MANDIANT

WHITE PAPER

ZERO TRUST FOR FEDERAL GOVERNMENT: A GUIDE TO ACHIEVING IMPROVED CYBER SECURITY

Introduction

The recent SolarWinds and Colonial Pipeline zero day incidents—uncovered by Mandiant—demonstrate the sophistication of today's cyber attacks.

The escalation of security incidents like these underpin the Biden Administration's recent Executive Order (EO),[1] which aims to modernize U.S. Government cyber security defenses. The Executive Order seeks to:

- Remove barriers to threat information sharing between government and the private sector
- Modernize and implement stronger cyber security standards in the Federal Government
- Improve software supply chain security
- Establish a cyber security safety review board
- Create a standard playbook for responding to cyber incidents
- Improve detection of cyber security incidents on Federal Government networks
- Improve investigative and remediation capabilities

Not only does the EO ask agencies to address these existing vulnerabilities, the Office of Management and Budget (OMB) is trying to mandate action. In January 2022 the OMB released Memo 22-09. M-22-09 provides specific goals and deadlines for implementing the zero trust goals outlined in the March EO. The goals are organized using the zero trust maturity model developed by the Cyber Security and Infrastructure Security Agency (CISA). The OMB is requiring agencies to achieve specific zero trust security goals by the end of Fiscal Year (FY) 2024.

Agencies will be challenged to meet that deadline. Today's security teams are also grappling with the increase of unmanaged devices outside the traditional purview of IT system security. The prevalence of user and machine devices, from smartphones and laptops to wearables and Internet of Things (IoT) sensors, has complicated management and security.

These factors require an overarching cyber security strategy and zero trust provides the underlying fabric. By adding layers of continuous security validation, detection and response and automation to threat intelligence, federal agencies can ensure a modern approach that efficiently and effectively addresses the cyber attack landscape and meets the mission of the cyber security Executive Order.

[1] FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cyber security and Protect Federal Government Networks.

What is Zero Trust?

Zero trust has gained rapid acceptance during the coronavirus pandemic because it is built on the principle of "never trust, always verify." This concept of least privilege access became crucial amid widely distributed workforces resulting in remote connectivity where individuals logged into agency and corporate networks from all manner of devices and public Internet connections.

Zero trust doesn't occur overnight. The path to maturity includes the implementation and integration of multiple technologies and capabilities. To simplify the journey, Mandiant recommends starting with these four actions:

- **Verify the identity:** An individual application, user or machine accessing a system must be validated to confirm that they are who they say they are. Automated policies should address access permissions, and those policies should be adaptive and dynamic to respond across different applications, clouds and on-premises systems.
- **Verify the device:** Users may use multiple devices— laptops, smartphones and desktops—to access organizational systems. Verification must be extended across all of these devices so that the asset is validated every time they connect.
- **Limit access and privilege:** Cyber criminals are typically attracted to personnel with administrative privileges to gain control over a business system. This makes it important to limit lateral movement. The principle of least privilege must be considered thoroughly in all cases, ensuring users only have enough access to successfully do their jobs.
- **Learn and adapt:** Information about the user, including their workstation, application use and server policies, should be collected and analyzed. Machine learning can help continuously improve this process, allowing security teams to recognize unusual behaviors, determine risk levels and decide whether risks are acceptable. Accuracy and availability of data—logging, log feeds, depth of content—is crucial.

All these actions can be addressed with a zero trust architecture (ZTA). As defined by the Executive Order, ZTA is a security model—a set of system design principles and a coordinated cyber security and system management strategy—and not just a single product or service offering.

At a high-level, the ZTA has a control plane and a data plane (Fig. 1). The control plane components authorize access to assets or resources. Actual transfer of information occurs in the data plane. Access to system resources is implemented by a policy enforcement point (PEP) in the data plane, which acts like a gatekeeper. It operates in consultation with policy engine and policy administration functions, and together these form the policy decision point (PDP). The PDP forms the control plane of a ZTA, which in turn is continually updated by inputs from the various control functions.

