DATA CONFIDENTIALITY: IDENTIFYING AND PROTECTING ASSETS AND DATA AGAINST DATA BREACHES

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of identifying and protecting information from threats to data confidentiality. This endeavor is being undertaken through collaboration with industry and the information technology (IT) community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the *Data Confidentiality: Identifying and Protecting Assets and Data Against Data Breaches* project, including background, challenges, goals, and potential benefits. If you would like to propose another architecture or know of products that might be applicable to the challenge, please contact us at ds-nccoe@nist.gov.

CHALLENGE

An organization's data is one of its most valuable assets and must be protected from unauthorized access and disclosure. Large and small data breaches threaten the function and survival of an organization when operational, financial, employee, and customer data are compromised. This can undermine the organization's work and success and lead to severe reputational damage.

GOAL

The goal of this project is to provide a practical solution to identify and protect the confidentiality of an enterprise's data. This project will also provide guidance on data confidentiality that parallels the *Detect, Respond to, and Recover from Data Breaches* Project. The NCCoE chose to address data confidentiality in two parallel projects to provide modular, adaptable guidance rather than an all-or-nothing approach.

BACKGROUND

The first group of data security projects at the NCCoE focused on data integrity (DI). The NIST Special Publications covered the ability to protect DI, detect and respond to attacks that impact DI, and recover DI after an attack. During presentations, demonstrations, Community of Interest calls, and other feedback mechanisms, many questions were raised related to data breaches and inclusion of technologies to prevent such attacks. While this was previously out of scope, the new data confidentiality projects seek to address this need.

BENEFITS

This project will answer specific questions pertaining to identifying and protecting data from data confidentiality attacks, such as:

- What data is present within an enterprise?
- What protections can be applied to the data?
- How should the data be accessed?
- What user types are defined by the organization?
- What controls should be applied to each user type's access?

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 challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

For more information about this project, visit: https://www.nccoe.nist.gov/projects/building-blocks/data-security/dc-detect-identify-protect

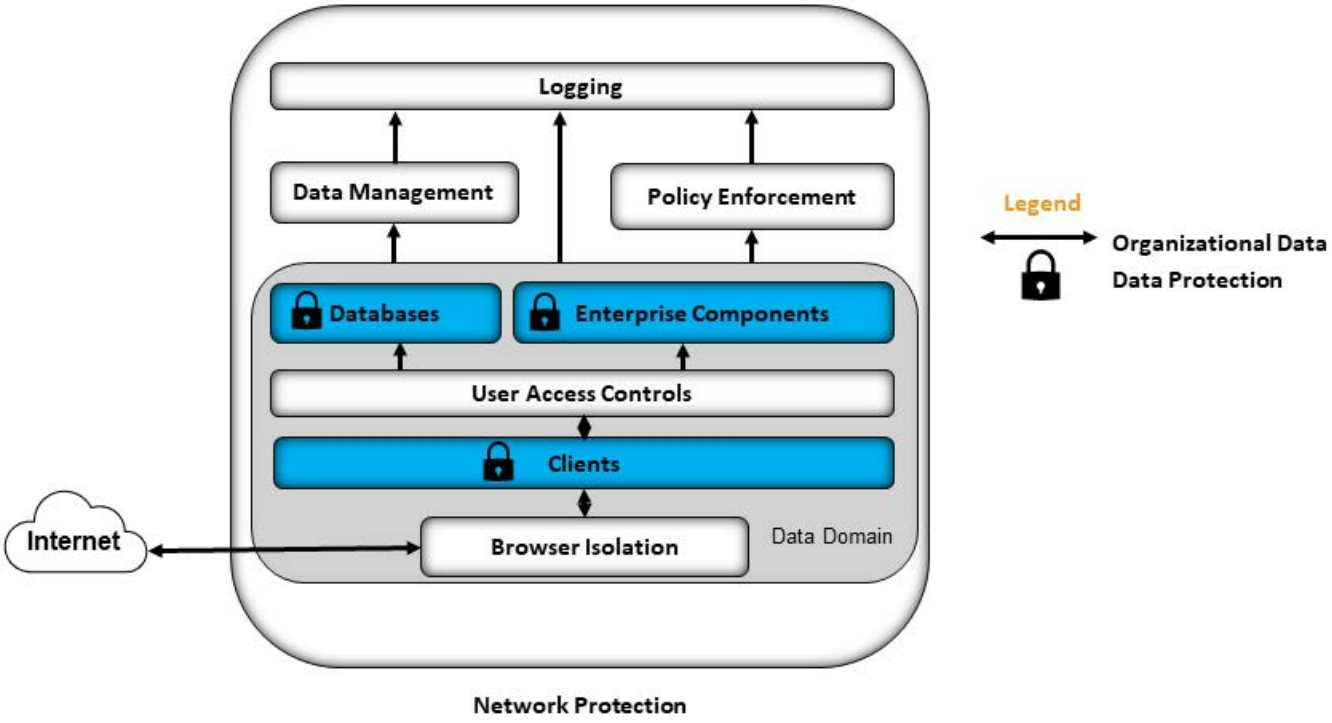
CONTACT US

nccoe@nist.gov
301-975-0200

This project will demonstrate:

- a data management solution that identifies and inventories data
- a solution that provides user access control mechanisms
- a policy enforcement solution that manages users and user access controls
- an audit log solution that baselines normal behavior for data access activity
- a file-level encryption scheme that protects data
- a system-level encryption scheme that provides physical access protection
- network measures to provide protection for data in transit

HIGH-LEVEL ARCHITECTURE



COMPONENT LIST

Solutions for this project include:

- log collection, collation, and correlation
- network protection solution
  - network mapping
  - network segmentation
  - network protection
- user access controls
- data management
  - data inventory
  - data discovery
- data protection
  - protection at rest
    - including file- and system-level encryption
  - protection in transit
  - protection in use
- protection against the use of removable media
- policy enforcement

COLLABORATORS

AVRIO SOFTWARE, CISCO, DISPEL, FIREEYE, GreenTec™ www.GreenTec-USA.com, PKWARE, STRONGKEY, Symantec. A Division of Broadcom

DOWNLOAD THE PROJECT DESCRIPTION

For more information about data security projects, please read the project descriptions at: https://www.nccoe.nist.gov/projects/building-blocks/data-security

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you are interested in contributing technology or expertise to this project, please email ds-nccoe@nist.gov.