the ZTA community of interest to develop a diverse but non-comprehensive set of use cases and scenarios to demonstrate the capabilities of the builds. The use cases are summarized in NIST SP 1800-35D, Functional Demonstrations.

1.2.1 EIG Crawl Phase Build Features

A general ZTA reference design is depicted in Figure 4-1 of Volume B. It consists of ZTA core components: a policy decision point (PDP), which includes both a PE and a PA, and one or more policy enforcement points (PEPs); and ZTA functional components for ICAM, security analytics, data security, and endpoint security. The EIG crawl phase builds that have been created so far differ from this reference design insofar as they do not include separate, dedicated PDP components. Their ICAM component serves as their PDP, and they include very limited data security and security analytics functionality. These limitations were intentionally placed on the initial builds in an attempt to demonstrate the ZTA functionality that an enterprise that currently has ICAM and endpoint protection solutions deployed will be able to support without having to add additional ZTA-specific capabilities.

Each EIG crawl phase build is instantiated in a unique way, depending on the equipment used and the capabilities supported. Briefly, the two builds are as follows:

- EIG E1B1 uses products from IBM, Ivanti, Mandiant, Okta, Radiant Logic, SailPoint, Tenable, and Zimperium. Certificates from DigiCert are also used.
1.2.2 Physical Architecture Overview

The laboratory environment in which the builds have been implemented is depicted and described in detail in Section 4.3 of Volume B. The laboratory architecture drawing from that volume is reproduced here in Figure 1-1. As shown, this laboratory environment includes two separate enterprise environments that each hosts its own distinct implementation of a ZTA architecture. The enterprises may interoperate as needed by a given use case, and the baseline enterprise environments have the flexibility to support enhancements. The laboratory environment also includes a management virtual local area network (VLAN) on which the following components are installed: Ansible, Terraform, MSV Director, and MSV Protected Theater. These management components support infrastructure as code (IaC) automation and orchestration.
Figure 1-1 Laboratory Infrastructure for the EIG Builds
The following two EIG crawl phase builds are supported within the physical architecture depicted in Figure 1-1 and documented in the remainder of this guide:


- EIG E3B1 components consist of DigiCert CertCentral, F5 BIG-IP, Forescout eyeSight, Lookout MES, Mandiant MSV, Microsoft Azure AD, Microsoft Defender for Endpoint, Microsoft Endpoint Manager, Microsoft Sentinel, Palo Alto Networks NGFW, PC Matic Pro, Tenable.ad, and Tenable.io.

For a detailed description of the architecture of each build, see Volume B, Appendices D and F. The remainder of this guide describes how to implement the EIG crawl phase builds E1B1 and E3B1.

1.3 Typographic Conventions

The following table presents typographic conventions used in this volume.

<table>
<thead>
<tr>
<th>Typeface/Symbol</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Italics</em></td>
<td>file names and path names; references to documents that are not hyperlinks; new terms; and placeholders</td>
<td>For language use and style guidance, see the NCCoE Style Guide.</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>names of menus, options, command buttons, and fields</td>
<td>Choose File &gt; Edit.</td>
</tr>
<tr>
<td>Monospace</td>
<td>command-line input, onscreen computer output, sample code examples, and status codes</td>
<td>mkdir</td>
</tr>
<tr>
<td>Monospace Bold</td>
<td>command-line user input contrasted with computer output</td>
<td>service sshd start</td>
</tr>
<tr>
<td>blue text</td>
<td>link to other parts of the document, a web URL, or an email address</td>
<td>All publications from NIST’s NCCoE are available at <a href="https://www.nccoe.nist.gov">https://www.nccoe.nist.gov</a>.</td>
</tr>
</tbody>
</table>

2 Enterprise 1 Build 1 (EIG E1B1) Product Guides

This section of the practice guide contains detailed instructions for installing, configuring, and integrating all of the products used to implement EIG E1B1. For additional details on EIG E1B1’s logical and physical architectures, please refer to Volume B.
2.1 Okta Identity Cloud

The Okta Identity Cloud is a software as a service (SaaS) solution that provides ICAM capabilities to an enterprise. The following sections describe the setup of the Okta Identity Cloud, the Okta Access Gateway, and the Okta Verify application. Okta integrates with Radiant Logic for identity information, SailPoint to receive governance information, and Ivanti to delegate authentication for users accessing resources using mobile devices.

2.1.1 Configuration and Integration

The purpose is to set up integrations with other ICAM tools so Okta can manage authentication and authorization of users accessing resources.

1. Sign up for an account with Okta (okta.com).
2. Set up an admin account, then set up Okta Verify for the admin account. (Repeat this step if needed so each administrator has a unique account.)
3. Log in to the Okta instance that was just created and into the admin account.
4. Set up directory integration with Radiant Logic. User identity information is pulled from Radiant Logic into Okta for authentication and authorization. Note: This step should be completed after Radiant Logic is configured.
   a. Review the background information and check the prerequisites.
   b. Install the Okta LDAP Agent on the Radiant Logic server and configure LDAP integration settings.
   c. Configure the LDAP Interface. Note that the service account and password that was created in Radiant Logic is used in this step.
   d. Once LDAP integration is successful, users from Radiant Logic can be imported into Okta.
5. Create Groups for Okta to apply a specific set of users to specific services or applications. From the main menu, navigate to Directory > Groups and click on the Add Group button. Create the name and description of the group and click Save.
6. Create API tokens to be used by SailPoint and Radiant Logic for communication.
   a. From the main menu, navigate to Security > API and click on the Create Token button. Type in the name for SailPoint and click Create Token.
b. Copy the token. It will be used in the SailPoint configuration. Once we configure SailPoint, the integration is complete. Please refer to the “Integration with Okta” subsection within SailPoint for integration configuration.

c. Repeat these steps to create a token for Radiant Logic.

7. Create a delegated authentication for Okta to be able to import users from Radiant Logic via LDAP. Note that a service account, created in the Radiant Logic Integration section of this document, needs to be created and used in this configuration.

8. Okta Access Gateway needs to be installed in order to configure on-premises applications. See Section 2.1.3 for installation instructions, which include information on configuring on-premises applications.

9. Create application integration for Ivanti Neurons for UEM.

   a. From the Okta admin page, select Applications from the Application drop-down menu.

   b. Click on the Browse App Catalog button. Type “MobileIron” and select the “MobileIron Cloud” app.

   c. Follow the step-by-step instructions to configure the app.

10. Create Identity Provider integration for Ivanti Access ZSO. This involves creating a custom application using SAML and then creating a SAML Identity Provider.

11. Configure Device Trust on iOS and Android devices to create device integrations.

12. Create authentication policies. By default, a “Catch All” policy is created when an application is created. We are creating an authentication policy that will allow Okta to trust Ivanti Access ZSO to be the delegated Identity Provider (IdP). To do this, when Okta checks that Okta Verify is a managed application on a device, it will delegate authentication to Ivanti Access ZSO. The screenshots below show the current policy created for the GitLab1 application. Note that iOS and Android devices are managed in the first policy.
For MobileIron

**IF**
- User type: Any
- Group: Any
- User is: Any
- Zone: Any
- Risk: Any
- Device: Registered, Managed
- Platform: iOS, Android

**THEN**
- Access: Enabled after successful authentication
- User must authenticate with:
  - Any 2 factor types
- Access with Okta FastPass is granted:
  - If the user approves a prompt in Okta Verify or provides biometrics (meets NIST AAL2 requirements)

**Available Authenticators:**
- Knowledge / Biometric factor types
  - Okta Verify* or Password / IdP or Security Question**

* authenticator that may satisfy multiple factor requirements
** Security Questions can’t be used with passwordless authentication. [Learn more.](#)
2.1.2 Okta Verify App

The Okta Verify app is installed when a new user is onboarded. The user can log in to the Okta Identity Cloud for the first time. For this setup, the user will be asked to change their password and perform setup. After the password update, the user can set up Okta Verify. Follow the instructions for Android or iOS devices to install Okta Verify and complete the process.

2.1.3 Okta Access Gateway

The Okta Access Gateway is part of the Okta Identity Cloud. It can be leveraged to integrate legacy, on-prem applications into the Okta Identity Cloud. More information on installing and configuring the Okta Access Gateway (AG) is available online. Tasks to perform include:

1. First, download and deploy the latest OVA image.
2. Once installed, start the server, log in to the Okta AG, and configure the Okta AG.
3. Next, log into the Okta admin console via a web browser (i.e.: https://zta-eig1-ad-min.okta.com/). Configure Okta as the Identity Provider for the AG.