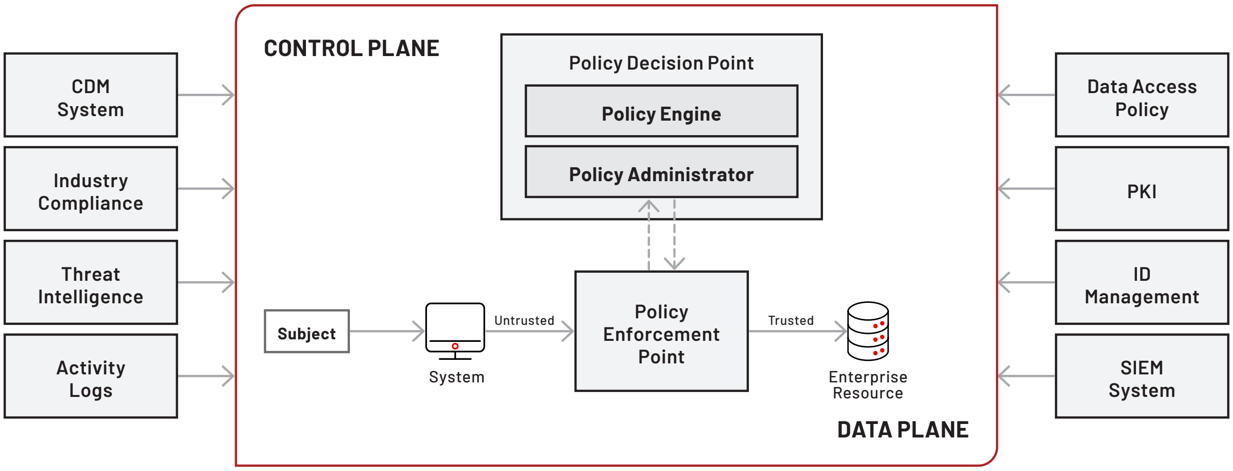

FIGURE 1. Example zero trust architecture.

Mandiant Approach To Zero Trust: Enhancement Through Intelligence

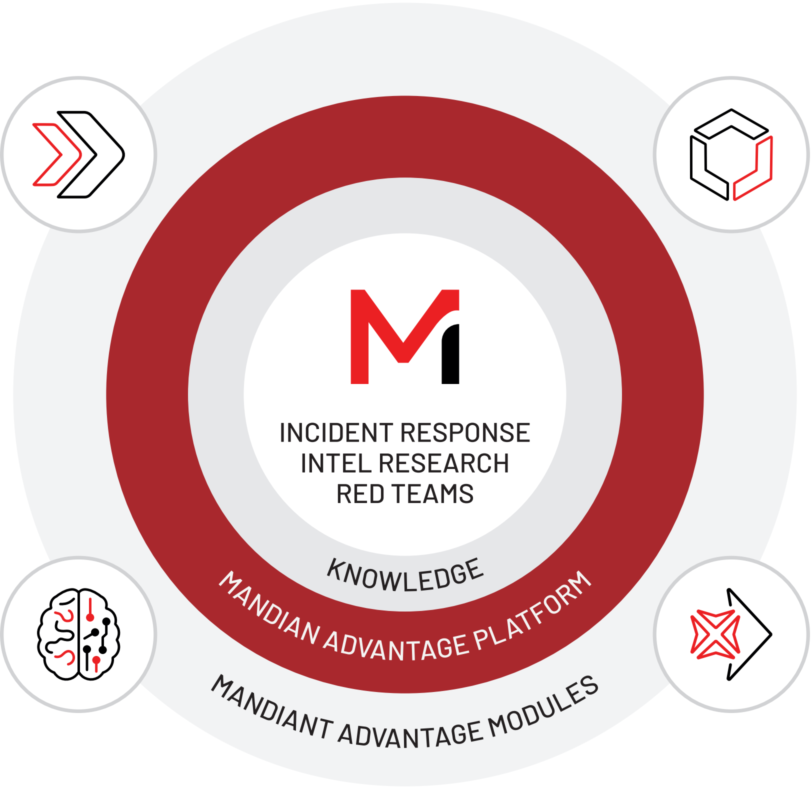

FIGURE 2. Mandiant Advantage.

Zero trust may seem daunting -but Mandiant is on a mission to make every organization secure from cyber threats and more confident in their overall readiness.

Effective security is not based on the security controls deployed, but the expertise and intelligence behind them. Mandiant takes an intelligence-led, multi-vendor approach to XDR, through the Mandiant Advantage platform.

Mandiant Advantage gives security teams an early knowledge advantage via the Mandiant Intel Grid, along with modules that offer current and relevant threat data and analysis expertise. Armed with continuous security validation, detection and response, organizations are more secure and better able to meet compliance deadlines.

The intelligent, data-centric Mandiant approach to ZTA helps ensure that federal agencies are better equipped to not only address the Executive Order, but also protect data in real time.

As they modernize and implement stronger cyber security standards to meet Executive Order goals, agencies can ease their zero trust journey by embedding technologies such as threat intelligence and automation.

Threat intelligence is critical in developing and maintaining a ZTA. It supports investigations into discovered software flaws, newly identified malware and attacks against external assets that may impact internal assets.

