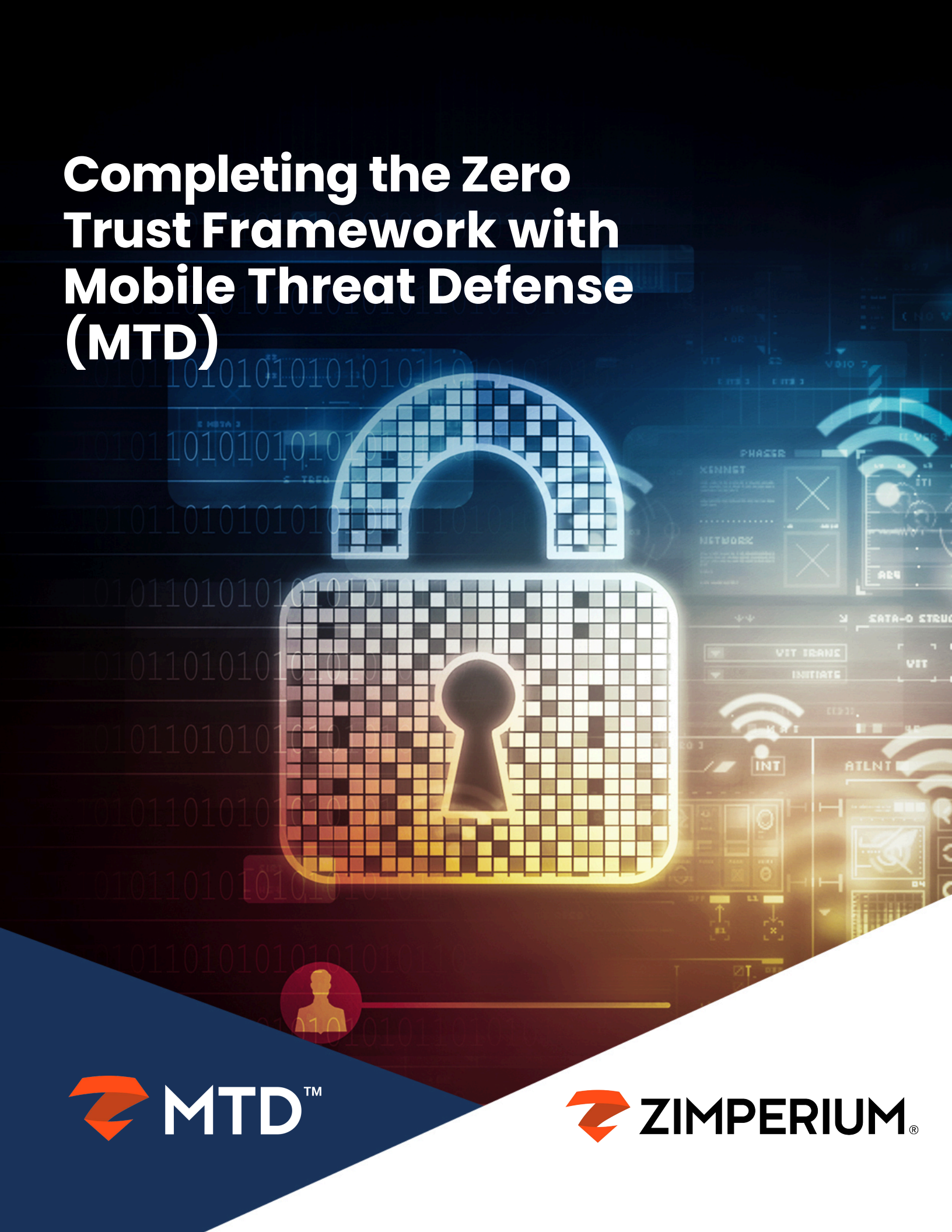
Completing the Zero Trust Framework with Mobile Threat Defense (MTD)



MTD™

ZIMPERIUM®

Introduction

On May 12, 2021, President Joe Biden announced Executive Order 14028 "Executive Order on Improving the Nation's Cybersecurity" (EO). As part of the EO's mandate, agencies must accelerate their cloud adoption strategies and establish a Zero Trust Architecture (ZTA).