4. Log into Okta AG via a web browser and configure enterprise applications in Okta AG.

### 2.2 Radiant Logic RadiantOne

Radiant Logic RadiantOne is an ICAM solution that unifies identity data, making access reusable and scalable for the enterprise.

#### 2.2.1 Installation

RadiantOne is to be installed on a Microsoft Windows 2019 server. See the RadiantOne v7.4.1 documentation from the Radiant Logic website for system specifications. Prerequisites are in Chapter 1 of the RadiantOne Installation Guide. Note: You need to create an account within the Radiant Logic website in order to access the installation and configuration documentation.

Once you download and launch the executable for a Windows server installation, follow the step-by-step instructions provided on the screen. We used default settings unless specified below. Instructions can also be found in Chapter 2 of the RadiantOne Installation Guide.

- Choose RadiantOne Federated Identity Suite New Cluster/Standalone for the Install Set.
- Provide a name and password for the Cluster settings.
- For the Server Configuration step, use the following ports: LDAP = 389, LDAPS = 636, and Scheduler Port = 1099.

#### 2.2.2 Configuration

##### 2.2.2.1 Sync with an LDAP server

1. Once installation is complete, log in to RadiantOne from a web browser on the Radiant Logic server, https://localhost:7171. Note: ensure the proper SSL certificate is on the server for HTTPS.

2. Initial configuration is to sync up with an LDAP server. Go to Settings > Server Backend > LDAP Data Sources. The screenshot below shows the information created for Enterprise 1 AD. See the RadiantOne Namespace Configuration Guide Chapter 3 for details.
3. Once the connection is tested and successful, the integration is completed.

4. Next, create a Directory Namespace by going to Directory Namespace and selecting **Create New Naming Context**. Click **Next** and click **OK**.

5. Find **DC=NCCOE,DC=ORG** under Root Naming Contexts on the left side of the screen. Click the **New Level** button. Enter **ent1** as the name for the **OU** and click **OK**.

6. Click on **ou=ent1** on the left side and click the **New Level** button on the right to create a sub-ou called **groups**.
7. Click on ou=ent1 on the left side as shown below and click the New Level button on the right to create a sub-ou called users.

8. Once configured and saved, click on ou=users and click on Backend Mapping on the right. Select LDAP Backend. Click Next and Browse for the proper Remote Base DN. Then click OK. The screenshot is the completed configuration for the sub-ou users Proxy Backend.

9. Go to Objects and create a primary object and Join Profile by clicking Add on each. Click Save. Now we have data sources from LDAP and our database.
2.2.2.2 Create a namespace to bring in users

1. In Directory Namespace, click the + sign. Create a naming context: `ou=hr,ou=lab,ou=nccoe,ou=org` and select Virtual Tree for the naming context type, then click Next.

2. Configure the Virtual Tree by choosing Create a new view (.dvx), setting the Directory View to `dv=ou_hr_ou_lab_ou_nccoe_ou_org` and clicking OK.

3. Next, create a sub-Namespace by clicking the + New level button and entering the information depicted below.

4. Click on the sub-Namespace that was just created and click on Backend Mapping. Specify `ou=east,ou=hr,ou=lab,ou=nccoe,ou=org` as the naming context and select HDAP Store as the type, then click Next. Note: Instead of having an actual HR database, we are importing sample users from a text file.
5. Click on **ou=east** to edit properties. Scroll down to the bottom of the screen and click on the **Initialize** button. Then select a file with database users to import for initializing the HDAP store.

Note: We are emulating an HR database with this file.

6. Go to the **Directory Browser** tab and refresh the data by clicking the **Refresh Tree** button.

7. Go to the OU that you just configured and expand it. The new users should now be available.

8. Go to **Directory Namespace** and click the + button to add new naming context (in our build, we used **ou=testing**). This is used to map to the LDAP backend the database information that was imported.

9. Click on the OU that was created. Click **OK** and **Save**.

10. Go to **Directory Browser** and hit the **Refresh** button.

11. Go to **Settings > Configuration > ORX Schema**, and find **OU=Testing** and check it. Click on **Generate LDAP Schema** at the bottom of the screen and click **OK**.

### 2.2.3 Integration

Other applications, including SailPoint and Okta, will need the following information in order to integrate with Radiant Logic and pull information from it:

- Hostname: radiant1.lab.nccoe.org (hostname of the Radiant Logic server)
- Port: 389 (LDAP) and 636 (LDAPS)
Also, a service account and password need to be created on Radiant Logic for each application to be integrated. The service account is in the form of: `uid=sailpointadmin,ou=globalusers,cn=config`. Follow these steps to create each service account for SailPoint, Okta, and any other desired applications:

1. Go to **Directory Browser**.

2. On the left, go to `cn=config`, then `ou=globalusers` underneath it. Right-click on `ou=globalusers`, click **Add**, then click **New InetOrgPerson**.

3. Fill in the necessary entries. Click **Confirm** to save the configuration.

### 2.3 SailPoint IdentityIQ

SailPoint IdentityIQ is the identity and access management software platform for governing the lifecycle of the enterprise user’s identity.

#### 2.3.1 Installation and Configuration

The steps below explain the installation of the IdentityIQ server, initial configuration to import users from the Radiant Logic identity store, and configuration to manage the lifecycle of users.

1. To install IdentityIQ, first identify the platform and prerequisites. For this build, we used Windows 2019 with Apache Tomcat 9.0, and MS SQL Server 2019 as recommended requirements for release 8.2. Download the installation file from the SailPoint website and follow the installation instructions.

2. Login into IdentityIQ from a web browser (http://localhost:8080) using the default login and password. Make sure to change the default password.

3. **Configure IQService**. This is needed in order to set up integration with AD.

4. Govern permissions by pushing both employee and contractor users and groups to AD and Okta. Note: This step should be completed after the integration with AD and Okta is completed. Steps to configure integration are in Sections 2.3.3 and 2.3.4. After integration with AD and Okta is completed, navigate to the **Setup** drop-down menu and select **Roles**. Here we will create birthright role and access profile for employees and contractors.

   a. Select **New Role** drop-down button and select Role. The screenshot lists the four roles that are created for this build.
b. For the **Employee Birthright Role**, use the configuration shown in the next two screenshots. Note that the **Assignment Rule** is where the value of **employee** is used to identify the users. This will push users into AD as a birthright. Once that role is configured, configure the corresponding contractor role the same way. Note that the **Assignment Rule** should be different for the contractor based on user information in SailPoint.

c. For the **Employee Access Profile** role, add the groups that the employees belong to. This means that these users will have access to these groups as a birthright. Perform the same for the corresponding contractor role. Note that the **Entitlements** should be different for the contractor based on group information in Okta and AD.
5. The next step is to synchronize users and groups. To begin, navigate to the **Setup** tab and select **Tasks**.

   a. To create user aggregation, select the **New Task** drop down button and select **Account Aggregation**. The figure below depicts the aggregation configuration for Radiant Logic. This allows SailPoint to sync with Radiant Logic on any updates made to users. Repeat this step for AD and Okta accounts. Note that the **Account Aggregation Options** section is where the AD and Okta applications need to be selected to create the proper account aggregation.

   ![Entitlements Table](image)

   ![Standard Properties](image)

   ![Account Aggregation Options](image)

   b. To create group aggregation, select the **New Task** drop down button and select **Account Aggregation**. This allows SailPoint to sync with AD on any updates made to users. Repeat this step for the Okta account. Note that the **Account Group Aggregation Options** section is where the Okta applications need to be selected to create the proper account aggregation.
6. Configure lifecycle processes through Rapid Setup Configuration. Click on the **Setup** cog and select **Rapid Setup** to begin. The Rapid Setup Configuration process allows onboarding of applications and manage functions such as joiner, mover, and leaver of identities. Use the “Using Rapid Setup” section of the [IdentityIQ Rapid Setup Guide](#) to guide the configuration.

   a. The following screen captures show the configuration we used for **Joiner**.
b. The following screen captures show the configuration we used for **Mover**.
c. The following screen captures show the configuration we used for Leaver.
<table>
<thead>
<tr>
<th>Joiner</th>
<th>Mover</th>
<th>Leaver</th>
<th>Identity Operations</th>
<th>Miscellaneous</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reassign Antifraud Types</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reassign Antifraud</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Select Rule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reassign Antifraud Alternate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The Administrator</td>
<td></td>
</tr>
</tbody>
</table>

Reassignment controls are prioritized as follows: the first to return a result is used. Assign to manager, Assign by rule, Assign to alternative.

