tripwire®
TAKE CONTROL.

WHITE PAPER

# CONTINUOUS MONITORING

## RESPONDING TO NEW THREATS AND MORE COMPLEX IT ENVIRONMENTS





IT SECURITY AND COMPLIANCE AUTOMATION SOLUTIONS

# INTRODUCTION

Today's information-driven organizations face the fundamental challenge of balancing high availability of business-critical information with maintaining its integrity and security. They must do this in spite of an increasingly complex IT environment that often includes traditional physical infrastructure, virtualized infrastructure and cloud computing. Other factors further complicate this challenge. Gartner predicts information storage to grow from 40 percent to 60 annually[1], while new variants of malware, such as polymorphic attacks that evade anti-virus software and intrusion vectors like web attack toolkits, grow exponentially—into the millions[2]. It's no small feat to balance access to data to meet business goals with protecting that very same data from hackers.

In many ways, the everyday challenge security practitioners deal with is a lot like a Faraday cage, which is designed to balance the need to protect its contents from external electromagnetic radiation while still allowing the device it's shielding to operate normally. In the case of IT security, the interior contents (the data, the systems, and the IT infrastructure in general) and exterior forces (types, quantity, sophistication and persistence of attacks) change frequently. As a result, yesterday's "cage" does not afford protection against tomorrow's threat. IT security needs guidance on how to continuously protect valuable data and systems in this constantly changing environment.

Fortunately, several guidelines have been developed to address this need. One of the key areas they emphasize is the practice of continuous monitoring, which quantifies and tracks risks in real-time, not just periodically. While its advocates tend to be more heavily from the U.S. Federal Government space, continuous monitoring is considered a best practice. However, like many other federal security standards the commercial sector should understand the security value of the solution.

This paper aims to provide clarity into the often-murky waters of continuous monitoring, offer ideas about tools that can make it easier to implement and reap the benefits, and advocate continuous monitoring as essential to an effective security solution in federal and commercial applications.

**FARADY CAGE** The invention named after Michael Faraday is often used for testing wireless devices in an interference-free setting. A more nefarious implementation of the concept are the aluminum foil-lined shopping bags used to thwart RFID anti-theft tags.[3]

## EXAMPLES OF GUIDELINES THAT FOCUS ON CONTINUOUS MONITORING

In part due to international attacks such as Stuxnet and Duqu, the U.S. Federal Government has sharpened its focus on cyber security. From this came the release of NIST Special Publication (SP) 800-37, which outlines a structure for government agencies to develop a measurable and repeatable process that takes into account risk management while balancing the demand for access to mission-critical data. The process relies on the risk management framework below:

- **Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis.
- **Select** an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.
- **Implement** the security controls and describe how the controls are employed within the information system and its environment of operation.


**FIG. 1** The NIST Risk Management Framework

- **Assess** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- **Authorize** information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
- **Monitor** the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.[4]

The final step in the cycle, Monitor, is of particular importance because it evaluates the effectiveness of a security control. But what if you only performed this evaluation periodically—for example, to satisfy a quarterly or annual audit for a regulation or other compliance-related demand? Unfortunately, it could be months or even a year before you'd realize that the security control was not functioning as intended.

Ideally, one would continuously monitor these systems and security controls. But how do you do that in today's dynamic environment, with ever-growing data stores, applications, system upgrades, and other frequently changing environmental factors? And all while dealing with motivated, persistent, and sometimes highly-skilled attackers? Obviously, a "set-it-and-forget-it" approach is destined to fail.

FEDTECH Magazine quotes the U.S. Army's Colonel Michael Jones, Deputy Director of Cyber Emerging Technologies, and an advocate for continuous monitoring, "We've always done monitoring through logs by systems administrators at various data centers, but when you have thousands of systems and logs to look through, there's only so much they can review in a particular day."[5] What's needed is not just continuous monitoring, but *automated* continuous monitoring.