The EO tasked NIST, CISA, and OMB with providing agencies guidance to help them comply with the mandates. While each agency takes a slightly different approach, all three concur on several fundamental ZTA requirements:

- Users and devices must be appropriately authenticated to networks.
- Endpoint Detection and Response (EDR) is mission-critical for ensuring all devices meet security standards.
- Malicious or compromised applications must not connect to Federal networks.
- End-user privacy must be maintained.

While these core elements are challenging in their own right, remote work models further complicate many ZTA initiatives. Users need and want to use their own devices, especially mobile ones. Allowing workforce members to use their own devices to connect to Federal networks enhances productivity and reduces technology spend. Despite Bring Your Own Device (BYOD) policies, agencies struggle to appropriately secure user-owned mobile devices while protecting workforce member privacy.

In addition to direct access to networks and data, mobile devices are also critical from a user attestation perspective. For example, employing multi-factor authentication, as required under the EO, often uses a mobile device for the second factor, using:

- SMS
- Email notifications
- Authentication apps
- Password managers
- Certification-based authentication

The disconnect between ZTA mandates, securing user-owned mobile devices, and remote working creates significant challenges as agencies seek to comply with the EO's requirements.

Mobile Device Security Challenges for Meeting Executive Order Mandates

In the year prior to the EO, threat actors increasingly focused attacks on mobile devices seeking to exploit weak security controls, e.g.,

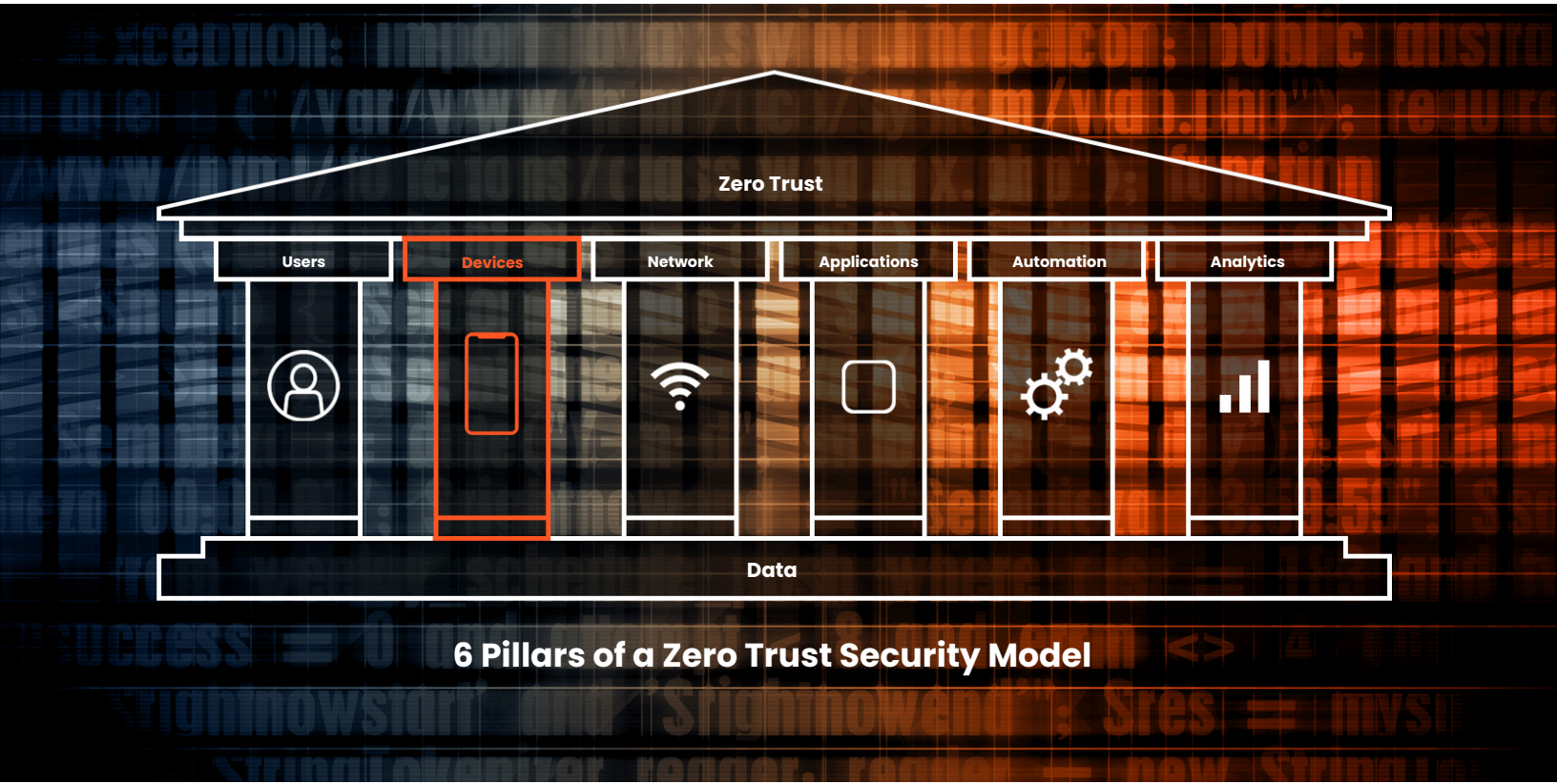
- 19% of mobile phishing attacks targeted productivity applications
- 37% increase in mobile phishing attempts between Q4 2019 and Q1 2020
- More than 90% of targeted attacks start with mobile devices
- 50,000 users were impacted by the spyware Pegasus