<table>
<thead>
<tr>
<th>Joiner</th>
<th>Mover</th>
<th>Leaver</th>
<th>Identity Operations</th>
<th>Miscellaneous</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reassign Identifies</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reassign Identifies To Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reassign Identifies Rule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Select Rule</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reassign Identifies Alternate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The Administrator</td>
<td></td>
</tr>
</tbody>
</table>

Send Leaver Notification to this Workgroup

Ownership Reassignment Notification Email Template
Leaver Ownership Reassignment Notification
Leaver Completed Notification Email Template
Leaver Completed Notification
d. The following screen captures show the configuration we used for **Identity Operations**.
e. Configure Rapid Setup specific to AD users: Aggregation, Joiner, Mover, and Leaver based on the following screenshots. Note: The Joiner setup used the default configuration, so it is not included in the screenshots.
7. Govern user permissions to applications on an individual basis. Configure procedures to provision and approve user access to resources. For Enterprise 1, the process is for an administrator or user to request approval to access an application. That request goes to the user’s manager.
for review and approval. Once the manager approves the request, SailPoint kicks off an API call to Okta to configure access for that user.

### 2.3.2 Integration with Radiant Logic

1. In the **Applications** tab, select **Application Definition**. When the screen comes up, click on the **Add New Application** button.

2. Enter values for the **Name** (e.g., “Ent1-HR”) and **Owner** (e.g., “The Administrator”) fields. Select **LDAP** as the **Application Type** and ensure that **Authoritative Application** is enabled.

3. Click on the **Configuration** tab next to the current tab. The credentials that were created in Radiant Logic will need to be added.

4. Scroll down the screen and under the **Account** tab, add the Search DN, which is the one created from Radiant Logic.

5. Click on **Test Connection** to make sure that SailPoint is able to connect to Radiant Logic. Click **Save**.

6. You can go back into the **Configuration** tab and **Schema** sub-tab. Toward the bottom of the screen, there is a **Preview** button. You can click on that to preview attributes imported. Note: We manually added schema attributes. This can be completed from Radiant Logic and imported. Please ensure that you have the correct attributes to integrate this.

7. To complete the setup, click **Save** to finish and import users from Radiant Logic.

8. Go to the **Setup** tab and click **Tasks**. Once in the new tab, click on the **New Task** button at the top right corner to create the account aggregation for Radiant Logic.
9. Perform identity attribute mapping. The screen capture shows mappings specific to this build only.

2.3.3 Integration with AD

1. Navigate to the Applications tab, click on Application Definition, then click the Add New Application button. Fill out the Name (e.g., “Ent1-AD-Ent-Users”), Owner (e.g., “The Administrator”), and Application Type (“Active Directory – Direct”).

2. Navigate to the Configuration tab. From here, input information for the IQ Service Host. The IP address is this server, the IdentityIQ server. IQ Service User is a user that was created in AD for this integration.

3. Scroll down to the Domain Configuration section. Input the domain information for where the users will be provisioned.
4. Scroll down to the **User Search Scope** section and input the Search DN information. This should be the AD domain location for your enterprise.

5. Navigate to the **Schema** and **Provisioning Policies** sub-tabs, and update information as necessary.

6. Then navigate to the **Correlation** tab to configure the correlation for application and identity attributes between SailPoint and AD.

7. Click **Save** to complete the configuration.

8. Go to **Setup** tab and click **Tasks**. Once in the new tab, click on the **New Task** button at the top right corner to create the account aggregation for AD.

### 2.3.4 Integration with Okta

1. Go into the **Applications** tab and select **Application Definition**. When the screen comes up, click on the **Add New Application** button.

2. Fill out the **Name** (e.g., “Ent1-Okta”) and **Owner** (“The Administrator”), select **Okta** as the **Application Type**, and enable the **Authoritative Application** option.
3. In the **Configuration** settings tab, the Okta URL and API token are needed. Note that the API token is created in Okta. Click **Save** to finish the setup.

![Okta Connection Settings](image)

### 2.4 Ivanti Neurons for UEM

Ivanti Neurons for UEM is a unified endpoint management (UEM) solution which is used to provision endpoints, grant access to enterprise resources, protect data, distribute applications, and enforce measures as required.

#### 2.4.1 Installation and Configuration

##### 2.4.1.1 Install an MDM certificate for Apple devices

The Apple Push Notification service (APNs) certificate needs to be installed in Ivanti Neurons for UEM to communicate with Apple devices. Apple devices use an APNs certificate to learn about updates, MDM policies, and incoming messages.

To acquire and install the MDM certificate:

1. Open the Ivanti Neurons for UEM console and go to **Admin > Apple > MDM Certificate** page to download a certificate signing request (CSR).
2. Upload the CSR to [Apple Push Certificates Portal](https://apple.com) to create a new certificate.
3. Save the resulting certificate.
4. Install the certificate for Ivanti Neurons for UEM tenant.
2.4.1.2 Configure Android Enterprise

Android Enterprise allows personal and corporate applications on the same Android device. Android Enterprise configuration depends on the type of Google subscription. Please follow Ivanti documentation to set up the integration.

The Android Enterprise Work Profile configuration defines which features and apps are allowed, and which are restricted on Android enterprise devices. Do the following to configure the profile:

1. In the Cloud portal, go to Configurations and click Add.
2. Select the Lockdown & Kiosk: Android Enterprise configuration.
3. Enter a configuration name and description.
4. Click the Work Profile lockdown type.
5. Select the lockdown settings for Android devices.

2.4.1.3 Add a Certificate Authority

A certificate authority (CA) generates self-signed certificates to be used by the devices that Ivanti Neurons for UEM manages. For this implementation we used an external certificate authority (DigiCert) and a Connector to access it. Ivanti Cloud Connector provides access from the Ivanti Neurons for UEM service to corporate resources, such as an LDAP server or CA.

1. Install and configure a Connector (Admin > Connector).
2. In the Certificate Management page, click Add under the Certificate Authority section.
3. Choose Connect to a publicly-trusted Cloud Certificate Authority.
4. Enter a name for the CA.
5. Download the certificate from DigiCert and upload it to Ivanti Neurons for UEM.
2.4.1.4 Configure user settings

User settings define device registration options. Access them by opening Ivanti Neurons for UEM and going to Users > User Settings. Configure device and password settings there.

2.4.1.5 Add a policy

Policies define requirements for devices and compliance actions (what happens if the rule is violated). To add a policy:

1. Go to Policies and click +Add (upper right).
2. Select a policy type and complete the settings. Policy types include Compromised Devices, Data Protection/Encryption Disabled, MDM/Device Administration Disabled, Out of Contact, and Allowed Apps.
3. Select the device groups that will receive this policy.

The following screenshots show an example of a Data Protection policy to be distributed to a custom group of devices.
2.4.1.6 Add a configuration for managed devices

Configurations are collections of settings that Ivanti Neurons for UEM sends to devices. To add a configuration:

1. Click Add.

2. Select the type of configuration. There are numerous types of configurations available, including Privacy, Certificate, Default App Runtime Permissions, Passcode, Exchange, Wi-Fi, VPN, iOS/macOS/Windows Restrictions, and Software Updates.
3. Click **Next**.

4. Select a distribution level for the configuration.

Here is an example of a Privacy configuration:

```
Name
Privacy policy

Add Description

Configuration Setup

- Collect Location Data
  - Collect the device's last known location based on check-in.
- Disable Device Wipe Action (User-Owned Devices Only)
  - Prevent admins and users from wiping the device.
- Prompt user to enable location services if WiFi/NTTD configuration
  - Pushed (Fully Managed and Work profile for Company-Owned Devices)

Collect App Inventory
- For Apps on the Device that are in the App Catalog
- For All Apps on the Device
  - This must be selected in order to use the Allowed Apps Policy

Note: Device Wipe action and option to collect App Inventory for all Apps on device is not applicable for User Enrollment.
```

This is an example of an iOS AppConnect configuration:
2.4.2 Integration with Ivanti Connector

Ivanti Connector provides access from Ivanti Neurons for UEM to corporate resources, such as an LDAP server. For the latest Connector installation instructions, select the appropriate version of the Cloud Connector Guide.
1. Once the Ivanti Connector has been set up and configured, navigate to the Ivanti Neurons for UEM console.

2. Connect to an LDAP Server to import users and groups. Navigate to Admin > Infrastructure > LDAP > Add Server. Complete configurations and save. Users can now be imported from the LDAP server.