Mandiant Advantage Threat Intelligence can be seamlessly integrated into a ZTA. It provides:

- **ZTA Policy Engine Support:** Intelligence is typically integrated into a ZTA policy engine, which uses a transactional model (similar to financial fraud monitoring) to determine the legitimacy of information accesses and technical transactions. Mandiant Threat Intelligence can provide context and identify risk on IPs used for communications to feed AI supporting the policy engine. When an analyst also trains the model and provides oversight, specific Mandiant Advantage Threat Intelligence indicators or observables can be injected into the policy engine itself to raise or lower the level of risk associated with any transaction.
- **Mandiant Advantage Threat Intelligence Integration:** Mandiant Advantage Threat Intelligence APIs allow ingestion of IOCs, observables, and vulnerabilities into detection and threat management tools to surface priority alerts automatically and create attack mitigation playbooks. The API enables access to the most recent and updated intelligence and observables to help automate monitoring of nefarious activity, validating alerts, confirming forensic analysis, creating proactive detections and investigating tippers.
- **Vulnerability Intelligence:** Vulnerability intelligence helps prioritize known technology vulnerabilities to minimize risks and mitigate efforts against prevalent attack methods. This intelligence gives organizations information on which existing vulnerabilities are currently being leveraged and exploited by threat actors.
- **Threat Actor Intelligence:** Threat actor intelligence helps put proper controls and detections in place to establish a threat profile and mitigate against known actors and their behaviors. This intelligence gives organizations information on ongoing attack campaigns as well as the tactics, techniques and procedures (TTPs) used by actors to preempt security measures against future attacks. Actor TTPs may include the use of existing vulnerabilities and malicious code in addition to undiscovered bugs that enable zero-day attacks.
- **Limit unnecessary open ports and services:** Physical, OT and infrastructure intelligence is required to inform decision-making regarding system configuration checks on resources and systems to improve cyber hygiene. Threat intelligence is needed to develop an overall strategy for systems configuration maintenance and information architecture. It also helps to determine what mitigations and controls are needed to protect resources and systems from both internal and external threats.
- **Credential or Intellectual Property Leaks:** Loss of user credentials and intellectual property (IP) for any reason continues to be a major risk. Searching through various aggregation sites and forums for potential credentials and IP leak can help identify whether data loss has occurred. These searches and alerts should include keywords that can identify credentials associated with all users' accounts, including personal accounts, as well as content searches for IP, keywords or codenames.
- **Brand Monitoring:** Social media, deep or dark-web research enables the discovery of imminent threats beyond the traditional perimeter. Based on the keywords, alerts can be generated if organizational confidential data or identities have been discovered.

All these capabilities support the cyber security Executive Order's objectives to improve detection of cyber incidents on Federal Government networks and modernize and implement stronger cyber security standards in the federal government.

Improved Investigation and Remediation with the Mandiant Approach

Mandiant also helps federal agencies address the Executive Order's goals of creating standardized responses to cyber incidents and improving investigative and remediation capabilities. The Mandiant Advantage is a multi-vendor XDR platform that delivers Mandiant's transformative expertise and frontline intelligence to security teams of all sizes. It includes:

Threat Intelligence

Security Validation

Automated Defense

Attack Surface Management

Mandiant Advantage Threat Intelligence

Public sector organizations and the industrial base are prime targets for sophisticated threat actors. Such actors pick their targets carefully as they evolve their techniques and tools. For example, in the Solar Winds case, the attackers compromised the supply chain and remained undetected for as long as possible. Not only must organizations be able to recognize threat actors and detect current threat actor activity–they must also be sure that adversary-specific security controls are working as intended.

Mandiant Threat Intelligence enables organizations to more effectively protect against targeted attacks by giving them:

- A holistic profile on threats targeting the organization based on vertical industry, geographic region or deployed technologies
- Insights into the motivations of attackers they are most likely to face
- Details on capabilities and specific indicators that can help rapidly and consistently detect those threat actors within their environment
- The ability to more effectively hunt for threat actor activity within their environments
- Information on industry attack events and trends so they can anticipate attacks

There are many elements—such as processes, software, hardware, skill capabilities—to consider when planning for cyber defense. They can all help agencies understand the current threat environment, successful security technologies, ways to align capabilities with mission requirements and ways to operate at full capability despite personnel shortages.

Mandiant Advantage Security Validation

Before you increase security spend, it's critical to know how well your existing security investments are working. You must be able to accurately and frequently measure the effectiveness of your security controls in place.