There are many elements of a complete ZTA, but two are critical to the discussion around mobile devices:

1. **Identity Validation:** Ability to assess and validate the identity of the person requesting network or data access; and
2. **Endpoint Risk Posture:** Ability to determine the risk posture of the device the user is using to access resources.

Based on the combination of those two elements, a ZTA can make a real-time decision as to what, if any, resources can be accessed. With sixty percent of endpoints attempting access being mobile, ZTA's are incomplete without a mobile threat defense solution that can assess mobile device risk. To comply with the ZTA endpoint requirements, mobile threat defense solutions provide agencies with real-time risk assessment and protection against zero-day cyberattacks, including:

- Device exploits
- OS vulnerabilities
- Network attacks
- Phishing attempts
- Malicious apps
- Application vulnerabilities



6 Pillars of a Zero Trust Security Model

Mobile threat defense is often referred to as "Mobile EDR" and meets the spirit of the EDR recommendations from NIST, CISA, and OMB. Legacy EDR solutions detect abnormal activity on traditional endpoints, but they fail to protect mobile endpoints for several reasons:

- Lack of visibility arising from locked down kernels in mobile OS's
- Inability to detect risky or malicious networks
- Disabled cloud-based detection by network attackers
- Inability to assess privacy and security risks in legitimate (non-malicious) mobile apps
- Privacy issues

Other "system of record" solutions such as Mobile Device Managers (MDM) provide data useful for rudimentary device-trust assessments against known threat approaches like jailbreaks and out of date operating systems. But they cannot offer near-real-time accounts of risks and attacks. Additionally, MDMs may not be used often in BYOD scenarios where user privacy is a concern. MDMs fails to meet the EO requirements for device risk attestation, including the inability to detect and resolve issues associated with:

- Advanced threats
- Mobile phishing attacks
- Device health, particularly in real-time
- Cloud application security
- Malicious applications downloaded from untrusted sources

Zimperium Mobile Threat Defense (MTD) for Federal Agencies: Advanced Security Solution for Complete Mobile

Best practices suggest leveraging AI/ML to set baselines and detect abnormalities across all mobile devices, then automate remediation responses.

Zimperium MTD - formerly known as zIPS -is an advanced mobile security solution that provides persistent, on-device protection against known and unknown threats, leveraging machine-learning-based detection for Android, iOS, and Chromebooks.

