FORTRA™

WHITE PAPER (TRIPWIRE)

Why Integrity Should Be Your Organizing Cybersecurity Principle

Reimagining Security as an Integrity Problem

While integrity has been a common word in the cybersecurity lexicon for years, its meaning and use have been relatively limited. It may be time to reconsider its central role in security. The reality of always-connected networks, fluid data transfers across cloud and hybrid environments, and broadly deployed endpoints presents an opportunity to take a fresh look at integrity as an organizing concept for security strategy.

Enterprise cybersecurity has been a vexing challenge for years. Most common approaches prove exhausting and ultimately insufficient. Focusing on keeping attackers out of a perimeter is an untenable strategy—as "the perimeter" is now fluid and porous. Fretting about whether attackers have gained access to the enterprise network is unproductive—they are already there. Obsessing over threat intelligence is only partially helpful—defenders remain caught in a never-ending game of catch-up. And security measures like system hardening and access controls can be effective—but timely and accurate insight into their effectiveness is elusive.

Within this context, integrity has often been defined in one of two ways:

1. The incorruptibility of data (as part of the CIA triad), and
2. File integrity monitoring (FIM), a system monitoring control which has become a compliance requirement in broadly-applicable standards such as PCI DSS (Payment Card Industry Security Data Security Standard).

Data security and FIM have been the primary domain of conversations on integrity.

When viewed as a broader concept, however, integrity emerges as a way to understand what matters to an organization and what to focus on to prevent undesired consequences. As the basis for trust and reliability, integrity becomes the ultimate measure of system security.

By reexamining security as an integrity problem, and realigning security controls accordingly, an organization can focus its efforts on maintaining trust in its people, processes and technology.

Integrity as the Basis for Security

By definition, true integrity allows for no variance between something's original and current state, between its intended and realized states.1 In other words, its current state can be trusted because nothing has changed from its original or desired, trustworthy state.

In a relational context, you determine that someone has integrity (therefore, can be trusted) when there is no variance between what they say they are going to do and what they actually do. In a physical context, I determine that a physical space has not been compromised (therefore, is safe to enter) when there is no change in the environment between the time you left and when you return.

The term "integrity" serves as the basis for trust, and security is the result. If security is the result of an environment's unchanged state, then integrity is a necessary condition of security. The same is true when applying integrity to a computing environment.

> Managing integrity is ultimately about managing change throughout the entire environment. Change can be internal or external, authorized or unauthorized, intentional or accidental, benign or malicious. When one takes an expansive view of change, it's clear that managing integrity is at the core of foundational security.

Integrity Defined

Most commonly, integrity is referenced as one of three CIA Triad principles—confidentiality, integrity and availability—that serve as a framework for organizations to make sound information security policies. In this context, integrity is generally focused on organizational data and making sure that data remains uncorrupted by external sources. While data integrity is certainly important to any security strategy, the term when used in this way significantly limits both the perspective and power of integrity in its broader application—one that impacts every area of an information system. Integrity is a necessary condition and essential element of confidentiality and availability, its peers in the CIA triad.

Unfortunately, most organizations have security strategies based on the traditional understanding of integrity as a specific control like FIM, alongside other important controls. Without broadening integrity as an operational concept across the entire computing environment, we will continue to see minimal improvements to organizational cyber maturity levels.

Why Now?

Technology continues to evolve at a rapid pace, and one of the greatest challenges we face is attempting to defend an expanding attack surface that is borderless, porous and interdependent. In this environment, the old security approach (perimeter-based security and network defenses) has become untenable, and new approaches (zero trust, artificial intelligence and machine learning) remain unproven.

Following a decade of tremendous growth of incidents causing massive financial, privacy and intellectual property losses, we know with certainty that bad actors are plentiful, and that traditional security solutions continue to fail to keep them out.

Given the explosive growth of data, the escalating number of endpoints attached to the network and the growing complexity of systems, it is nearly impossible—regardless of size or budget—to defend an organization from intruders. Of growing concern is not just the escalating number of endpoints, but the rapid speed at which remote endpoints such as laptops are being added to enterprise networks due to COVID-19 and other telework requirements.

Adding to this challenging situation is the explosive growth of the "Internet of Things" and the "Industrial Internet of Things," (IoT and IIoT, respectively) or dedicated, connected devices that can collect and exchange data using embedded sensors, including medical devices, security cameras and electric meters.

One significant result of an integrity-related attack is that decision-making by corporate executives and other stakeholders is impaired because they're not able to trust the information they're receiving—or perhaps worse, they make decisions based on inaccurate or manipulated data. Destructive malware, ransomware, malicious insider activity, and even honest mistakes all set the stage for why organizations need to quickly detect and respond to an event that impacts integrity.