### 2.4.3 Integration with Okta

#### 2.4.3.1 IdP setup

1. Go to Admin > Infrastructure > Identity > Add IdP.

2. Generate a key for uploading to Okta IdP.

3. Log in to Okta IdP. Search IdP for the MobileIron Cloud App and add it to the IdP account.

4. Configure the MobileIron Cloud App on the IdP by pasting the above-generated key and the host information.

5. Export metadata from Okta to the Ivanti Neurons for UEM console.

6. In Admin > Infrastructure > Identity > Add IdP, select Choose File to import the downloaded metadata file to Ivanti Neurons for UEM and complete the setup.

7. When an IdP is added, user authentication automatically switches from LDAP to IdP.

#### 2.4.3.2 Okta Verify app configuration preparation

1. In the Okta Admin console, navigate to Security > Device Integrations and click Add Platform.

2. Select platform and click Next.

3. Copy the Secret Key for later usage and enter Device Management Provider and Enrollment Link settings.

4. Repeat for any other device platforms.

#### 2.4.3.3 Okta Verify app configuration - Android

1. In the Ivanti Neurons for UEM console, navigate to Apps > App Catalog. Click Add.

2. Select the Google Play Store and search for Okta Verify. Select the official Okta Verify app.

3. Continue through the wizard until you reach the App Configurations page. Click the + button in the Managed Configurations for Android section.
4. Add desired settings. Under **Managed Configurations**, add the **Org URL** and **Management Hint** from the Okta Admin console. The Management hint will be the **Secret Key** you saved from the Okta console during preparation.

5. Click **Next**, then click **Done**.

**2.4.3.4 Okta Verify app configuration - iOS**

1. In the Ivanti Neurons for UEM console, navigate to **Apps > App Catalog**. Click **Add**.
2. Select the iOS Store and search for **Okta Verify**. Select the official **Okta Verify** app.
3. Continue through the wizard until you reach the App Configurations page. Click the **+** button in the Apple Managed App Configuration section.
   a. For the first item, the key will be **domainName**, the value will be your Org URL, and the type will be STRING.
   b. For the second item, the key will be **managementHint**, the value will be the **Secret Key** you saved from the Okta console during preparation, and the type will be STRING.
5. Click **Next**, then click **Done**.

**2.5 Ivanti Sentry**

Ivanti Sentry is an in-line gateway that manages, encrypts, and secures traffic between the mobile device and back-end enterprise systems. In this build, Ivanti Sentry acts as a PEP that controls access to enterprise resources.

**2.5.1 Installation and Configuration**

For this implementation we used a Standalone Sentry installation on-premises. For the latest Sentry installation instructions, select the appropriate version of the **Standalone Sentry On-Premises Installation Guide** at [https://www.ivanti.com/support/product-documentation](https://www.ivanti.com/support/product-documentation).

Next, create a profile for Standalone Sentry in the Ivanti Neurons for UEM console. For information on how to create a profile for Standalone Sentry and configure Standalone Sentry for ActiveSync and AppTunnel, see the **Sentry Guide for Cloud**.

**2.5.2 Ivanti Tunnel Configuration and Deployment**

Ivanti Tunnel is an application that connects a mobile device to the Ivanti Sentry. The process to deploy this app is similar to the deployment of the Okta Verify app in **Section 2.1.2**.
1. On the **App Configurations** page for the Tunnel app, create a Managed Configuration.
2. Set the **Tunnel Profile Mode** to **MobileIron Sentry + Access**.
3. Set the **Sentry Server** to the Sentry instance you created previously.
4. Set the **SentryService** to the name of the IP Tunnel defined on the Sentry.
5. Set the **ClientCertAlias** to the Sentry certificates you defined during Sentry configuration.
6. Set any other options as needed.
7. Save the Managed Configuration and deploy to devices as needed.

### 2.6 Ivanti Access ZSO

Ivanti Access ZSO is a cloud-based service that allows access to enterprise cloud resources based on user and device posture, and whether apps are managed or not. In this build, Ivanti Access ZSO functions as a delegated IdP, with Okta passing certain responsibilities to Ivanti Access ZSO.

#### 2.6.1 Integration with Ivanti Neurons for UEM

1. Ensure that you have the **Manage MobileIron Access Integration** role in Ivanti Neurons for UEM enabled at **Admin > System > Roles Management**.
2. Navigate to **Users > Users** and click **Add > API User**.
3. Next, navigate to **Users > Users** and click on the username of the user you just created. Navigate to the **Roles** tab of that user and add the **Manage MobileIron Access Integration** role.
4. In the Ivanti Neurons for UEM console, go to **Admin > Infrastructure > Access**.
5. Enter the following: **Access Admin URL**, **Access Admin Username** (username for the Access administrator account created for Access integration), and **Access Admin Password**.
6. Click **Register**.
7. When Access is registered with Ivanti Neurons for UEM, you should see the following:
2.6.2 Integration with Okta

1. In the Okta Admin console, navigate to Security > API and generate an API token. Save this token for use in Access.
2. In the Ivanti Access ZSO console, navigate to Profile > Federation.
3. Select Add Pair > Delegated IDP and choose Okta.
4. Enter the Okta Domain URL and the Okta API Token you generated in Step 1. Click Verify.
5. Once the verification is complete, select the routing rules you’d like configured and click Next.
7. Choose the desired Unmanaged Device Authentication setting and click Done.
8. You will see Okta in the Delegated IDP section, and Okta will route authentication requests based on your settings.

2.7 Zimperium Mobile Threat Defense (MTD)

Zimperium can retrieve various device attributes, such as device name, model, OS, OS version, and owner’s email address. It then continuously monitors the device’s risk posture and reports any changes in the posture to Ivanti Neurons for UEM.

2.7.1 Installation, Configuration, and Integration

2.7.1.1 Create an API user

To configure a Zimperium MTD console to work with Ivanti Neurons for UEM, an API user needs to be created and assigned a few roles.

1. In the Ivanti Neurons for UEM admin console, select Users.
2. Click + Add > API user. The Add API User dialog page opens.
3. Enter the following details: Username, Email, First Name, Last Name, Display Name, and Password.
4. Confirm the password.
5. Deselect the Cisco ISE Operations option.
6. Click Done.
2.7.1.2 Assign roles to the API user

1. From the admin console, go to Users.
2. Select the new API user created previously.
3. Click Actions.
4. From the User details page, select Assign Roles.
5. Select the following roles: App & Content Management, App & Content Read Only, Common Platform Services (CPS), Device Actions, Device Management, Device Read Only, System Read Only, and User Read Only.

2.7.1.3 Add an MDM server to the Zimperium console

1. Log in to the Zimperium MTD console.
2. Navigate to Manage > Integrations > Add MDM.
3. Select Cloud to add it to the MTD console as an MDM server.
4. Enter the following required information: URL, Username/Password, MDM Name, and Background Sync.
5. Click Finish.

2.7.1.4 Activate MTD on Ivanti Neurons for UEM

1. From the Ivanti Neurons for UEM admin console, go to Configurations.
2. Click +Add.
3. Click Mobile Threat Defense Activation.
4. In the Create Mobile Threat Defense Configuration page, enter a name for the configuration.
5. In the Configuration Setup section, select the vendor Zimperium.
6. In the License Key field, enter a unique encrypted Mobile Threat Defense activation code.
7. In the Wake up Intervals (mins) field, set a time.
8. Click Next.
9. Select the Enable this configuration option.
10. Select All Devices.
11. Click **Done**.

### 2.7.1.5 Add custom attributes in Ivanti Neurons for UEM

Custom device attributes will be applied to both Android and iOS devices based on threat severity.

1. To create custom attributes, in the Ivanti Neurons for UEM admin console go to **Admin > System > Attributes**. Enter each attribute name in lower case.

2. Create the custom attribute **mtdnotify** for **Low or Normal** severity threats:
   
   a. Click **Add New**. The **Attribute Name** and **Attribute Type** fields are displayed.
   
   b. Select **Device** as the attribute type.
   
   c. Name the custom attribute **mtdnotify**.
   
   d. Click **Save** to monitor and notify.

3. Create the custom attribute **mtdblock** for **Elevated or Critical** severity threats:
   
   a. Click **Add New**.
   
   b. Select **Device** as the attribute type.
   
   c. Name the custom attribute **mtdblock**.
   
   d. Click **Save** to monitor and notify.

4. Create the custom attribute **mtdquarantine** for **Elevated or Critical** severity threats:
   
   a. Click **Add New**.
   
   b. Select **Device** as the attribute type.
   
   c. Name the custom attribute **mtdquarantine**.
   
   d. Click **Save** to monitor, notify, and quarantine.