Many public sector organizations use Mandiant Advantage Security Validation. It puts your security posture to the test—literally— by tapping into the Mandiant Intel Grid to get the latest threat intelligence on threat actor TTPs and and automates a testing program that gives you real data on how your security controls are performing, so you can optimize your environment and make the right investments in the future. Mandiant Security Validation accurately measures the behavior of security controls when challenged with authentic threat activity.

The solution specifically and continuously monitors the effectiveness of each element of the security stack and how they work together to enable organizations to rapidly identify gaps, redundancies, misconfigurations and broken processes of security controls. Ultimately, with Mandiant Security Validation you can identify where and how attackers can operate unnoticed. Agencies can repeatedly and accurately calculate security effectiveness and gain evidence required to prove cyber defenses are working and identify areas that present the most risk to the organization. Validation can also identify what controls bring the most value and which proposed investments would mitigate the most risk.

Mandiant Advantage Automated Defense

The growth of security data coupled with the shortage of skilled security personnel leaves public sector organizations at risk. Security teams of all sizes are resource-constrained, filtering alerts to match the analysis capacity of their staff and existing security investments. This practice leads to unattended alerts or potential evidence of active threats remaining hidden in the network or on the endpoint, increasing the likelihood and impact of a security incident.

Agencies need to use automation and machine learning within the security operations workflow to reduce monotonous tasks, incorporate threat intelligence to detection capabilities and apply consistent alert triage and incident investigation escalation. Automation enables organization to augment the capacity of their skilled security personnel, reduce false positives, prioritize real incident and adapt to the latest adversary tactics and techniques.

Mandiant Advantage Automated Defense uses decision automation to combine data from an agency's security stack, correlating the data with up-to-the-moment threat intelligence to triage alerts and enrich incident investigations for escalation and remediation. Pre-built with data science models that are continuously learning from the latest threat actor activity derived from Mandiant Threat Intelligence, the solution delivers:

- Prioritized investigations based on asset criticality, attack stage progression, attributed threat intelligence and likelihood of incident
- Detailed cases in an intuitive incident summary with all available evidence of malicious activity
- Investigations and the detected attack stage progression mapped to the MITRE ATT&CK™ Framework
- Visibility into the quantity of alerts that are monitored, analyzed, and escalated, as well as false positives identified
- Insight into health of sensors and controls

Mandiant Advantage Attack Surface Management

Attack Surface Management generates comprehensive visibility of the extended enterprise. The module uses the power of robust graph-enabled mapping to illuminate assets, alert on exposures, and enable security teams to operationalize intelligence with incredible speed and agility.

Mandiant Attack Surface Management allows organizations to:

- Have comprehensive visibility through graph-based mapping and discover assets and cloud resources
- Monitor your infrastructure in real time to detect changes and exposures so you you can stay ahead of threats
- Empower security operations to mitigate real-world threats by applying Mandiant expertise and intelligence to your attack surface. This is especially vital now in a time of geopolitical upheaval and heightened cyber threats, especially to critical infrastructure.