## WHO CARES ABOUT CONTINUOUS MONITORING—AND WHY?

In April 2010, the U.S. Office of Management and Budget released memorandum M-10-15. This document provides guidelines to federal departments and agencies, such as the U.S. Departments of State, Justice, and Treasury, for their 2010 Federal Information Security Management Act (FISMA) reporting. The memorandum urges these agencies to "continuously monitor security-related information from across the enterprise in a manageable and actionable way."[6]

Then, in September 2010, the Federal Network Security Branch of the U.S Department of Homeland Security (DHS) issued a document entitled "Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture," or CAESARS. In effect, CAESARS mandated federal agencies to cooperate with the DHS to provide a new framework for security. CAESARS called for these agencies to look at security in a new way—one that would enable information security regardless of infrastructure or malevolent dynamics.[7]

While the net results remain to be seen, an 18-month study of an earlier risk management scoring system that is similar CAESARS has shown substantial security improvements. The system, known as iPost, was implemented at the Department of State. In fact, the improvements resulting from iPost were so noteworthy that the department won the National Security

> *"With continuous monitoring, we know where the problems are and know what we need to do. It's an enterprise approach to monitoring that's faster, better and cheaper."*
>
> **COLONEL MICHAEL JONES**
> **US ARMY**

Agency's 2009 Frank B. Rowlett award for Organizational Achievement.[8] These findings validate the wisdom of moving toward continuous monitoring. A risk management scoring system such as CAESARS or iPost is viewed as a prerequisite for changing security management from isolated, point-in-time assessments to active, continuous security.

Clearly CAESARS and iPost are designed to provide a framework that agencies can use to quantify risk and measure their security posture—and improve that posture over time. Isn't this the goal of common commercial security practices like the Payment Card Industry Data Security Standard (PCI DSS)? If so, commercial entities should take advantage of the improved security posture provided by the continuous monitoring strategies used in US Federal environments.

## WHAT TYPES OF SOLUTIONS HELP WITH CONTINUOUS MONITORING?

Security professionals need a solution that tells them what changed, who changed it, the ramifications of the change, and the quickest path back to a known secure state when a change introduces risk. Depending on the setting, they may also need a solution that eases the burden of NIST 800-53 requirements for FISMA compliance and enables visibility into the state of security through dashboards and user-customizable alerts. And they need it in an enterprise-wide solution that can correlate log and security event data with change and configuration data.

Ideally, this solution would also provide a framework for integrating operational solutions such as patch management and network management tools with security tools such as change management, configuration management, log monitoring, SIEM, risk management and vulnerability scanning solutions.

Such a solution could discover vulnerabilities by correlating suspicious configuration changes and troublesome security events, automatically remediating detected vulnerabilities to a known and secure state. And it would do this all continuously—not just periodically—through automation. By integrating change and event information, it would also provide ongoing system integrity. Together, this provides enterprise-class continuous monitoring that helps manage risk.

## CONCLUSION

Balancing the demand for access to information with the requirement to protect its integrity requires an active, ongoing approach. Since information can only be deemed secure (or not secure) at the precise moment it has been examined, today's complex IT infrastructure and evolving threat landscape require new ways to continuously evaluate the organization's security posture. And change, whether from external or internal sources, and whether planned or unplanned, is the one constant that drives the need for this reliable, ongoing process. The risks introduced by this constant change demand a solution that can accommodate dynamics in an ongoing manner. "With continuous monitoring, we know where the problems are and know what we need to do. It's an enterprise approach to monitoring that's faster, better and cheaper," offers the US Army's Colonel Michael Jones. Only a solution that offers automated continuous monitoring can address these needs.

## CONTINUOUS MONITORING WITH TRIPWIRE VIA PLATFORM SOLUTIONS

### TRIPWIRE ENTERPRISE

- Continuous file integrity monitoring
- Compliance policy management
- On-demand, automated remediation of undesirable change

### TRIPWIRE LOG CENTER

- Log capture/storage of tens of thousands of events per second
- Flexible collection of logs from almost any source
- Detection of and alerting to suspicious events

1 http://www.cioinsight.com/c/a/Latest-News/Data-Growth-Now-a-FirstTier-Challenge-for-Enterprises-Gartner-Reports-273073/)

2 Internet Security Threat Report: http://www.symantec.com/business/threatreport/topic.jsp?id=threatreport&aid=notable_statistics