5. Create the custom attribute **mtdtiered4hours** for **Low, Normal, Elevated, or Critical** severity threats:
   
   a. Click **Add New**.
   
   b. Select **Device** as the attribute type.
   
   c. Name the custom attribute **mtdtiered4hours**.
   
   d. Click **Save** to monitor and notify, wait for four hours, block, wait for another four hours, and quarantine.
2.7.1.6 *Create Compliance Policy*

Create compliance actions using custom policies based on the MTD custom attributes created above.

1. In Ivanti Neurons for UEM admin console, go to **Policies**.
2. Click **+ Add**.
3. Select **Custom Policy**.
4. Enter **mtdnotify** as the policy name.
5. Under **Conditions**, select **Custom Device Attribute**.
6. Select **mtdnotify** from the drop-down box and set the condition is equal to 1.
7. Under **Choose Actions**, select **Monitor** and **Send Email and Push Notification**.
8. Under **Email Message** fields, enter the subject and body text.
10. Click **Yes, Next**, and **Done**.
11. Repeat this procedure to add the following policies: **mtdblock**, **mtdquarantine**, **mtdtiered4hours**.
12. Add other policies if needed.
2.7.1.7 Create device groups and match with custom policies and custom device attributes created above

1. In Ivanti Neurons for UEM admin console, go to Devices > Device Groups.
2. Click + Add.
3. Enter mtdNotify as the device group name.
4. Under Dynamically Managed groups, select Custom Device Attribute.
5. Select mtdnotify from the drop-down box and set the condition is equal to 1.
6. Click Save.
7. Repeat this procedure to add the following groups: mtdBlock, mtdQuarantine, mtdTiered4hours.

2.7.1.8 Configure Zimperium MTD management console

Set up, configure, and use the MTD console for supported MTD activities. When configuring policies in the Zimperium admin console, use the available MDM actions and Mitigation actions.

2.8 IBM Cloud Pak for Security

IBM Cloud Pak for Security platform enables the integration of existing security tools and provides understanding and management of threats in the environment.
1. **Deploy an OpenShift cluster.** OpenShift needs to be in place before Cloud Pak for Security can be installed.

2. **Install Cloud Pak for Security.**

3. **Configure LDAP authentication** so Cloud Pak for Security can leverage an existing LDAP directory server for authentication.

Once those steps are complete, open a web browser and navigate to the DNS name for Cloud Pak for Security. Additional documentation can be found at Cloud Pak for Security Documentation.

### 2.9 IBM Security QRadar XDR

IBM Security QRadar platform provides various security capabilities including threat detection and response, security information and event management (SIEM), and security orchestration, automation and response (SOAR).

Install and configure QRadar following IBM’s QRadar Installation and Configuration Guide.

Once that is complete, open a web browser and navigate to the QRadar server web interface by using its IP address or DNS name.

### 2.10 Tenable.io

Tenable.io is a cloud-based platform that is used in this build to provide network discovery, vulnerability, and scanning capabilities for on-premises components.

#### 2.10.1 Installation and Configuration

As a cloud-based platform, a license must first be obtained, and a cloud instance deployed by Tenable. Once deployed by a Tenable representative, Tenable.io can be accessed through the web interface located at https://cloud.tenable.com.

#### 2.10.1.1 Deploy an agent

1. In Tenable.io, click the hamburger menu (☰) in the top left corner and navigate to **Settings > Sensors > Nessus Agents.**

2. Click **Add Nessus Agent** and save the Linking Key.


4. In the setup window, fill in the key from step 2, the server (in our case, cloud.tenable.com:443), and the agent groups that this agent will be part of (in our case, Default). Click **Next.**
5. Click **Install** and approve the request if User Account Control (UAC) comes up.

6. When installation completes, updates will continue running in the background. The update and connection process may take some time. The endpoint will then be shown in the cloud tenant.

![Screen shot of Tenable.io with Nessus scanner details]

### 2.10.1.2 Deploy a scanner

1. In Tenable.io, navigate to **Settings > Sensors > Cloud Scanners**.

2. Click **Add Nessus Scanner** and save the Linking Key.

3. Download the Nessus Scanner .ova file from [https://downloads.tenable.com](https://downloads.tenable.com).

4. Deploy the .ova file in your virtual environment.

5. Once the scanner is running, navigate to the IP address shown in the console in a web browser.

6. Login with the default username *wizard* and default password *admin*.

7. Enter new administrator credentials and click **Create Account**.

8. Click **Finish Setup** and authenticate with the new administrator credentials.

9. On the left-side navigation pane, click **Nessus**.

10. Click the URL shown in the **Nessus Installation Info** pane.

11. Click the radio button next to **Managed Scanner** and click Continue.

12. Enter the Linking Key from step 2 and click **Continue**.

13. Enter credentials for a new administrator account and click **Submit**.

14. The scanner will initialize and be visible on tenable.io. Scans can now be scheduled.

### 2.10.2 Integration with QRadar

For Tenable.io and QRadar integration, follow the [Tenable and IBM QRadar SIEM Integration Guide](https://www.tenable.com/resources/whitepapers/qradar-siem-integration-guide).
2.11 Tenable.ad

Tenable.ad provides AD monitoring to detect attacks and identify vulnerabilities. In this build, Tenable.ad is integrated with the on-premises AD installation and configured to forward alerts to the IBM QRadar SIEM.

For Tenable.ad installation and configuration, follow the [Tenable.ad On-Premise Installation Guide](#).

For Tenable.ad and QRadar integration, follow the [Tenable and IBM QRadar SIEM Integration Guide](#).

2.12 Mandiant Security Validation (MSV)

Mandiant Security Validation (MSV) allows organizations to continuously validate the effectiveness of their cybersecurity controls by running actions that may conflict with the organization’s policy and determining if those actions are detected and/or blocked. In this build, MSV is configured to regularly test the build’s zero trust policies and report on the results.

2.12.1 MSV Director Installation/Configuration

1. Download the MSV Director software from the Mandiant web portal and deploy it in a virtual environment.
2. Log into the MSV command line interface using credentials provided by Mandiant.
3. Run the command `sudo vsetnet` to apply network configuration.
4. Run the command `sudo vsetdb --password new_password` to set a new password for the Director database.
5. Use a web browser to access the MSV Director web interface at `https://Director IP/`.
6. Sign into the web interface using credentials provided by Mandiant.
7. Accept the End User Licensing Agreement and apply the license provide by Mandiant.
8. Configure the DNS settings by navigating to **Settings > Director Settings > DNS Servers**.
9. Configure the NTP settings by navigating to **Settings > Director Settings > NTP Servers**.
10. Add Security Zones corresponding with the enterprise’s network segments by navigating to **Environment > Security Zones**.
11. Download security content from the Mandiant web portal.
12. Navigate to **Settings > Director Settings > Content**.
13. Select **Import**, browse to the downloaded security content, and select the content files.
14. Click **Upload Import** and upload the files into the MSV Director web interface.
15. Once the upload is complete, click **Apply Import** to import the content files into MSV.

### 2.12.2 MSV Network Actor Installation/Configuration

1. Download the MSV Network Actor software from the Mandiant web portal and deploy it in a virtual environment.
2. Log into the MSV command line interface using credentials provided by Mandiant.
3. Run the command `sudo vsetnet` to apply network configuration.
4. In the MSV Director web interface, navigate to **Environment > Actors**.
5. Click **Add Network Actors** and fill out the new **Actor** form.
6. Identify the Actor you just created in the **Pending Actors** table, expand the **Actions** menu, and click **Connect** to initiate a Director-to-Actor registration.
7. Enter the Actor’s FQDN or IP address.

### 2.12.3 MSV Endpoint Actor Installation/Configuration

1. Deploy an endpoint machine running Windows, macOS, or Linux.
2. In the MSV Director web interface, navigate to **Library > Actor Installer Files** and download the relevant installer onto the endpoint.
4. Execute the Actor installer on the endpoint and proceed through the install process.
5. At the end of the install process, identify the actor you just created in the **Pending Actors** table and enter the value from the **Code** field into the Actor configuration field.
6. The endpoint will register itself with the MSV director and setup will be complete.
2.12.4 MSV Evaluation Configuration

1. Once the MSV Director and Actors have been configured, evaluations can be created to test security controls and policies. In the MSV Director web interface, navigate to Library > Actions.

2. Find the action(s) you would like to use for the evaluation and select the +Queue button to add the action to the Queue. Repeat this process until you have added all needed actions to the Queue.

