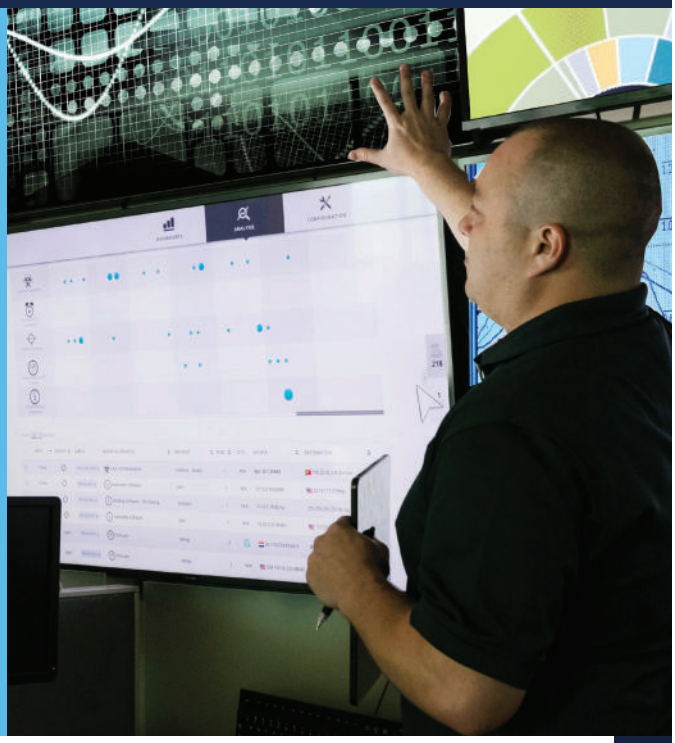
DATAPRISE DATA SHEET

Dataprise Security Gap Assessment

To keep your organization's security posture hardened and risk exposure minimal, your organization needs visibility into the current state of your cybersecurity posture.

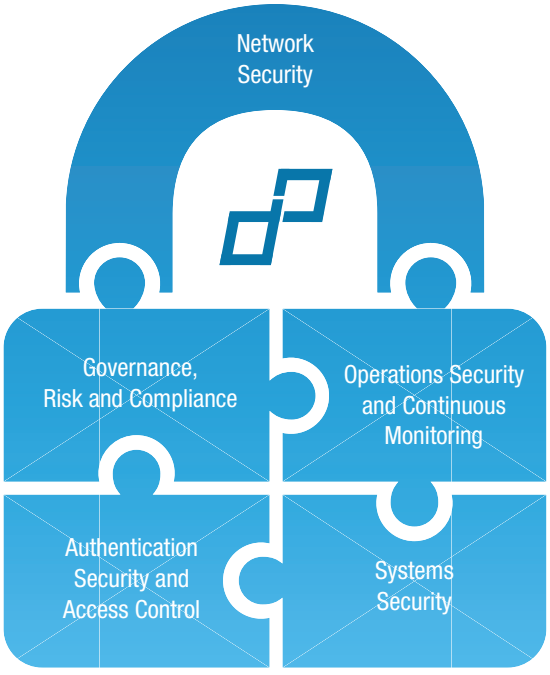
No matter what the current security maturity level is for your organization, our Security Gap Assessment provides you with a baseline and a customized strategic roadmapof short-and long-term milestones, as well as a plan of action to achieve your security goals.



Our Security Gap Assessment:

- Provides an initial baseline of your cybersecurity posture tailored to your business requirements and objectives
- Evaluates the susceptibility of core infrastructure to external access or disruption
- Reviews your environment and management, and analyzes how they stack up to your given industry and best practices
- Includes a Personally Identifiable Information (PII) scan
- Verifies if controls are in place to minimize risk and exposure
- Provides numerical security maturity scores - Current State, Quick Win State, Target State - and prioritized recommendations to focus on actions with immediate and high-value payoff

Areas Assessed:



DATAPRISE DATA SHEET

Security Gap Assessment Framework

Dataprise has a proven Security Gap Assessment framework that is executed by our highly-trained vCISO consulting team.

STEP 1

Conduct Stakeholder Interview and Gather Information

- Define business needs and compliance requirements
- Discuss business risk tolerance
- Discuss existing disaster recovery and business continuity plan
- Discuss security culture and existing security policies and procedures

STEP 2

Discover Network Security

- Gather existing network documentation and analyze for in-place boundary defense layers
- Run scans and review security configurations across the organization's LAN
- Analyze documentation for in-place boundary defense layers
- Review use of wireless access and the configured controls

STEP 3

Conduct Security Scans

- Identify all network resources accessible from outside the network
- Conduct a personally identifiable information (PII) scan
- Perform vulnerability and network scans
- Perform a Security Configuration Hardening Baseline scan
- Perform an internal software security patch audit

STEP 4

Discover Systems Security

- Perform audit of email system protection and internet browser security controls
- Verify inventory control of authorized and unauthorized devices and software
- Discover controlled access and use of administrative privileges
- Verify overall application security controls (e.g., firewall, antivirus, authentication)

STEP 5

Discover Authentication Security and Access Control

- Review existing data classification scheme standards and policies and implemented procedures and controls for accessing key business data points
- Review internal and external access control of Customer's data/information
- Audit Active Directory and the administrative privileges
- Review existing Data Loss Prevention (DLP) solution

STEP 6

Analyze Security Posture

- Identify Customer's Current State as related to the security maturity
- Establish a Target State maturity score based on the Customer's industry, organization size, compliance requirements, and risk profile
- Identify gaps that exists in the environment
- Create key recommendations for improving network design, security, and overall IT posture
- Identify Quick Win recommendations
- Develop a phased roadmap Action Items to Mitigate (AIM) for the Quick Win State and Target State

STEP 7

DEVELOP AND DELIVER SECURITY GAP ASSESSMENT REPORT