proofpoint.

SOLUTION BRIEF

Enabling an Evergreen Zero-Trust Environment

Simplify how your agency protects people and defends data while adopting a zero-trust maturity model

Products

- Proofpoint Email Threat Protection platform
- Proofpoint Identity Threat Protection platform
- Proofpoint Threat Response
- Proofpoint Insider Threat Management
- Proofpoint Security Awareness
- Proofpoint Archive
- Proofpoint Emerging Threats Intelligence
- Proofpoint Threat Intelligence Services

Key Benefits

- Unmatched visibility into your people and identity threats
- Threat intelligence and protection for email, the No. 1 threat vector
- Flexible government deployments on-premises, virtually on-premises and in our FedRamp cloud environments

Federal agencies face many challenges as they transition to a zero-trust security architecture. Zero-trust principles might not be familiar, for example, especially to those who are making the move for the first time. Setting up a proper system and adhering to a host of confusing requirements and deadlines can also be quite daunting. And embracing zero trust may even require a fundamental shift in an agency's cybersecurity philosophy and culture. This solution brief provides an overview of the zero-trust approach, especially as it relates to federal agencies. It also describes the Proofpoint solutions that can simplify the process of adopting a zero-trust model.

Zero-Trust Overview

Zero trust includes concepts, ideas and principles that assume that no one can be fully trusted. This includes even those who are already part of an organization. The approach involves the premise of least privilege, which holds that every person, process and program in a computing environment should have access only to the data or resources that they need to accomplish their legitimate tasks—nothing more.

But adopting zero-trust is just the first step. True zero-trust is an evergreen process. Maintenance of the system must be constant. And the system must provide continuous visibility into security controls. The architecture also must allow for updates of these controls over time, based on the dynamic nature of an environment and the people who access its data.

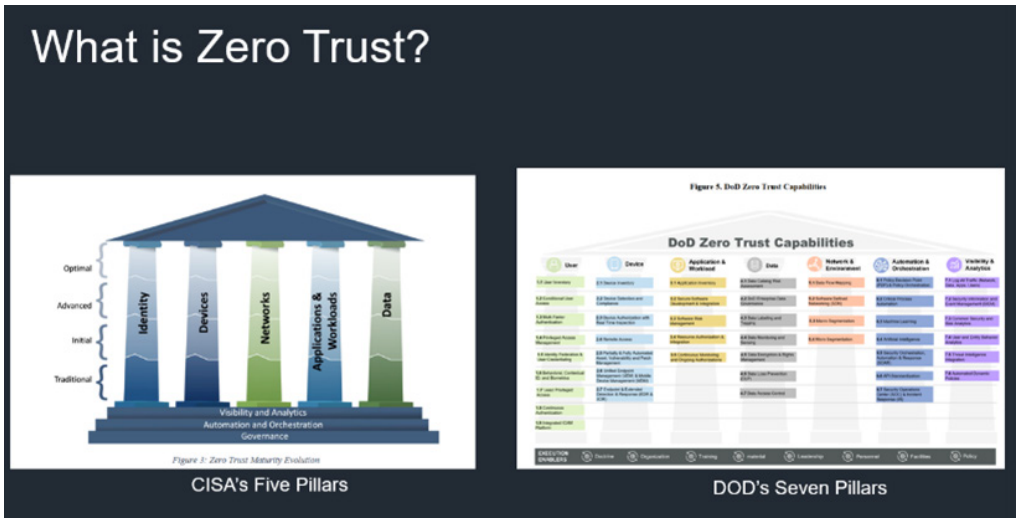

Figure 1: Zero-trust pillars for CISA and the DoD

Zero-Trust Maturity Models for Federal Agencies

There is no one-size-fits-all way to adopt a zero-trust architecture. But aligning defenses and controls around a zero-trust maturity model is the best starting point. A maturity model is a roadmap for developing and implementing zero-trust strategies. Two zero-trust maturity models are designed for federal agencies. One is from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the other is from the U.S. Department of Defense (DoD).