3. After actions have been added to the Queue, click the Queue button in the upper right side of the web interface.

4. Select each of the actions in the Unassigned section and drag them to the Current Actions section.

5. Scroll up to the top of the page and click the Save button.

6. Under the Test Type dropdown, choose Evaluation.
7. Under the **Name** section, enter a name.

8. Under the **Description** section, enter a description.

9. Select the **Save** button to save the evaluation.

10. Your new evaluation can be found by navigating to **Library > Evaluations** and filtering on **User Created**.

### 2.12.5 MSV Evaluation Execution

1. Navigate to **Library > Evaluations** and select the evaluation you’d like to run. Click the **Run** button.

2. From the Evaluation screen, press the **Run Evaluation** button.

3. Select the **Source Actor** and **Destination Actor** from the dropdown menus. Click **Run Now**.

4. The evaluation will run, providing results once the actions have been attempted/completed.
2.13 DigiCert CertCentral

CertCentral simplifies digital trust and automates certificate management by consolidating tasks for issuing, installing, inspecting, remediating, and renewing TLS/SSL certificates in one place. In this build, CertCentral provided TLS/SSL certificates to any system needing those services.

For the latest CertCentral setup and usage instructions, see https://docs.digicert.com/get-started/.

2.14 AWS IaaS

This section will be part of the EIG run phase and will be included in the next version of the practice guide.

3 Enterprise 3 Build 1 (EIG E3B1) Product Guides

This section of the practice guide contains detailed instructions for installing, configuring, and integrating all of the products used to implement EIG E3B1. For additional details on EIG E3B1’s logical and physical architectures, please refer to NIST SP 1800-35B.

3.1 Microsoft Azure Active Directory (AD)

Azure AD is a SaaS Identity and access management platform. No installation steps are required. You will need to create your organization’s instance of Azure AD and configure it to allow your users access to applications that use it for authentication and authorization.
1. After logging in to portal.azure.com, create an Azure AD Tenant.
2. Create a connection between your on-premises AD and Azure AD to replicate user, group, and authentication information from your AD to Azure AD.
3. Configure the Azure AD Tenant to enable Single Sign-On Password Reset (SSPR). This gives users the ability to reset their passwords from https://aka.ms/sspr or from within their profile in Azure AD. This will be effective for both their AD and Azure AD accounts.
4. Configure password writeback, which enables password changes in Azure AD to be replicated back to the on-premises AD.
5. The conditional access feature in Azure AD specifies conditions under which a user would be given access to a resource or application that uses Azure AD for authentication. MFA was configured as a requirement for access to all applications. Configure MFA for all users.
6. Access to resources based on device compliance was implemented as an essential feature in this solution. Access would only be granted to a user if the client device is compliant. Compliance is reported to Azure AD by Microsoft Endpoint Manager. Enable this feature, Conditional Access, Device Compliance.
7. Configure an enterprise application, GitLab, to use Azure AD for authentication:
   a. GitLab was configured to directly authenticate to Azure AD using the SAML protocol. GitLab must first be registered in Azure AD before Azure AD can be configured as the application’s IdP.
   b. Configure Azure AD as a SAML IdP for the GitLab application. Once that is implemented, access attempts to the target application will be redirected to Azure AD for authentication and authorization.

### 3.2 Microsoft Endpoint Manager

Microsoft Endpoint Manager is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM).

### 3.2.1 Configuration and Integration

#### 3.2.1.1 Add and verify a custom domain

To connect an organization’s domain name with Intune, a DNS registration needs to be configured. This gives users a familiar domain when connecting to Intune and using resources.

1. Go to the Microsoft 365 Admin Center (admin.microsoft.com) and sign into your administrator account.
2. Choose Setup > Domains.

3. Choose Add domain and type a custom domain name. Select Next.

4. The Verify domain dialog box opens, giving the values to create the TXT record with the DNS hosting provider.

3.2.1.2 Add users

Once you sign into Microsoft Intune, you can add users directly or synchronize users from an on-premises AD. Once added, users can enroll devices and access company resources.

3.2.1.3 Enroll devices in Microsoft Intune

Enrolling devices allows them to receive configuration profiles and compliance policies. Configuration profiles configure features and settings on devices. Compliance policies help devices meet an organization’s rules.

1. Get an Apple MDM push certificate and add it to Endpoint Manager. This certificate is required to enroll iOS/iPadOS devices. Then enroll iOS devices in Microsoft Intune.

2. Create an iOS enrollment profile. An enrollment profile defines the settings applied to a group of devices during enrollment.
3. **Enroll Android devices in Microsoft Intune**. To enable Android Enterprise, an administrative Google account needs to be connected to the Intune tenant.

4. **Create an iOS compliance policy in Microsoft Intune**. It will be evaluated before access is allowed from iOS devices.

5. **Create an Android compliance policy in Microsoft Intune**. It will be evaluated before access is allowed from Android devices.

6. **Create an iOS/macOS configuration profile** for iOS or Mac devices.

7. **Create an Android configuration profile**.

8. **Create a Windows configuration profile**.

**3.2.1.4 Configure Conditional Access rules**

Conditional Access is used to control the devices and apps that can connect to company resources.

1. Go to **Devices > Conditional Access** and click **New Policy**. Choose cloud apps or actions, conditions, and access controls to create a policy. The screenshot below illustrates this.

2. The multi-factor authentication rule enabled in the screenshot will require MFA before granting access to enterprise Office 365 apps.
3. The Conditional Access Device Access Policy is enabled in the screenshot. It requires devices to be marked as compliant in order to get access to enterprise resources.

3.2.1.5 Managing Applications

iOS/iPadOS: Use the instructions at Add iOS Store Apps to select apps from the iOS/iPadOS store that will be approved for installation on your managed iOS or iPadOS devices.
Android: For this build we added Managed Google Play apps. Managed Google Play is Google’s enterprise app store which serves as a source of applications for Android Enterprise in Intune. Use the instructions at Add Android Store Apps to select apps that will be approved for installation and made available to your managed devices.

Windows: We tested this build with Microsoft 365 Apps for Windows 10 and later. To add Windows apps:

1. Open the Microsoft Endpoint Manager admin center.
2. Select Apps > All apps > Add.
3. Select Windows 10 and later in the Microsoft 365 Apps section of the Select app type pane.
4. Click Select. The Add Microsoft 365 Apps steps are displayed.

There is more than one way to configure Windows apps in Intune. We configured the app using App suite information. For other ways, refer to the Microsoft documentation.

macOS: Follow these steps to add macOS apps:

1. Open the Microsoft Endpoint Manager admin center.
2. Select Apps > All apps > Add.
3. Select macOS in the Microsoft 365 Apps section of the Select app type pane.
4. Click Select. The Add Microsoft 365 Apps steps are displayed.
5. Confirm or modify the default values in the App suite information page.
3.3 Microsoft Defender for Endpoint

Microsoft Defender is an enterprise defense suite. Its main role is to detect and prevent threats and to provide protection to endpoints, identities, email, and applications. Microsoft Defender can provide device health information to the Microsoft Endpoint Manager (Intune).

3.3.1 Configuration and Integration

3.3.1.1 Enable Microsoft Defender for Endpoint

1. Open the Microsoft Endpoint Manager admin center.

2. Select Endpoint security > Microsoft Defender for Endpoint, and then select Open the Microsoft Defender for Endpoint admin console. This opens the Microsoft 365 Defender portal.

3. Select Settings > Endpoints > Advanced features.

4. For Microsoft Intune connection, choose On.

5. Return to the Microsoft Defender for Endpoint page in the Microsoft Endpoint Manager admin center.

6. Under MDM Compliance Policy Settings, enable Microsoft Defender connections for Android, iOS, and Windows devices. To be guided through the steps on licensing validation, tenant configuration, and network configuration, follow Microsoft’s documentation.

7. Onboard devices that run Android, iOS/iPadOS, and Windows 10/11.

3.3.1.2 Create Endpoint Detection and Response policy (Windows 10 and Later)

1. Open the Microsoft Endpoint Manager portal.

2. Navigate to Endpoint security > Endpoint detection and response. Click on Create Profile.


4. Enter a name and description, then select Next.

5. Select settings as required, then select Next.

6. Add scope tags if necessary, then select Next.

7. Click on Select groups to include and choose a group, then select Next.

8. Review and accept and select Create.

9. The completed policy appears in Endpoint detection and response.
3.3.1.3 Create an antivirus policy

1. Open the Microsoft Endpoint Manager portal.
2. Navigate to Endpoint security > Antivirus > Create Policy.
3. Select Platform - Windows 10 and Later - Windows and Profile – Microsoft Defender Antivirus > Create. Enter name and description, then select Next.
4. On the Configuration settings page, set the configurations for Microsoft Defender Antivirus
5. Add scope tags and select Next.
6. Select and assign groups to include, then select Next.
7. Review and then select Create.
8. The completed policy appears in Endpoint security.
3.3.1.4 Create Microsoft Defender compliance policy

Compliance policies can help protect organizational data by requiring users and devices to meet some requirements.

