eBook

Forcepoint

Zero Trust in Multi-level Network Environments

Strategies for Achieving Rapid and Secure Innovation

Table of Contents

The Challenge: A New Cybersecurity Mandate

The recent Executive Order on Improving the Nation's Cybersecurity aims to modernize cybersecurity and better protect federal networks. Among its directives for government organizations are cybersecurity best practices, including a Zero Trust security model. But in achieving that goal, your organization faces significant challenges:

Information sharing

Zero Trust guidelines advocate for cooperation among functional areas in both civilian and military organizations. The need for information sharing is noted in Zero Trust guidance from the National Institute of Standards and Technology (NIST) and Department of Defense (DoD). But many organizations take a siloed approach to cybersecurity.

Assessment

An early step toward Zero Trust is assessment of data resources and the policies and processes to protect them. This requirement is specified in NIST Special Publication (SP) 800-207 "Zero Trust Architecture" and the DoD "Zero Trust Reference Architecture." However, few organizations fully understand their cybersecurity posture.

Multi-level networks

These challenges are compounded by the need to manage multi-level networks of unclassified and classified information. Different users have different views of data resources. A single user might appear as multiple entities across various devices and network levels. As a result, organizations struggle to mitigate cyber-risk across their domains.

Best Practices for Achieving Zero Trust

Embrace a Zero Trust mindset

Zero Trust requires a new approach to cybersecurity. It replaces implicit assumptions about who is trusted with explicit decisions made every time a user or system attempts to access sensitive data.

NIST and the DoD offer robust Zero Trust architectures, so there's no need to create a new framework from scratch—or submit to vendors who impose their own. But zero trust does require a new way of thinking. Embrace the NIST and DoD frameworks. Collaborate with other government organizations to improve security. Recognize that cybersecurity risk is present in your networks—and that you need to take action now to mitigate that risk.

Map security requirements to NIST and DoD frameworks

"Zero Trust" isn't a single security solution you can buy. Rather, it's a security model enabled by a set of technologies and capabilities.

The DoD Zero Trust framework includes a maturity model that you can use to assess your existing security posture and establish a baseline of capabilities. You can then measure your progress against the framework's intermediate and advanced levels of data protection.

The DoD architecture also specifies seven Zero Trust pillars that cover users, devices, networks, applications, data, analytics, and automation. By mapping your security capabilities and gaps to these pillars, you can document the security solutions you already have and identify what you need to augment. Are you taking full advantage of existing security investments? Have you overlooked crucial elements of achieving zero trust?

Create risk scores for user behavior

A key capability of zero trust is assessing the trustworthiness of users accessing your systems and data. To achieve that goal, you first must be able to confirm user identities across networks.

Leverage user-behavior monitoring and behavioral analytics to create a risk score for every user. An effective solution combines your organization's policies with business rules to establish baselines of normal behavior for every user. It then automatically detects anomalous patterns to expose risky behavior and escalate relevant cases. Your security team can focus on actual threats, without wasting time on false positives —or slowing the productivity of legitimate users.

Automate data protections

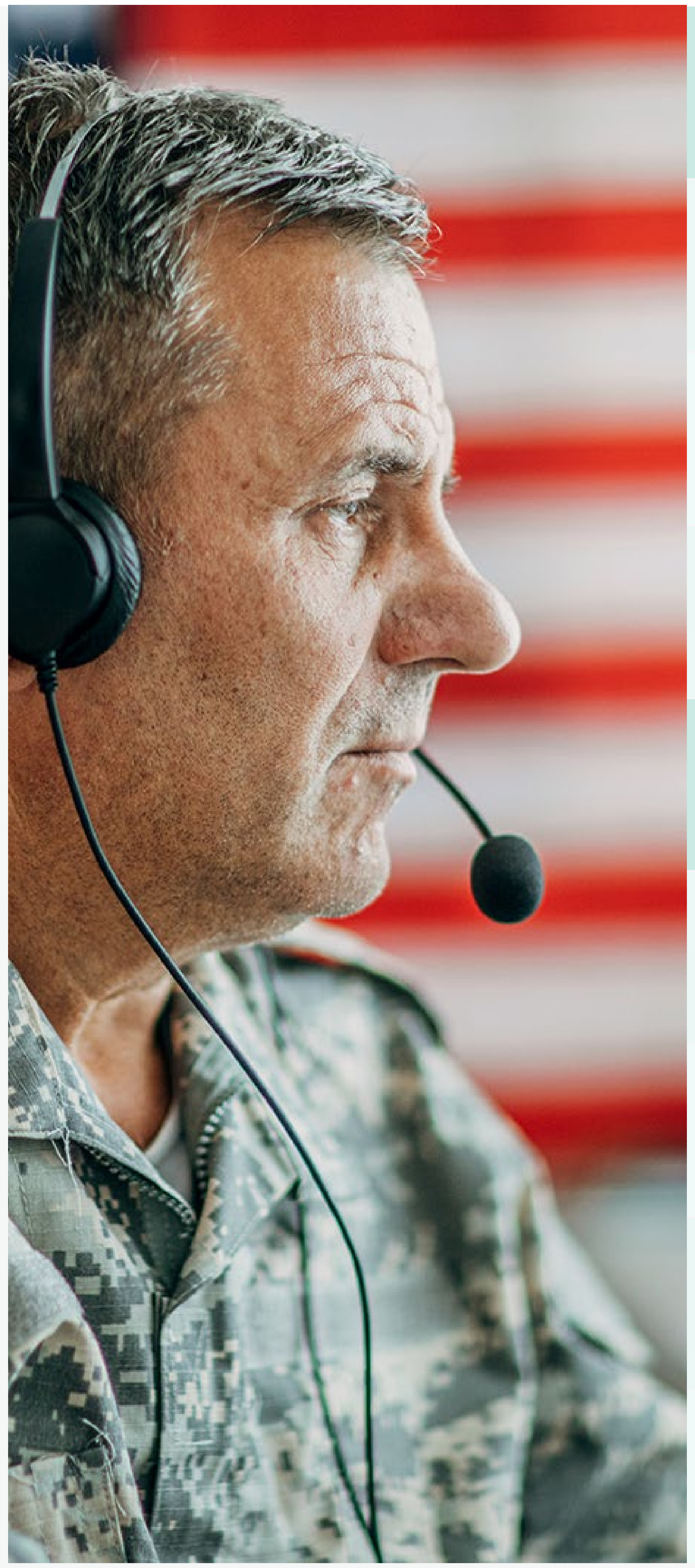
Fundamentally, zero trust is about protecting sensitive data. You need solutions to properly assess and classify data, enforce policies and processes for protecting that data, and ensure device security—at scale and at cloud speeds.

