FORTRA™

WHITE PAPER (TRIPWIRE)

Building the Foundation of Zero Trust for Long Term Success

As highlighted in the Biden Administration's Cybersecurity Executive Order (EO) in May 2021, Zero Trust Architecture (ZTA) is increasingly becoming an essential element of federal cybersecurity programs. Those responsible for implementation must have a clear understanding of what ZTA is, and how best to implement it for maximum impact.

In the pages that follow, Fortra's Tripwire presents a point of view on how security professionals must first address how integrity is established and maintained before implementing zero trust across their enterprises.

After 20+ years of assisting federal agencies in improving their security, we believe that adopting this alternative perspective will not only bring clarity on how to apply and maintain a zero trust environment, but will confidently deliver the Executive Order's intended long-term outcomes.

Traditional Zero Trust

According to NIST, the term "zero trust" is used when referencing both a security architecture model and when identifying the security state of an environment:

> *Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established.*[1]

Traditional zero trust as a security architecture model is based on withholding access of the devices, applications/software, people, and services that connect into a network until trust is established. Often referred to as "deny-by-default," this has traditionally been achieved by using a combination of identity and network access solutions such as software-defined perimeters, secure web gateways, risk-based authentication, along with frameworks such as DISA's Comply-to-Connect, etc.

INTEGRITY ONLY MATTERS IF DONE WELL

In most cases, organizations have the tools in place to manage integrity—they are just not managing integrity well. What does "managing integrity well" look like?

Organizations centralize security and compliance visibility across the enterprise, from industrial spaces to data centers to a cloud environment.

They continuously monitor, assess and compare secure configurations for each piece of hardware and version of software to established guidelines so that even the smallest configuration change of a critical asset doesn't increase a system's vulnerability

While monitoring for changes to files and file attributes, they can tell the difference between business-as-usual changes and ones that spell trouble

Last but not least, organizations that do integrity well deploy effective baselining to enable detection of unauthorized or potentially malicious changes.

When implemented across an enterprise, the model establishes a security "state," also referred to as "zero trust." Through constant revalidation of the trustworthiness of connecting devices, user accounts, and applications, the security state of the environment is maintained. Whether referencing the model or the security state, zero trust is well on its way to becoming the de facto security approach of the federal government.

There is an abundance of guidance available to assist agencies on their zero trust journey, but Tripwire advocates for taking an integrity-focused approach to establishing the foundation for any zero trust environment. At the same time that continuous revalidation of connecting devices, user accounts, and applications is implemented as a default process, organizations must also implement an ongoing process for revalidation of the critical systems to which they are connecting.

A Fresh Look at Integrity

While the term "integrity" has been commonly used in the cybersecurity lexicon for years, its meaning and use have been relatively limited to how it is defined within the CIA (Confidentiality, Integrity, Availability) Triad. The need to reconsider its central role in security is long overdue and becomes imperative for those planning a zero trust strategy.

In the new world of pervasive information and operational technology, always on/always connected networks, fluid data transfers across cloud and hybrid cloud environments, and broadly deployed endpoints, federal agencies must take a fresh look at integrity.

Integrity: The Basis for Trust

By definition, integrity, when applied to any realm (physical, relational, etc.), assumes little to no variance between something's original or desired state, and its current or actual state, between what was intended and what was realized. In other words, its current state can be trusted because nothing has changed from its original or desired, trustworthy state. In the enterprise computing realm, the meaning of integrity is no different.

"Managing integrity is ultimately about managing change throughout your entire environment," says Tim Erlin of Tripwire. "Change can be internal or external, authorized or unauthorized, intentional or accidental, benign or malicious."

Integrity as an operational concept is the basis for trust and the foundation of cybersecurity within an organization.

The CIA Triad: Integrity is the foundation of Confidentiality and Availability

Agencies start applying this concept by extending their information management (IM) practices and policies from critical File Integrity Monitoring (FIM) to include the full range of assets managed. It's no longer enough to watch solely for changes to organizational data/file structure—any change within a system can be a threat to an organization's security. By applying "Integrity" throughout, you can better manage the attack surface, and address more cumulative security and operational risks.

Integrity is foundational to setting up systems in a known and secure state and being able to maintain that state or know when something changes.

All Zero Trust is Established and Maintained with Integrity

In the context of zero trust, integrity controls are required to ensure ongoing trustworthiness. It cannot be a set-it-and-forget-it approach. In viewing integrity as a broad program, one that encompasses all aspects of architecture and security measures across IT and OT environments, its role as the foundation of zero trust comes into focus. A mature view of integrity management organizes security controls to align with key elements of the architecture with system integrity at the top. On-premises, cloud, and hybrid infrastructures all fall under the purview of zero trust.

- **System Integrity** ensures that unauthorized changes are not made to critical assets, and includes file integrity monitoring (FIM), secure configuration management, host-based intrusion detection systems (IDS), vulnerability management and patching, and privileged account management (PAM) along with the following additional areas of integrity:
- **Data Integrity** protects the incorruptibility of data, and includes data backup and recovery, encryption, blockchain, identity and access management (IDAM), and file access monitoring
- **Security Control Integrity** captures the state of all your systems security controls as dictated by a standard such as DISA, NIST, CIS, PCI, HIPAA, SOX and many others.
- **Network Integrity** maintains the reliability of connections and protects the data in transit, and includes firewalls, network-based intrusion detection systems (IDS), encryption, virtual private networks (VPNs), and secure remote access.
- **Network Device Integrity** captures the configuration of all your network devices and is a critical part of any security system. This includes, routers, switches, firewalls, IDS systems, VPN concentrators and others.