3 http://www.absoluteastronomy.com/topics/Faraday_cage

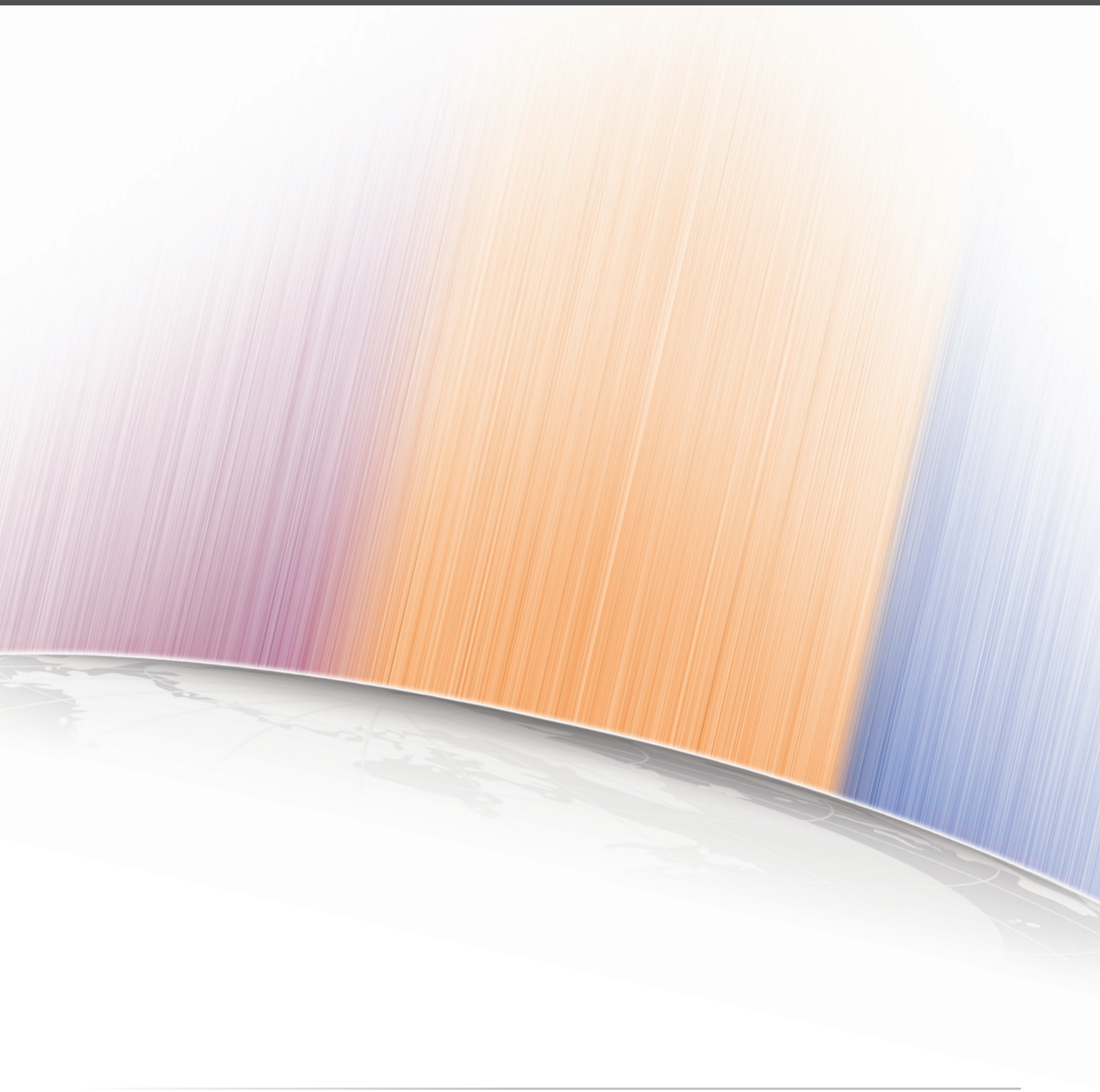
4 (Source: Risk Management Framework, NIST SP 800-37)

5 http://www.fedtechmagazine.com/article.asp?item_id=876&sv=eoa).

6 http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf

7 http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf

8 http://www.state.gov/documents/organization/156865.pdf



tripwire®
TAKE CONTROL.

.:. Tripwire is a leading global provider of IT security and compliance solutions for enterprises, government agencies and service providers who need to protect their sensitive data on critical infrastructure from breaches, vulnerabilities, and threats. Thousands of customers rely on Tripwire's critical security controls like security configuration management, file integrity monitoring, log and event management. The Tripwire® VIA™ platform of integrated controls provides unprecedented visibility and intelligence into business risk while automating complex and manual tasks, enabling organizations to better achieve continuous compliance, mitigate business risk and help ensure operational control. .:.

**LEARN MORE AT WWW.TRIPWIRE.COM OR FOLLOW US @TRIPWIREINC ON TWITTER.**



WPCM1n 201111