1. Open the Microsoft Endpoint Manager admin center.
2. Select Devices > Compliance policies > Policies > Create Policy.
3. Select a Platform for this policy.
4. On the Basics tab, specify a Name for the Policy.
5. On the Compliance settings tab, expand the available categories, and configure settings for the policy.
3.3.1.5 Deploy Defender for Endpoint on iOS via Intune company portal

1. In the Microsoft Endpoint Manager admin center, go to Apps > iOS/iPadOS > Add > iOS store app and click Select.
2. On the Add app page, click on Search the App Store, type Microsoft Defender for Endpoint in the search bar, and click Select.
3. Select the desired value for the Minimum operating system. Review the rest of information about the app and click Next.
4. In the Assignments section, go to the Required section and select Add group. Click Select and then Next.
5. In the Review + Create section, verify that all the information entered is correct and then select Create.

3.3.1.6 Configure supervised mode for iOS devices via Intune

1. Open Microsoft Endpoint Manager admin center and go to Apps > App configuration policies > Add. Select Managed devices.
2. In the Create app configuration policy page, provide Policy Name, Platform: iOS/iPadOS, Targeted app: Microsoft Defender for Endpoint.
3. In the next screen, select **Use configuration designer** as the configuration settings format. Specify the following property:

   a. **Configuration key:** issupervised
   b. **Value type:** String
   c. **Configuration value:** {{issupervised}}

3.3.1.7 **Deploy Microsoft Defender for Endpoint on Android with Microsoft Intune**

1. In the Microsoft Endpoint Manager admin center, go to Apps > Android Apps > Add > Android store app and choose Select.

2. On the Add app page enter: Name, Description, Publisher as Microsoft, App store URL as https://play.google.com/store/apps/details?id=com.microsoft.scmx (Defender for Endpoint app Google Play Store URL).

3. Select Next.

4. In the Assignments section, go to the Required section and select Add group, Select group and click Next.

5. The completed Android app configuration policy appears under All services > Apps.

6. On the Android mobile device, tap the Microsoft Defender for Endpoint app icon and follow the on-screen instructions to complete onboarding the app.

3.3.2 **Microsoft Defender Antivirus**

Microsoft Defender Antivirus is leveraged by Microsoft Defender by Endpoint, which is anti-malware software built into Windows client devices. It detects threats and malware on client devices and quarantines infected files. Defender Antivirus is enabled by default.

Ensure that real-time protection is enabled by running

```powershell
(Get-MpComputerStatus).RealtimeProtectionEnabled
```

at an elevated PowerShell prompt as shown in the screenshot below.

![Administrator: Windows PowerShell](image-url)
If real-time protection is off, it can be turned back on by executing

```powershell
Set-MpPreference -DisableRealtimeMonitoring $false
```

at an elevated PowerShell prompt as shown in the screenshot below.

Verify that real-time protection is on by going to Control Panel > System and Security > Security and Maintenance > Security > Virus Protection.

### 3.4 Microsoft Sentinel

Microsoft Sentinel is a cloud-native SIEM and SOAR system. It can be used for security analytics, threat intelligence, attack detection, and threat response.

There is no need to install Sentinel, as it is a managed service. Instead, it needs to be enabled and configured in your Azure environment. It also needs a workspace to store and correlate ingested data.

1. **Enable Sentinel and configure a workspace.**
2. Use the general instructions found at [Connector to Data Sources](#) to enable log forwarding to Sentinel from various devices, systems, and services. Each data source will have to be connected independently from other data sources, so you must perform this step once per data source. In this build, Azure AD, Endpoint Manager, Defender for Endpoint, Office365, and Tenable.io were configured to send logs using this method.
3. The Log Analytics Agent is a log forwarder that accepts syslog and common event format (CEF) formatted logs and then forwards the logs to Sentinel. If you have a product or device without a native Sentinel integration, install and configure the Log Analytics Agent on a virtual machine. Once completed, the log forwarder will be able to receive syslog data on UDP port 514. Then configure the product or device that will be the data source to send logs via syslog to the log forwarder using the product’s instructions.

### 3.5 F5 BIG-IP

BIG-IP is both a load balancer and an identity-aware proxy. In this phase of the build, it was primarily used as an identity-aware reverse proxy that forwarded or denied traffic to protected back-end applications.
3.5.1 Installation, Configuration, and Integration

BIG-IP was deployed into the environment using a virtual machine image or open virtual appliance (OVA) file. Once this OVA import operation is complete, you would log into the virtual machine console and assign an IP address to a network interface, then continue configuration by connecting to its web interface. This BIG-IP image has both the Access Policy Manager (APM) and the Local Traffic Manager modules installed.

1. Deploy BIG-IP OVA into your VMWare environment.

2. Access the BIG-IP web interface by entering the IP address or DNS name into a web browser. Then complete the initial setup and configuration of BIG-IP.

3. Create virtual servers which map to back-end protected applications—in this build, to our Guacamole application server.

4. Configure BIG-IP to use Azure AD as the SAML IdP for external authentication to access back-end applications. The instructions at Configure BIG-IP Easy Button for Header Based SSO and the video at Azure AD and BIG-IP APM Integration Video provide additional references.

5. Once these instructions are completed, BIG-IP, leveraging Azure AD for external authentication, will only allow successfully authenticated and authorized users to access Guacamole. Access to the backend application is either done by connecting directly via the DNS name of the application or by going to myapps.microsoft.com and selecting the backend application icon, such as F5 Guacamole_SSO as shown below.

6. For this build, configure BIG-IP to send logs to Microsoft Sentinel. Then you can observe BIG-IP logs in Sentinel, as shown below.
3.6 Lookout Mobile Endpoint Security (MES)

Lookout Mobile Endpoint Security (MES) solution is used to control mobile device access to corporate resources based on risk assessment. Risk is assessed based on information collected from devices by the Lookout service. Lookout then communicates this risk level to Mobile Device Management (Microsoft Endpoint Manager (Intune)) which determines whether the device is compliant or not.

3.6.1 Configuration and Integration

Before configuring Lookout, collect the following information from Azure AD: Azure AD tenant ID and Azure AD group object ID.

1. Go to Azure Active Directory > Properties and locate Tenant ID. Copy and save it to the text file.
2. Go to Azure Active Directory > Groups to open the Groups | All groups pane.
3. Select the group with full access rights (Lookout Admin group).
4. Copy the (group) **Object Id**, and then save it in a text file.

The following steps are to be completed in the Lookout Enterprise admin console and will enable a connection to Lookout’s service for Intune enrolled devices.

1. Sign in to the Lookout for Work console and go to **System > Integrations**, and then select **Choose a product to set up**. Select **Microsoft Azure**. Copy and paste the Azure AD (AAD) tenant ID and group object ID from the text file that was created in previous steps.

2. Stay in **System > Integrations**, and then select **Choose a product to set up**. Select **Microsoft Intune**.

3. Configure Intune connector settings.
After Lookout MES is enabled, a connection to Lookout in Intune needs to be set up.

1. Go back to Microsoft Endpoint Manager and enable the Mobile Threat Defense connector there.
2. Select Tenant administration > Connectors and tokens > Mobile Threat Defense.
4. For Mobile Threat Defense connector to setup, select Lookout MTD solution from the drop-down list.
5. Configure the toggle options according to the organization's requirements. This screenshot shows examples.

When Lookout is integrated with Intune MTD and the connection to Intune is enabled, Intune creates a classic conditional access policy in Azure AD. To view classic conditional access policy, go to Azure Active Directory > Conditional Access > Classic policies. Classic conditional access policy is used by Intune MTD to require that devices are registered in Azure AD so that they have a device ID before communicating to Lookout MTD. The ID is required so that devices can report their status to Intune.

3.6.2 Create MTD device compliance policy with Intune

Compliance policy is needed to detect threats and assess risks on mobile devices to determine if the device is compliant or not.

1. Open the Microsoft Endpoint Manager admin center.
2. Select Endpoint security > Device Compliance > Create Policy.
3. Select the Platform, and then Create.
4. On Basics, provide Name, and Description. Select Next to continue.
5. On Compliance settings, expand and configure Device Health. Choose the Mobile Threat Level from the drop-down list for Require the device to be at or under the Device Threat Level. Choose the level for compliance.
6. Select Next to go to Assignments. Select the groups or users to assign this policy.

3.7 PC Matic Pro

PC Matic Pro is an endpoint protection system that consists of a server for centralized management and agents installed on endpoints. In addition to scanning for malware, it uses a default-deny approach in preventing malicious or unauthorized programs and processes from executing. To configure PC Matic Pro, you will need to install the server, install the agents, and configure a list of allowed software.

