tripwire

WHITE PAPER

Securing the Cyber EO's Four Critical Frontiers

What Every Federal Executive Needs to Know in a New Era of Accountability

FOUNDATIONAL CONTROLS FOR SECURITY, COMPLIANCE & IT OPS

Cybersecurity during the Obama administration can be characterized by the shift from a "check-the-box" compliance mind-set to a "risk management" perspective. With the government's information technology and connected resources now under constant attack from increasingly disciplined, well-funded and innovative cyberterrorists and hackers, the Trump administration is moving to further ramp up the federal government's cybersecurity policies and capabilities.

The "Presidential Executive Order (EO) on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," the first cybersecurity executive order issued under the new administration, in May 2017, takes the risk management approach to the next level. Most notably, the Trump administration declared its intention to hold senior leadership accountable for implementing risk management measures—and making sure that those measures are aligned with strategic operational and budgetary planning processes.

Adding to this responsibility, the EO also suggests that agency IT and cybersecurity personnel will be required to expand their organization's reach across three relatively new frontiers:

» A modernized and resilient IT architecture. Although the funding source for this has not been identified, the Trump administration is directing agency heads to begin planning for the deliberate modernization of the government's "antiquated" IT systems to better manage cyber risk.

» Greater reliance on shared IT services, especially cloud-enabled services, in all future procurements, wherever feasible and possible, as a way to optimize IT performance, increase usability, efficiency and economy, and boost security.

» Broader support for securing critical infrastructure (CI) assets. As connectivity and automation have increased, so too have attacks. They may intend to disrupt, mismanage or take control of CI assets such as the electric grid, nuclear plants and weapons systems, as well as non-CI assets common to all agencies, such as mail processing equipment and physical security systems.

Finally, as a result of an increased investment in these three areas, the rise of an additional fourth frontier must also be anticipated: the frontier of scale, or the exponential increase in the sheer number (and type) of assets agencies will need to cover as they execute effective security operations and meet reporting requirements.

Getting Your Agency Leaders Up to Speed

So how can CISOs help agency leaders attain the confidence and the capability they need to make informed risk decisions in an environment of increased accountability and greater scale? A heightened focus on integrity management, expanded network visibility and the ability to simultaneously address security, compliance and operations will be critical to the decision-making process—and ultimately to achieving the desired outcome.

The EO itself provides some much-needed guidance in this regard. Specifically, it mandates—rather than just encourages—CISOs and other cybersecurity leaders to align their efforts with the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF). This measured yet flexible six-step process allows agencies to drive the security solutions that are most appropriate to their mission and risk tolerance, while also providing the ability to continuously monitor, analyze and document any changes for easier reporting capabilities.

In helping to craft and oversee their organization's action plan for implementing the RMF, security leaders will also need to identify a baseline for understanding where improvements in overall cybersecurity strategy and investments can—and should—be made.

Prioritizing Integrity

To effectively implement the RMF, agencies must continually focus their investments on three essential components as identified in the SANS Institute's CIA Triad. All three of these areas are critical to successfully identifying and mitigating risk, according to researchers at the SANS Institute:

» **Confidentiality**—Protecting sensitive information from unauthorized access by defining and enforcing appropriate access levels

» **Integrity**—Protecting data from modification or deletion by unauthorized parties and ensuring that damage can be repaired/reversed[1]

» **Availability**—Ensuring systems, access channels and authentication mechanisms are working properly and are protected to remain available

Interestingly, IDC recently reported in its Worldwide Security and Vulnerability Management Forecast, 2016–2020: Enterprises Continue Focus on Security Operations that integrity management tools that assure the integrity of data, configurations, files, and settings account for just 12 percent of organizations' total security budgets. While the original CIA model assigns equal importance to all three elements, this data suggests that the reality on the ground now requires a shift in thinking—and prioritization.

One need only look to the most recent and most destructive breaches, such as the WannaCry ransomware attack, to realize that organizations need to beef up their ability to "see" exactly what is happening within their systems in real time. WannaCry managed to infect and disable hundreds of thousands of computer systems around the world by exploiting a known vulnerability, easily invading systems that weren't inoculated with the published fix that had been available for more than two months.

Because most tools supporting data and systems integrity are not easily or efficiently scaled for enterprise-level deployment, the majority of federal

agencies have historically prioritized confidentiality and availability. Nonetheless, a compromise in integrity now represents the biggest threat to national security. The longer a system change or vulnerability goes undetected, the more damage is likely to be inflicted. In fact, a report by Mandiant M-Trends found that, on average, hackers spend 146 days rooting around and wreaking havoc on an IT network before they're found out. The key to integrity is having ongoing "visibility"—the ability to detect, alert on and investigate malicious or unauthorized cyber activity across systems, files and logs.

This is where an effective integrity management solution comes in. It enables large-scale enterprises to protect against advanced attacks, pick up on otherwise undetected intrusions that have made it past perimeter defenses, and guard against insider threats and unauthorized changes by adequately maintaining and assuring the accuracy and consistency of data over its entire life cycle. Integrity management also helps achieve compliance with federal civilian, DoD and intelligence community regulations.

Finding an Enterprise Solution

Any solution that assures integrity management must provide foundational controls for these five areas:

» Asset Management

» Configuration Management

» Change Management

» Vulnerability Management

» Log Management

These five components, integrated and scaled to an enterprise level, will assure the integrity of a system while adding an additional layer to confidentiality and availability defenses. They also provide visibility into network, data and security operations that is both broad and deep—an absolute necessity to meeting the demands for accountability across the EO's three new frontiers. According to the IT Process Institute, 90% of breaches can be prevented through effective integrity assurance.