Some organizations have experienced systemic attacks that force operations to cease. One variant of a data integrity attack—ransomware—encrypts data, leaving it modified in an unusable state. Other data integrity attacks may be more dynamic, targeting machines, spreading laterally across networks, and continuing to cause damage throughout an organization. In either case, behaviors are exhibited—such as files inexplicably becoming encrypted or network activity—that provide an ability to immediately detect the occurrence and respond in a timely fashion to curtail the ramifications.

Enterprise Integrity as a Security Strategy

Integrity as an enterprise-wide organizing concept for security would extend beyond its currently narrow application as specific controls to encompass all aspects of architecture and security measures across IT and OT environments.

Rather than a deployment of new capabilities, the emphasis would be on leveraging (and prioritizing) existing and emerging capabilities to maintain trust throughout the ecosystem, thus providing the necessary foundation for security.

An expansive view of integrity management would organize security controls to align with key elements of the ecosystem:

- **Data integrity** protects the incorruptibility of data, and includes data backup and recovery, encryption, blockchain, identity and access management (IDAM), and file access monitoring
- **System integrity** ensures that unauthorized changes are not made to critical assets, and includes FIM, secure configuration management, host-based intrusion detection systems (IDS), vulnerability management and patching, and privileged account management (PAM)
- **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
- **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

Aligning security controls and integrity accordingly builds trust in organizations' people, processes, and technology. Many tools help achieve and maintain visibility, and visibility is essential to ensuring that unauthorized or malicious changes have not occurred. Building trust and then maintaining it is key to integrity management—and essential for achieving enterprise security.

The Role of FIM in Enterprise Integrity

In the context of compliance, FIM has been used to satisfy certain requirements under standards such as PCI DSS. FIM includes the ability to view changes to configurations, files and file attributes throughout the IT infrastructure.

When people think of FIM, most think of file or data integrity. In fact, FIM is a capability with a long history, going back to the original open source Tripwire tool for monitoring file hashes. While there are many approaches to FIM, agencies that do FIM well deploy solutions with capabilities beyond basic change monitoring.

These capabilities allow organizations to detect change by first establishing a highly detailed baseline version of each monitored file or configuration in a known and trusted state. Using real-time monitoring, the organization can detect change to any aspect of a file or configuration and capture these in subsequent versions. Versions provide critical before-and-after views that show exactly who made the change, what changed, and more.

"To many organizations, FIM mostly means noise—too many changes, no context around those changes, and very little insight into whether a change actually poses a risk," says Tripwire expert David Bisson.

Organizations that do FIM well also apply change intelligence to each change to determine if it impacts integrity (for example, rules that determine if the change takes a configuration out of policy or is one that is typically associated with an attack). "FIM is a critical security control, but it must provide sufficient insight and actionable intelligence," says Bisson.

If one thinks of the desired state measured in terms of acceptable risk, then maintaining integrity is all about maintaining that acceptable level of risk. While "check-the-box" FIM applies this concept very narrowly to files and to limited configuration elements, mature integrity management seeks to apply this concept to the entirety of an organization's IT ecosystem including systems, network devices, and cloud infrastructure.

"Check-the-Box Integrity" vs. Integrity Done Well

But, as has been noted, in most cases organizations have the tools in place to manage integrity—they are just not managing integrity well.[1]

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
- In addition to scanning for vulnerabilities, they estimate and score the risk of vulnerabilities, enabling them to prioritize and focus remediation efforts on the highest risk hosts and the highest scoring vulnerabilities
- 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

Baselining is an under-appreciated and not-well-implemented security control that establishes "knowns" about an organization's systems, so they can quickly recognize when something is out of place, both in a static and a dynamic sense.

Baselining helps defenders know what to focus on by alerting them to critical, unauthorized, potentially malicious changes on likely-targeted systems. It shifts the dynamic from just guessing where the attackers may be or just trying to harden systems in a tactical sense, to actually operationalizing enterprise risk management, and provides a single source of truth to understand the security, compliance and operational state of an asset by highlighting deviations from business-as-usual activity and known secure conditions.[2]

The True Measure of Enterprise Security

Integrity when viewed as an operational concept in a computing environment is the basis for trust and the foundation of cybersecurity within an organization. Agencies can start applying this concept by extending their IM practices and policies from FIM to include the full range of assets managed. This will reduce their overall attack surface and address more cumulative security and operational risks. It's no longer enough solely to watch for changes to organizational data—any change within a system can be a threat to an organization's security.

Next, agencies need to assess the capabilities of their existing integrity management tools and identify a solution that provides visibility into critical assets, assurance of system integrity, and ensures operations stay focused on the right action.

Sources

[1] https://gcn.com/cybersecurity/2020/03/why-integrity-matters-in-2020/303306/

[2] Ibid

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.