CISA Zero Trust Maturity Model

The CISA Zero Trust Maturity Model serves as a guide mainly for federal civilian agencies. It outlines 37 distinct capabilities organized into five pillars. These pillars include:

- Identity
- Devices
- Networks
- Applications and workloads
- Data

DoD Zero Trust Maturity Model

The DoD Zero Trust Maturity model is mainly for the military and agencies that are responsible for national security. The DoD's approach is distinct from that of CISA, as security and military mission requirements can be quite different from those of civilian agencies. The DoD model includes 45 capabilities that are organized around the following seven pillars:

- Users
- Devices
- Networks and environments
- Applications and workloads
- Data
- Visibility and analytics
- Automation and orchestration

Timelines and Expectations

The White House Office of Management and Budget has set a **deadline** of Sept. 30, 2024, for most federal civilian agencies to adopt some level of zero-trust architecture. For the DoD, component-level execution plans that lay out how zero trust is applied across their networks, including all infrastructure and systems, were due in September 2023. The DoD expects all of its components to achieve target-level goals by fiscal year 2027.

These frameworks, however, serve only as starting-point guidance for agencies and partners. The hard part lies in translating these frameworks into practical adoption plans for each group.

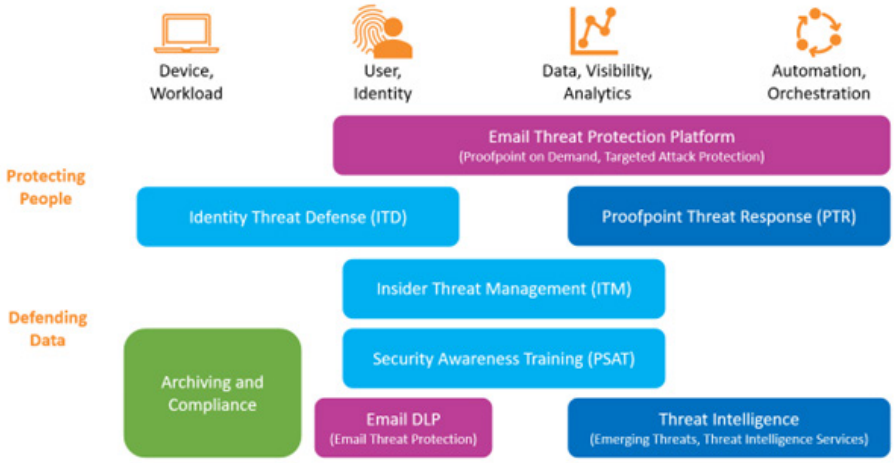

Figure 2: Proofpoint solutions that protect people and defend data.

Proofpoint Zero-Trust Alignment

Proofpoint has been the leader of the email security market for more than 20 years. We have a solid record of protecting agencies and their people from initial compromise. Our approach breaks every step of the attack chain to protect people and defend data. We provide visibility and protection in the middle stages of the attack chain. And we defend against persistence, privilege escalation and lateral movement. We also cover the end stages of the attack chain to prevent impact from a data-loss event. Our solutions meet all five pillars of the CISA framework requirements. They also meet all but the networks pillar of the DoD framework requirements.

Proofpoint Zero-Trust Solutions

The following table outlines Proofpoint offerings that help federal agencies with their zero-trust systems.

SOLUTION	DESCRIPTION	DOD ZERO-TRUST PILLAR ALIGNMENT
Proofpoint Email Threat Protection	The Proofpoint Email Threat Protection platform provides unmatched visibility as well as email threat detection and remediation. It protects against initial compromise attacks and data-loss incidents around email.	• Applications and workloads • Automation and Orchestration, • Visibility and analytics
Proofpoint Identity Threat Defense	The Proofpoint Identity Threat Defense platform provides end-to-end protection against identity threats. It employs agentless deception-based detections. These allow you to discover, prioritize and remediate vulnerable identities and they help you detect and respond to active threats.	• Users • Devices • Applications and workloads • Visibility and analytics

