State of Love & Trust

Sean Frazier - Advisory CISO - Federal
sean@duo.com | @seanfsez
What is Zero Trust, industry edition?

- 2004ish - Jericho Commandments
- 2010 - John Kindervag, father of Zero Trust
- 2014 - Google BeyondCorp
- 2017 - O’reilly Zero Trust Networks
Perimeter?
Securing Access in the Enterprise
Access happens everywhere – how do establish trusted access?

**Workforce**

- All Corp IT
- User & Device Access

**Workload**

- Data Center
  - Apps
  - Servers
  - Database
  - VM

**Workplace**

- Corporate Network
  - Network Traffic
  - Wireless
  - IoT Devices
  - User & Devices
  - Network Access

Access happens everywhere – how do establish trusted access?
Cisco Zero Trust

Secure the Workforce
With Duo

Secure Your Workloads
With Tetration

Secure the Workplace
With Software-Defined Access

MFA + Device Trust
Application Micro-Segmentation
Network Segmentation

Visibility | Policy | Enforce | Report

All Corp IT
Application Access
User & Device Access

Data Center
Apps
Servers
VM

Database
SaaS
Azure
AWS
Google Cloud

Servers
WAN
Routing

Corporate Network
Network Traffic
Wireless
IoT
Devices
User & Devices

User & Device Access
Workload Access
Network Access

Application Access
Workload Access
Network Access

Visibility
Policy
Enforce
Report
Figure 2: Core Zero Trust Logical Components
The User Journey – Cisco Zero Trust

Value to the Business Priorities

1. Ease of
   - Implementation
   - Use
   - Operations/FTE
   - Integration
2. Compliance
3. Risk Reduction
4. Visibility
5. Culture

Legacy to Cloud

BYOD & Agility

Network

IOT & Process Control

BYOD & Agility

Admiralrs

Tetration

Stealthwatch

Stealthwatch

Cloud Resources

Data Loss Phishing Malware

Umbrella

C2 Malware Phishing

User + Device

Administrators

AMP

CES

Value to the Business Priorities
Login Request
Protected by Duo Security

bedrock
Okta

fred@bedrock.mobi
69.42.7.98
Concord, CA, US
4:37:34 PM PST
February 19, 2018

Approve
Deny

wilma - microsoft
Microsoft Azure Active Directory

wilma@bluebox806.onmicrosoft.com
69.42.7.98
Concord, CA, US
4:40:26 PM PDT
March 19, 2018

Approve
Deny

Admin Panel
bedrock

Approve
Deny
Your System
mac-daddy.local

- macOS is up to date
- System password is set
- FileVault is enabled
- Firewall is enabled

Login secured by Duo
## Wired for Zero Trust

<table>
<thead>
<tr>
<th>Microsoft</th>
<th>VPNs</th>
<th>Cloud Apps</th>
<th>On-Premises</th>
<th>Identity</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office 365</td>
<td>Juniper Networks</td>
<td>Salesforce</td>
<td>Epic</td>
<td>Windows Active Directory</td>
<td>REST APIs</td>
</tr>
<tr>
<td>Outlook</td>
<td>Cisco</td>
<td>Google Apps</td>
<td>PeopleSoft</td>
<td>Active Directory Federation Services</td>
<td>WEB SDK</td>
</tr>
<tr>
<td>Remote Desktop Services</td>
<td>Citrix</td>
<td>Amazon Web Services</td>
<td>VMware Horizon View</td>
<td>Okta</td>
<td>RADIUS</td>
</tr>
<tr>
<td>Windows Server</td>
<td>Palo Alto Networks</td>
<td>Box</td>
<td>Unix</td>
<td>PingIdentity</td>
<td>SAML</td>
</tr>
<tr>
<td>RRAS</td>
<td>Pulse Secure</td>
<td>Dropbox</td>
<td>Shibboleth</td>
<td>OneLogin</td>
<td>OIDC</td>
</tr>
</tbody>
</table>

Integration documents are available at [duo.com/docs](http://duo.com/docs)
Our Vision: **Passwordless Authentication**

User to Device ➔ To Every Application

![Platform Logos](apple, facebook, google) ➔ ![Duo Security Platform](logo)
WebAuthn
A better alternative for securing our sensitive information online

Suby Raman
Suby is a software engineer at Duo Security, working on the team responsible for Duo’s Authentication Prompt. He has helped drive Web Authentication development at Duo.

Notably, he has contributed over 175 custom emoji to Duo’s Slack workspace.

@subyraman

Nick Steele
Nick Steele is an R&D engineer with Duo Labs and a W3C Invited Expert for the WebAuthn standard.

While his focus lies in user authentication and authorization, he also has strong opinions about sci-fi and ramen.

@codekaju

webauthn.guide / webauthn.io
Trust Engine

https://duo.com/labs

https://twitter.com/duo_labs
What is BeyondCorp?

- 2014 - Google BeyondCorp paper
- 2016 - Google BeyondCorp progress update
- 2017 - BeyondCorp migration, user experience and lessons learned

BeyondCorp
A New Approach to Enterprise Security

Rory Ward is a site reliability engineering manager in Google Ireland. He previously worked in Ireland at Valsala, in Silicon Valley at ACI, Netscape, KIVA, and General Magic, and in Los Angeles at Retre. He has a BSc in computer applications from Dublin City University.

Betsy Beyer is a technical writer specializing in virtualization software for Google SRE in NYC. She has previously provided documentation for Google Data Center and Hardware Operations teams. Before moving to New York, Betsy was a lecturer in technical writing at Stanford University. She holds degrees from Stanford and Tulane.

Virtually every company today uses firewalls to enforce perimeter security. However, this security model is problematic because, when that perimeter is breached, an attacker has relatively easy access to a company’s privileged intranet. As companies adopt mobile and cloud technologies, the perimeter is becoming increasingly difficult to enforce. Google is taking a different approach to network security. We are removing the requirement for a privileged intranet and moving our corporate applications to the Internet.

Since the early days of IT infrastructure, enterprises have used perimeter security to protect and gain access to internal resources. The perimeter security model is often compared to a medieval castle: a fortress with thick walls, surrounded by a moat, with a heavily guarded single point of entry and exit. Anything located outside the wall is considered dangerous, while anything located inside the wall is trusted. Anyone who makes it past the drawbridge has ready access to the resources of the castle.

The perimeter security model works well enough when all employees work exclusively in buildings owned by an enterprise. However, with the advent of a mobile workforce, the surge in the variety of devices used by this workforce, and the growing use of cloud-based services, additional attack vectors have emerged that are stretching the traditional paradigm to the point of redundancy. Key assumptions of this model no longer hold. The perimeter is no longer just the physical location of the enterprise, and what lies inside the perimeter is no longer a blessed and safe place to host personal computing devices and enterprise applications.
Google BeyondCorp: Zero-Trust at Work
Google hasn’t suffered an employee phishing compromise in over a year

24 JUL 2018

Google, Phishing, Security threats

Get the latest security news in your inbox.

you@example.com  Subscribe