- **Database and Application Integrity** identifies what applications are installed on your infrastructure and how those applications are setup, configured, and structured in all aspects to include any auditing and then monitoring to detect deviation. Directory services such as AD/LDAP are good examples of applications that are critical to all organizations.
- **Firmware Integrity** ensures there are no firmware compromises, and enables you to know the state of your firmware configurations.
- **Physical Integrity** protects the facilities and spaces within which critical assets reside, and includes access controls, security monitoring, all-hazards mitigation (fire, water, earthquakes, etc.), and uninterrupted power supplies
- **Process Integrity** ensures that multiple controls are properly integrated, controlled, and coordinated to ensure a holistic approach to incorruptibility and resilience, and includes security incident and event management (SIEM), security orchestration, automation and response (SOAR), analytics and reporting, and a well-functioning security operations center (SOC)
- **People Integrity** seeks to maintain trust in the humans who use IT and OT systems, create and use data, and oversee enterprise security efforts, and includes security awareness training, certification, role-based access controls (RBAC), end-user behavior analytics (EUBA), organizational policy enforcement, and background screening

Integrity should be a foundational control for any organization. Aligning security controls with an integrity platform accordingly builds and monitors trust in organizations' people, processes, and technology and is essential for establishing and maintaining a trusted state. Rather than a deployment of new capabilities, the emphasis is on leveraging (and prioritizing) existing and emerging capabilities to maintain trust throughout the architecture, thus providing the necessary foundation for zero trust security.

While the zero trust approach trusts no one, establishing and maintaining a trusted state is crucial to any zero trust implementation. In fact, NIST includes integrity as a guiding principle of zero trust: "The enterprise ensures all owned and associated systems are in the most secure state possible and monitors systems to ensure that they remain in the most secure state possible."

Tripwire takes this a step further by referring to integrity as the very foundation of zero trust, because true zero trust without integrity as the foundation is not zero trust.

Planning for Zero Trust: Where to Start

As agency leaders moved quickly to meet the Executive Order's directive to develop an implementation plan, the question most often asked was, "Where do we start?"

Tripwire suggests that the answer is to establish a baseline of integrity. All zero trust architectures must be built from a trusted state as it applies to both an agency's systems and information. How do we successfully achieve a baseline of integrity from which we then build, monitor, and maintain a zero trust architecture?

Organizations that do integrity well are deploying centralized security and compliance visibility across the enterprise, estimating and scoring vulnerability risk, continuously monitoring, assessing and comparing secure configurations for both hardware and software, distinguishing between business-as-usual vs. malicious changes, and thus, are able to create a baseline that will enable detection of unauthorized or potentially malicious changes. This baseline of integrity then serves as the foundation for zero trust moving forward.

Prevention and Detection

An integrity baseline provides a single source of truth to understand the security, compliance and operational state of assets over time. Only if you establish a "single source of truth" through baselining, can you can monitor for low priority, routine changes, as well as detect changes that signify a much more potentially malicious or bad incident, things like new unrecognized binaries being added, access privileges that are changing on critical files, listening ports being opened, logging disabled, etc. With this continuous monitoring capability, the integrity platform also becomes critical to successful prevention and detection within a zero trust environment. Integrity management not only serves as the foundation for ZTA, it serves as the ultimate back-stop, should attackers get in, since they must make a change sooner or later.

Zero Trust Over Time

Maintaining a good handle on the systems and devices that fall within the purview of federal agencies has always been extremely difficult. As systems diffuse across remote, cloud, hybrid, and on prem platforms, the challenge becomes even greater. Further separation through increased use

of containerization, software as a service, etc., all lead to challenges in maintaining visibility and integrity across a zero trust architecture.

An organization must continuously revalidate the trustworthiness of systems and information by using strong configuration and robust change management tools such as those offered by Tripwire. Monitoring and maintaining integrity throughout the environment over time ensures a zero trust state and even identifies the threats that might make it past the zero trust architecture.

Adopting the point of view that "zero trust without integrity as the foundation is not zero trust" will ensure that your organization not only gets it right the first time, but that it can maintain zero trust over the course of time and throughout the entire environment.

HOW TRIPWIRE HELPS

Tripwire's best-in-class technology and services allow agencies to focus on the right endpoints in real-time, on-site and in the cloud, and enable intelligent decisions and actions to strengthen security. Our integrity management solution is an essential cybersecurity platform that enables federal departments and agencies to see with confidence, decide with confidence and operate with confidence, while meeting requirements established by independent frameworks and regulatory standards such as FISMA, NIST, DISA and CIS.

Tripwire's known and trusted IT/OT security capabilities are well suited for complex environments in the nation's critical infrastructure sectors, across dispersed on-prem deployments, hybrid cloud architectures, and industrial control systems.

Our award-winning cyber integrity solutions are used across the DoD, numerous intelligence agencies and their mission partners, nearly every federal department and in most of the independent agencies, as well as components of the Legislative and Judicial branches.

Let us take you through a demo of Tripwire security and compliance solutions and we'll answer any of your questions.
Visit www.tripwire.com/demo

Sources

1. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

Copyright © Fortra, LLC and its group of companies. Fortra™, the Fortra™ logos, and other identified marks are proprietary trademarks of Fortra, LLC.
(fta-tw-gd-1123-r1-hm)