Agency executives who can tie performance—derived from actual threat sources and prioritized based on demonstrated effectiveness—back to a foundational controls framework will have a much more dynamic way to manage risk and an easier way to demonstrate their success to auditors.

Choosing the Best Way Forward

As agency CISOs consider the priorities and mandates outlined in the EO, they must begin to evaluate which solutions will help their agencies successfully expand into and navigate these new frontiers. They especially need to answer:

» How do your security tools work together to manage all IT and operational assets as an enterprise?

» Can your tools provide integrity management controls across physical, virtual and on-premise and public cloud landscapes?

» Can the tools take an inventory of all of your assets, whether endpoint devices or operational systems, across all frontiers, especially on- and off-premise cloud and critical infrastructure assets?

» Do the tools provide real-time visibility into what is going on at any given time in files, applications and networks, or do you rely on regular, after-the-fact scans?

» When an unauthorized change is detected, are you able to take a deep forensics dive into the history of the change or the user who made it?

» Can the tool or suite sift through the vast quantities of generated data to rapidly classify and prioritize the most important vulnerabilities, changes and events?

Unfortunately, most agencies will find that many of their investments in point solutions for individual controls simply aren't up to the task. These tools, even those considered best-in-class, provide a stovepipe view of data and events, rather than offer the single, broad context required to know exactly what is happening—at the moment when something can still be done to address it.

According to the IT Process Institute, 90% of breaches can be prevented through effective integrity assurance.

Instead, to align with the EO's priorities, agencies will need an integrated, trusted portfolio of products that enable security personnel to understand in real time exactly what is on the network, when it changes and whether that change is helpful or detrimental.

The Tripwire Difference

This is where Tripwire stands apart. Our enterprise solutions and real-time monitoring work in tandem across all computing and operational landscapes and across a wide variety of enterprise risk vectors. Known for its ability to effectively and efficiently scale, Tripwire's integrated suite provides holistic coverage of all necessary integrity assurance controls. Tripwire offers the industry's best capabilities in file integrity monitoring, system monitoring and change detection, as well as a detailed understanding of the difference between good and bad changes.

Thriving in a Changing Environment

Although the Tripwire integrity management portfolio is designed to meet an agency's comprehensive needs, individual products can be used to fill current gaps. Then over time, customers can add other suite portfolio components for a more cohesive and holistic approach.

Agency leaders who want to ensure that they meet the demands of the administration's new EO and significantly enhance the security of their data resources, cloud services and critical infrastructure assets should be encouraged to invest in some form of foundational controls that enable and assure data integrity.

Tripwire's integrity management portfolio addresses not just the symptoms of security issues but their root causes. By implementing and monitoring these tools, your security team will be able to detect a significant percentage of security breaches before they impact your data, your operations and your overall security posture.

Whether implementing a hybrid cloud initiative, a new critical infrastructure or operational assets or modernization project, Tripwire's proven portfolio will enable U.S. federal agencies and partners to expand their security reach into the newest IT frontiers with a greater degree of confidence.

1 While SANS uses the term "integrity" in the context of data integrity, FISMA broadens the scope of the term to refer to systems integrity (including database configurations, file settings, etc.)

Assure Integrity with Tripwire's Integrated Solution Suite

Tripwire Enterprise

Foundational control capabilities start with Tripwire's flagship product Tripwire® Enterprise, which provides support for both the NIST RMF and the Federal Information Security Management Act (FISMA). Tripwire Enterprise can help agencies guard across an expanding attack surface by identifying and then continuously monitoring all IT and operational assets in real-time for undesired changes, anomalies and insecure configurations. We provide the industry's deepest system visibility into files, directories, registries, configuration parameters, ports, services, protocols and other system components.

Tripwire actually invented file integrity monitoring, and Tripwire Enterprise's File Integrity Manager remains the most robust solution in the industry. That's because it has the ability to add business context to the massive amounts of change data generated by systems and other nodes in the network. Tripwire Enterprise then makes that change data both intelligible and actionable by creating focus on the most critical issues, providing deeper insights into exactly what happened and under what circumstances, and automatically validating and remediating those changes that take a configuration out of policy. Tripwire Enterprise can then prioritize security risks to provide high-value, low-volume change alerts, remediate threats and harden selected configurations. As a result, Tripwire Enterprise alone allows agencies to reduce their attack surface, broaden their reach and focus their limited resources in a way that achieves a much greater security posture.

Tripwire IP360

While Tripwire Enterprise takes an inventory of organizational assets, Tripwire IP360™, a vulnerability management solution, takes that capability to an even higher level by identifying every enterprise device and software component on your network. It then calculates a precise vulnerability prioritization score based on impact, ease of exploit and age. The results are shared with existing IT systems (including helpdesk, asset management, other security solutions and Tripwire Enterprise) so you can prioritize response or monitor selectively, based on asset value and risk.

Tripwire Log Center

Proven as a pioneer in the log collection arena, this product integrates on a very deep level with Tripwire Enterprise by building on its visibility and collection capabilities. Tripwire Log Center® provides the contextual footprint around change within a system. For example, if an employee increases his/her administrative privileges to effect a nefarious change, the program will immediately collect that event and all other events around the users actions. This guards against any significant time lags in discovering suspicious activity and allows agencies to redirect their limited cybersecurity resources to deal with other high-value tasks. When integrated with a big data SIEM solution, Tripwire Log Center provides a filtering function to extract and highlight only events of interest, reducing the overall volume of data to be analyzed.

Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. **Learn more at** tripwire.com

The State of Security: Security News, Trends and Insights at tripwire.com/blog
Follow us on Twitter @TripwireInc » **Watch us at** youtube.com/TripwireInc

WPSCE01j 201708