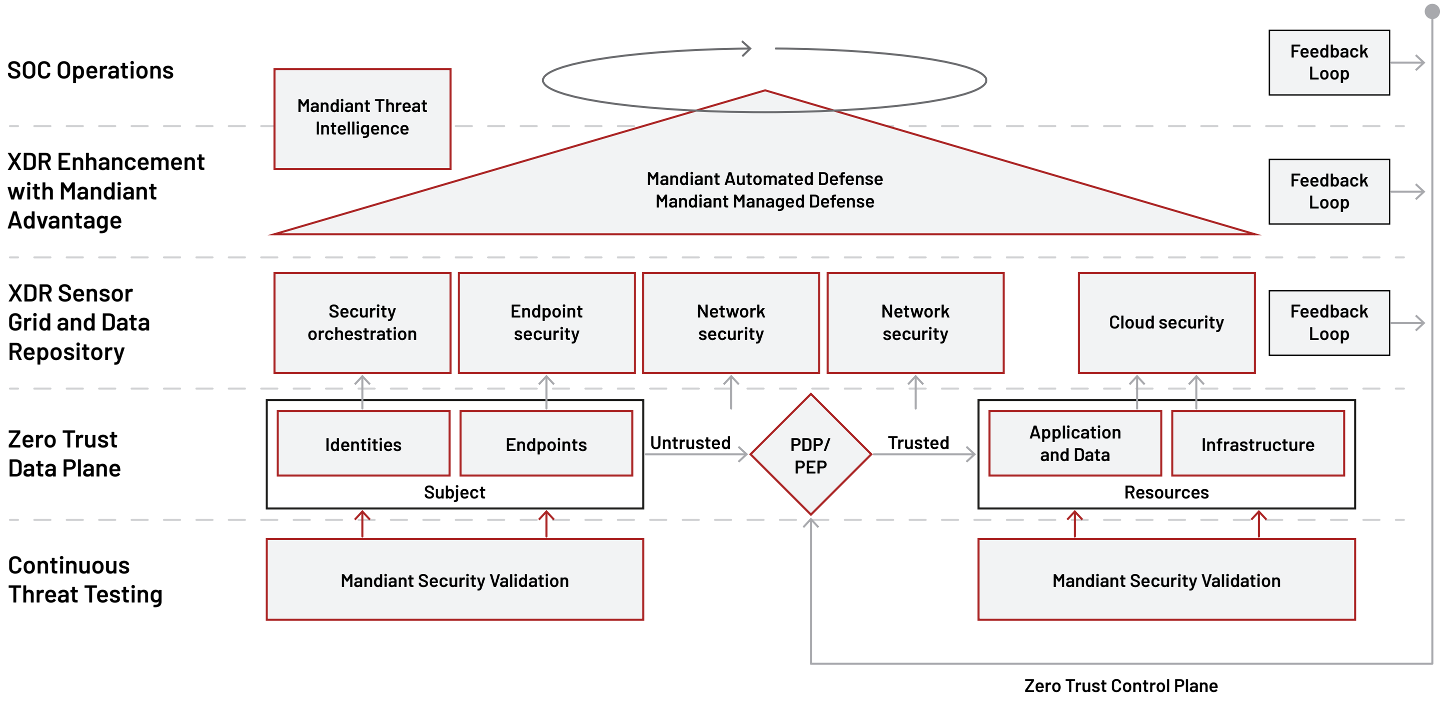

FIGURE 3. An intelligence-led platform to pursue Zero Trust initiatives.

Tying It All Together

Mandiant also helps federal agencies address the Executive Order's goals of creating standardized responses to cyber incidents and improving investigative and remediation capabilities. The Mandiant Advantage is a multi-vendor XDR platform that delivers Mandiant's transformative expertise and frontline intelligence to security teams of all sizes. It includes:

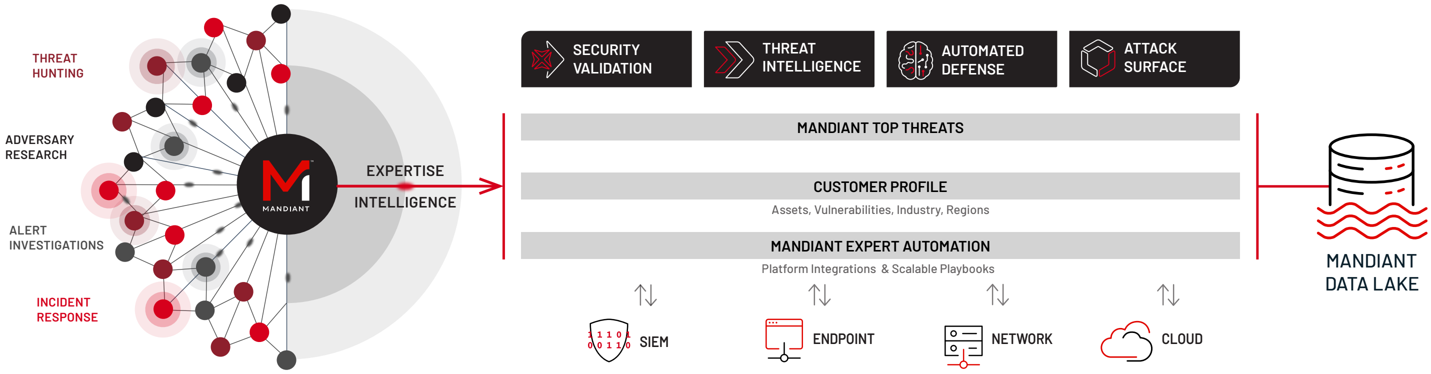

FIGURE 4. Mandiant Advantage Platform.

The platform combines scalable detection and response capabilities with the ability to measure and prove security effectiveness against the threats that matter most. This enables security leaders to allocate spend and personnel where they are likely to mitigate the most risk, identifying gaps and redundancies in your security programs as well as opportunities for optimization. The result is the ability to make data-driven decisions where more resources may be needed or areas where costs can be cut without impacting risk.

Ultimately, Mandiant experts can recommend a clear path to stronger security based on your existing investments, in-house resources and forward-looking requirements. We can help you achieve a zero trust approach and meet the mission laid out in the cyber security Executive Order.

Learn more at **www.mandiant.com**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant

Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.