While your organization may have policies for classifying data, users don't always classify it properly, store it in the right location or share it safely. And that's to say nothing of malicious actors—both internal and external—who try to circumvent protections and exfiltrate information. So you need tools to make sure your policies are enforced, your devices are protected and your data remains safeguarded. Automated processes and advanced technologies like machine learning are essential.

Enable data access from anywhere, on any device

The ultimate goal of zero trust is not only to protect data but also to support your mission, so you need cross-domain security that enables safe, adaptive access to all data and applications on your multi-level networks.

The capability to enable authorized users to leverage a single device to safely access all your networks from any policy-permitted location is key. It can help optimize productivity, fuel research and innovation, and advance your mission. You save the cost and time of managing large numbers of devices while empowering your people to do their jobs how and where they need to—all while maintaining Zero Trust cybersecurity.



Need to know

- → A new executive order calls for organizations to implement Zero Trust cybersecurity.
- → NIST and the DoD offer guidelines for a Zero Trust architecture, but real-world progress is challenging.
- → Best practices and solutions can equip you to achieve zero trust in a multi-level network environment.

Benefits of effective zero trust

- → Comply with government cybersecurity mandates.
- → Safeguard data across all your domains, enclaves, and multi-level networks.
- → Prevent data exfiltration, system shutdowns, operational disruptions, and the costs of remediation.
- → Empower your people to advance your mission—while protecting vital information and systems.

Solutions for a Zero Trust Architecture

Forcepoint offers a complete portfolio that maps directly to the capabilities required to achieve zero trust. Key cybersecurity solutions for government include:

Forcepoint Behavioral Analytics

Combines visibility, analytics, and automated control to detect and block anomalous user activity before it becomes a breach.

Forcepoint User Activity Monitoring

Proactively detects high-risk behaviors and compromised access.

Forcepoint Insider Threat Solutions

Monitors, analyzes, and mitigates high-risk user behavior.

Forcepoint Data Analyzer

Employs virtual data warehousing, federated search, and algorithms for automated information discovery to respond to cyber-threats as they're happening.

Forcepoint Data Loss Prevention

Protects sensitive information, simplifies compliance with predefined policies, and automatically prevents data breaches.

Forcepoint Cross-Domain Solutions

Provides secure, automated, and scalable transfer of data across multi-level networks.

Forcepoint Trusted Thin Client

Empowers authorized developers to securely access unclassified and classified networks through a single pane of glass.

The Forcepoint Advantage

→ One of the largest private cybersecurity providers, serving thousands of government and enterprise clients.

→ More than 20 years of expertise supporting organizations that protect national security.

→ A uniquely comprehensive portfolio of cybersecurity solutions to enable the most secure and complex missions.

Next Steps on Achieving Zero Trust in Your Multi-level Environment

→ Read our informative blog, **"Zero Trust: A Smarter Approach to Security."**

→ Watch our insightful webinar, **"A Modern Approach to Zero Trust."**

→ Download our deep-dive whitepaper, **"Implementing Zero Trust: A Forcepoint Guide for Agencies."**

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

[Zero Trust in Multi-level Network Environments eBook] 22Jul2021