PC Matic Pro Server needs to be installed on a server with Windows 2019 Server and SQL server preinstalled.

1. Obtain the $OnPremInstallerRun.ps1$ installation script from the vendor and open an elevated PowerShell window.

2. Execute the $OnPremInstallerRun.ps1$ script by entering \OnPremInstallerRun.ps1 registryUser pcmatic -registryPwd <insert_password_here> -localDBUser pcm-app to install docker, pull down the container images, and deploy the container instances that make up the PC Matic Pro server.

3. Navigate to the PC Matic web server and verify that it is operational by opening a web browser and going to $https://<pcmaticDNSName>/web_portal$. In this build, the DNS name is nist.pcmaticfederal.com; as such, to access the server’s web interface, we would go to https://nist.pcmaticfederal.com/web_portal.

Follow these steps to install PC Matic Endpoint Agents:

1. Open a web browser on a Windows or macOS client device. Navigate to the PC Matic Server web interface by browsing to https://nist.pcmaticfederal.com from the client device and log on with your credentials.

2. Click Add a Device and then click Windows Installer or Mac Installer, as appropriate, to download the PC Matic Endpoint Agent.

3. Install the agent.

4. Once installed, the agent will establish communications with the server and show up on the list of managed devices once you log on to the server as previously described.

5. Devices with an agent will register and come online.
3.8 Tenable.io

For installation, configuration, and integration instructions, refer to Section 2.10.

3.8.1 Integration with Microsoft Sentinel

1. In Tenable.io, click the hamburger menu (☰) in the top left corner and navigate to Settings > Access Control > Users.

2. (Optional) Click Create User and create a new API user for Microsoft Sentinel. In this implementation, a standard administrator account was used.

3. Click the user who needs API keys generated. Then click API KEYS > Generate > Continue. Save the Access and Secret Keys, as they will not be shown again.

4. In Microsoft Sentinel, navigate to Data Connectors. Search tenable and click Tenable.io Vulnerability Management (Preview) > Open Connector Page.

5. Scroll down in the Instructions panel and save the Workspace ID and Primary Key.

6. Click Deploy to Azure.

7. Select the appropriate resource group.

8. In the Workspace ID and Workspace Key fields, enter the values obtained in step 5.

9. In the Tenable Access Key and Tenable Secret Key fields, enter the values obtained in step 3.

10. Click Review + create.

11. Click Create. Function deployment will begin. Once deployment is complete, it will take some time before Sentinel begins making calls to Tenable.io.

3.9 Tenable.ad

For installation, configuration, and integration instructions, refer to Section 2.11.
3.10 Mandiant Security Validation (MSV)
For installation, configuration, and integration instructions, refer to Section 2.12.

3.11 Forescout eyeSight
Forescout eyeSight provides asset discovery with both active and passive techniques, and through integrations with network and security infrastructure. In this build, Forescout eyeSight was deployed on-premises in two virtual hosts: an Enterprise Manager and Forescout Appliance.

For Forescout eyeSight installation instructions, visit the Forescout Installation Overview.

3.11.1 Integration with AD
1. In AD, create a domain administrator service account for Forescout and save the credentials.
2. In the Forescout console, navigate to Tools > Options > HPS Inspection Engine.
3. In the Domain Credentials section, click the Add button.
4. Enter the domain information and credentials you saved earlier. Click OK.
5. Click Apply. After the new configuration is saved, click Test to verify that the credentials are working as expected.

3.11.2 Integration with Cisco Switch
For Cisco Switch integration instructions, visit the Switch Plugin Configuration Guide.

3.11.3 Integration with Cisco Wireless Controller
For Cisco Wireless Controller integration instructions, visit the Wireless Plugin Configuration Guide.

3.11.4 Integration with Microsoft Sentinel
1. In the Forescout console, navigate to Tools > Options > CEF.
2. Click Add.
3. In the Add Server dialog, enter a Name, select Use UDP for Connection, and enter the IP address of the Sentinel Log Forwarder. Click Next.
4. Click the Assign CounterACT Devices radio button, and check all of the checkboxes next to the listed devices.
5. Click Finish. Verify that logs are being received by the Sentinel Log Forwarder.
3.11.5 Integration with Palo Alto Networks NGFW
For Palo Alto Networks Next-Generation Firewall (NGFW) integration instructions, visit the eyeExtend for Palo Alto Networks Next-Generation Firewall Configuration Guide.

3.11.6 Integration with Tenable.io
For Tenable.io integration instructions, visit the eyeExtend for Tenable.io Vulnerability Management Configuration Guide.

3.12 Palo Alto Next Generation Firewall
In this build, a virtualized Palo Alto Next Generation Firewall was deployed on-premises as a security and access control device. The firewall provides zone-based network filtering for both inbound and outbound traffic, including remote access virtual private networks (VPNs) using the GlobalProtect clients.
For GlobalProtect VPN access installation instructions, visit: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFbCAK

3.13 DigiCert CertCentral
For setup and usage instructions, refer to Section 2.13.
## Appendix A  List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAD</td>
<td>(Microsoft) Azure Active Directory</td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>AG</td>
<td>(Okta) Access Gateway</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>APM</td>
<td>Access Policy Manager</td>
</tr>
<tr>
<td>APNs</td>
<td>Apple Push Notification service</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CEF</td>
<td>Common Event Format</td>
</tr>
<tr>
<td>CRADA</td>
<td>Cooperative Research and Development Agreement</td>
</tr>
<tr>
<td>CSR</td>
<td>Certificate Signing Request</td>
</tr>
<tr>
<td>DN</td>
<td>Domain Name</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>E1B1</td>
<td>EIG Enterprise 1 Build 1</td>
</tr>
<tr>
<td>E3B1</td>
<td>EIG Enterprise 3 Build 1</td>
</tr>
<tr>
<td>EIG</td>
<td>Enhanced Identity Governance</td>
</tr>
<tr>
<td>FQDN</td>
<td>Fully Qualified Domain Name</td>
</tr>
<tr>
<td>HDAP</td>
<td>High-Availability Directory Access Protocol</td>
</tr>
<tr>
<td>HR</td>
<td>Human Resources</td>
</tr>
<tr>
<td>IaC</td>
<td>Infrastructure as Code</td>
</tr>
<tr>
<td>ICAM</td>
<td>Identity, Credential, and Access Management</td>
</tr>
<tr>
<td>IdP</td>
<td>Identity Provider</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITL</td>
<td>Information Technology Laboratory</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>MAM</td>
<td>Mobile Access Management</td>
</tr>
<tr>
<td>MDM</td>
<td>Mobile Device Management</td>
</tr>
<tr>
<td>MEM</td>
<td>Microsoft Endpoint Manager</td>
</tr>
<tr>
<td>MES</td>
<td>(Lookout) Mobile Endpoint Security</td>
</tr>
<tr>
<td>MFA</td>
<td>Multi-Factor Authentication</td>
</tr>
<tr>
<td>MSV</td>
<td>Mandiant Security Validation</td>
</tr>
<tr>
<td>MTD</td>
<td>Mobile Threat Defense</td>
</tr>
<tr>
<td>NCCoE</td>
<td>National Cybersecurity Center of Excellence</td>
</tr>
<tr>
<td>NGFW</td>
<td>Next-Generation Firewall</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OU</td>
<td>Organizational Unit</td>
</tr>
<tr>
<td>OVA</td>
<td>Okta Verify App, Open Virtual Appliance</td>
</tr>
<tr>
<td>PA</td>
<td>Policy Administration</td>
</tr>
<tr>
<td>PDP</td>
<td>Policy Decision Point</td>
</tr>
<tr>
<td>PE</td>
<td>Policy Engine</td>
</tr>
<tr>
<td>PEP</td>
<td>Policy Enforcement Point</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertion Markup Language</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
</tr>
<tr>
<td>SOAR</td>
<td>Security Orchestration, Automation, and Response</td>
</tr>
<tr>
<td>SP</td>
<td>Special Publication</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign-On</td>
</tr>
<tr>
<td>SSPR</td>
<td>Single Sign-On Password Reset</td>
</tr>
</tbody>
</table>
### TLS
Transport Layer Security

### UAC
User Account Control

### UDP
User Datagram Protocol

### UEM
Unified Endpoint Management

### URL
Uniform Resource Locator

### VLAN
Virtual Local Area Network

### VPN
Virtual Private Network

### ZSO
Zero Sign-On

### ZTA
Zero Trust Architecture