SOLUTION	DESCRIPTION	DOD ZERO-TRUST PILLAR ALIGNMENT
Proofpoint Threat Response	Proofpoint Threat Response recalls malicious emails that have already been delivered to user inboxes. It follows the path of these emails so it can find and retract messages sent to larger groups of recipients. It generates reports of quarantine attempts, successes and failures and lists of users who are targeted the most. It also confirms malware infections, checks for evidence of past infections and enriches security alerts by automatically adding internal and external context and intelligence. Proofpoint Threat Response can be deployed virtually, on-premises or as a cloud solution. It takes the manual labor and guesswork out of incident response. This reduces the workload of your security teams by helping them resolve threats faster and more efficiently.	• Applications and workloads • Automation and Orchestration, • Visibility and analytics
Proofpoint Insider Threat Management	Proofpoint Insider Threat Management (ITM) is the leading people-centric ITM solution. It protects against data loss and brand damage involving insiders who act maliciously, negligently or unknowingly. Proofpoint ITM correlates activity and data movement. It empowers security teams to identify user risk, detect insider-led data breaches and accelerate security incident response	• Data • Visibility and analytics
Proofpoint Security Awareness	Proofpoint Security Awareness tackles one of the most pressing concerns of every organization: reducing the security risk posed by your people. Our threat-driven approach to training makes users resilient. It also empowers security admins with operational efficiency. And it gives them the ability to scale globally.	• Visibility and analytics
Proofpoint Archive	Proofpoint Archive is a FedRAMP Moderate-authorized, cloud-based email archiving solution. It provides a central, searchable repository to help you simplify legal discovery, respond to Freedom of Information Act (FOIA) requests and implement email-records management according to guidance from the National Archives and Records Administration (NARA) Capstone. With Proofpoint Archive, you know where your data is stored. And you can quickly collect, search and retrieve it on demand. Your data is protected in transit from your data source as well as while under management within our cloud infrastructure. It is secure with SSAE- 16 Type 2 certification for its fully managed service as well as the Proofpoint facilities that host the service.	• Devices • Applications and workloads • Visibility and analytics

Proofpoint Threat Intelligence Solutions

Our threat intelligence solutions support automation of cyberthreats. They provide unmatched analysis into the email and network threat landscape. To learn more about Proofpoint's threat intel capabilities, visit **Threat Intelligence Services** and **ET Intelligence**).

SOLUTION	DESCRIPTION	DOD ZERO-TRUST PILLAR ALIGNMENT
Emerging Threats Intelligence	Emerging Threats Intelligence is the gold standard for threat researchers. It offers 100% verified threat intelligence from one of the world's largest malware exchanges. It integrates seamlessly with your security tools. And it helps you understand the deeper historical context of the origins and authors of threats. Unlike other intelligence sources that report only domains or IP addresses, our intel includes a 10-year history and proof of conviction. It covers more than 40 threat categories and related IPs, domains and samples. It helps you with threat discovery, security enforcement and incident response as well as enriches other solutions. It combines actionable information, such as up-to-the-minute IP and domain reputation feeds, with a database of globally observed threats and malware analysis.	• Visibility and analytics
Proofpoint Threat Intelligence Services	Proofpoint Threat Intelligence Services provide you with a deep situational understanding of the threat landscape and your organization's place in it. This can help you better prioritize your security decisions. Threat Intelligence Services offer: • Direct access to our industry-leading U.S. threat researchers for RFIs • Monthly custom threat reports • Advanced warning for emerging threats through access to our analyst logbooks • The services can help you retain hard-to-find security analyst staff by reducing the number of manual processes and allowing them to focus on the most critical issues. Our researchers have more than a combined 100 years of experience within federal agencies like the National Security Agency, the U.S. Cyber Command and service branches.	• Visibility and analytics

Click **here** to learn more about Proofpoint's federal solutions and reach out to Proofpoint's Federal team.

LEARN MORE

For more information, visit **proofpoint.com**.