Zimperium MTD augments an agency's EDR and MDM technologies, giving agencies the mobile device integrity attestation necessary for a complete approach to zero trust. TheMTD agent deploys to a device then:

- Scans for known and unknown malware, device exploits, malicious networks and phishing attacks
- Verifies device configurations comply with policy
- Inventories applications for risky or side-loaded apps
- Provides data to security tools via API

Zimperium MTD is built with a focus on end-user privacy. Zimperium solutions detect threats on-device rather than relying on a cloud look up, protecting mobile devices without the need to collect or process any personally identifiable information (PII). By design, MTD protects end-user privacy, ensuring that Federal agencies comply with ZTA and privacy mandates.

Zimperium MTD runs locally on mobile devices, recognizing standard baseline configurations for operating systems and apps. It also recognizes regular web traffic activity. When it detects abnormal activity on a device, MTD sends the user an alert. In addition, it can also block certain activities, such as preventing a phishing link from loading.

Zimperium MTD's on-device security capability enables it to understand the risk and threat posture of the device, providing the attestation necessary to determine whether a user should be trusted or not. It can detect whether a device meets security baselines or has been exposed to an elevated level of risk, ultimately reinforcing the ZTA implementation.

Zimperium uses its mobile threat defense engine to detect the latest zero-days, protecting the whole device whether connected to the internet or not. With MTD, organizations have continuous mobile device monitoring without requiring a persistent connection for signature validation. This protects devices from threat actors disconnecting or redirecting traffic when connected to a cellular tower.

Zimperium MTD is critical to securing mobile devices, providing the visibility into threat and risk postures that impact overall user and device attestation necessary for successfully implementing ZTA. Zimperium augments an agency's IDM, EMM/MDM, and CASB, integrating critical data collection and advanced mobile endpoint security.

Zimperium is a trusted solution across the Federal landscape. Zimperium was the first mobile threat defense provider to be granted an Authority to Operate (ATO) status from the Federal Risk and Authorization Management Program (FedRAMP). Further, the U.S. Department of Defense (DoD), through its Defense Information Systems Agency (DISA) and Defense Innovation Unit (DIU), selected Zimperium to deliver comprehensive Mobile Endpoint Protection (MEP) to service members around the world. Zimperium's MTD solutions will protect DoD mobile endpoints against phishing, malicious/risky apps, OS exploits, and network attacks.

HOW DO WE SOLVE THE PROBLEM?

Detection
Device, Network, Apps & Phishing threat detection

Visibility
Proactive visibility into risks and vulnerabilities

Remediation
On-device remediation and UEM driven compliance actions

Threat Intelligence
Deep forensics for Threat Hunting & Incident Response

Key Features and Enterprise-Grade Capabilities

Zimperium MTD's on-device, machine learning-powered detection is capable of evaluating the risk posture of a user's device, securing the enterprise against even the most advanced threats.

With a privacy-by-design approach, Zimperium MTD provides users with a transparent experience by delivering customizable user settings and insight into what data is collected and used for threat intelligence.

Built with advanced threat security in mind, Zimperium MTD meets the mobile security needs of enterprises and governments around the world.

Powered by Machine Learning
On-device, machine learning-based detection provides prevention against the latest mobile threats, including zero-day malware.

Critical Data, Where You Need It
With integrations into enterprise SIEM, IAM, UEM, and XDR platforms, administrators always have the data they need.

Deploy Anywhere
Address local data laws and compliance needs by deploying to any cloud, on-premise, or air-gapped environments.

Zero-Touch Deployment
Deploy and activate Zimperium MTD on your employees' and contractors' mobile endpoints without the need for complicated activation steps by the end-user.

Critical Data
Comprehensive device attestation enables enterprises to have a complete picture of their mobile endpoint security and shores up Zero Trust architectures through existing integrations.

Complete Mobile Coverage
From tablet to phones, Zimperium provides complete security coverage across Android, iOS, and ChromeOS.

About Zimperium

Zimperium, the global leader in mobile security, offers the only real-time, on-device, machine learning-based protection against Android, iOS, and Chromebook threats. Powered by z9, Zimperium provides protection against device, network, phishing, and malicious app attacks. For more information or to schedule a demo, contact us today.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244