# Continuous Monitoring in a Virtual Environment

*By: JD Sherry, Director of Public Technology and Tom Kellermann, Vice President of Cybersecurity*

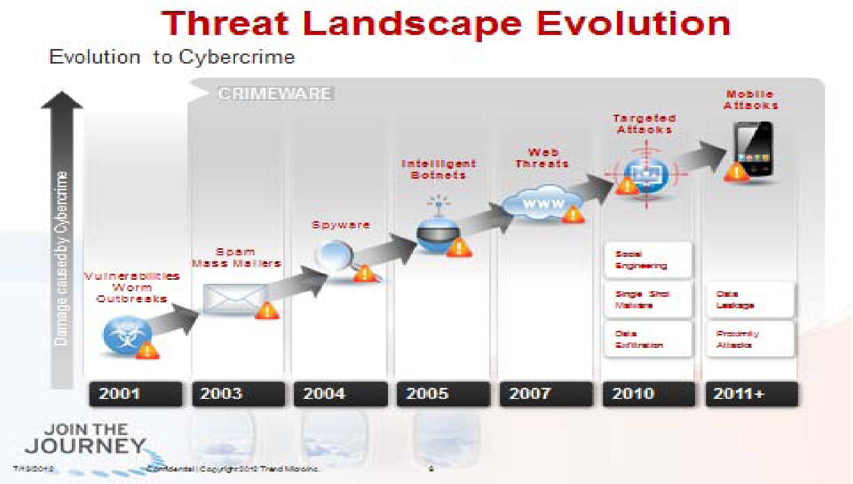
Trend Micro, Incorporated

» The future of cybersecurity will be grounded in continuous monitoring and increasing the level of our adversaries' discomfort so they no longer attack and/or remain persistent within our networks.

A Trend Micro White Paper | August 2012

## BACKGROUND

The threat landscape of 2012 is extremely sophisticated and hostile. Trend Micro's Global Threat Report (http://blog.trendmicro.com) illustrates a notable shift in the organization of cybercriminals and state actors, as well as a significant evolution of the stages of cyberintrusion.



Threat Landscape Evolution

Evolution to Cybercrime

Today's cyber criminals use a seemingly endless array of techniques to compromise and infiltrate nearly every aspect of our electronic environment.  As our daily lives and the global economy become increasingly dependent on web-based systems and interconnectivity to operate smoothly, cyber-attacks emerge to stalk us nearly every step of the way.  In fact, these attacks have grown so complex and varied that traditional IT system defenses – such as antivirus (AV) software and intrusion prevention systems (IPSs) – have been rendered obsolete.

There are specific emerging trends in today's cyber-attacks:

- Professionalization and commoditization of exploit kits. i.e. BlackHole Exploit Kit
- A high degree of modularization in more advanced malware like SpyEye and FLAME
- Increased sophistication with Traffic Direction Systems (TDS), which are used as initial landing pages, also known as "doorway pages," which direct traffic to content
- Ransomware
- New exploitation vectors introduced via HTML5
- Evolution of mobile threats
- Continued exploitation of social networks

On this last point, consumer-oriented threats seek to victimize millions of people using social networking services such as Facebook and Twitter. By taking advantage of the trust relationships formed on social networking sites, cyber criminals can steal personal data and infect massive swaths of end-point machines with botnet programs. Attackers are also using web-based connections to manipulate critical world-wide grid infrastructures or shut them down altogether.

Current cloud computing clusters allow individuals to have high performance computing at their fingertips. With a simple credit card transaction they can use the cloud to wage large-scale, brute force attacks as well as Distributed Denial of Service storms, creating serious problems for both government and commercial organizations.  These events can have personal and professional ramifications on everyone.  So how do we prepare for this new cyber world?  How do we react and defend our networks on a continuous basis? This highly complex threat matrix calls for new countermeasures to increase our defensive postures.

Continuous monitoring began with a memo sent from the President's Office of Management and Budget to all heads of U.S. executive departments and agencies. For many, continuous monitoring represented a leap forward in helping these organizations adopt the practices necessary to begin gathering enterprise-level security metrics. The directive issued from the highest levels of federal oversight has compelled organizations to aggressively ramp up their security testing practices.

Continuous monitoring is a risk management process facilitated by people and technology to ensure overall ecosystem health, integrity and quality of service.  According to NIST (National Institute of Standards and Technology) continuous monitoring has many key tenants[1]:

- Promote near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes
- Encourage the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions
- Integrate information security into the enterprise architecture and system development life cycle
- Provide emphasis on the selection, implementation, assessment, and monitoring of security controls, and the authorization of information systems
- Link risk management processes at the information system level to risk management processes at the organization level through a risk executive (function)
- Establish responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems (i.e., common controls)

[1] NIST, GUIDE FOR APPLYING THE RISK MANAGEMENT FRAMEWORK TO FEDERAL INFORMATION SYSTEMS: A SECURITY LIFE CYCLE APPROACH, SPECIAL PUBLICATION 800-37 (GAITHERSBURG, MD.: FEBRUARY 2010).

The people, process, and technology core areas are comingled within these tenants. Without question, the implementation of stronger, more robust security controls is neither trivial nor does it happen overnight.  Continuous monitoring is an evolution and one that should be done in parallel with the implementation of policy and procedure.  Completing the strategy consists of partnering with companies that have invested millions of dollars in research and development to protect your best interests and secure your workloads. With an experienced partner, your efforts can focus on automation and embedding security into your organization’s operating system and ecosystem.  If the enemy is going to shift the playing field, we must be prepared to shift the end zone by implementing calculated countermeasures.

## WHERE TO START?

Data and asset categorization are critical for any organization.  These can be accomplished at a very high level to establish a baseline or with a more sophisticated and granular approach, which is required for highly complex government operations.  Once a data and asset categorization policy is defined and incorporated into an organization’s security management program, it can then be ingrained into its software and systems lifecycles.  This allows organizations to create a continuous monitoring fabric supported by calculated measurements, which map to risks against the information security posture.  Security profiles can be designed to incorporate information assets with risk/relevancy ranking assignments.  Therefore, when events occur to those respective systems and security profiles, real-time situation awareness is demonstrated and acted upon according to their risk/relevancy rank.

Information technology and cloud ecosystems are rapidly evolving and changing.  Deployment of information assets happens within minutes.  If poor configuration and unpatched assets become too difficult to manage because they aren’t being embedded completely into the systems development/release lifecycle, data exfiltration can also take place in minutes.  “Instant on” protection and continuous monitoring is achieved by managing security profiles for both data and assets.

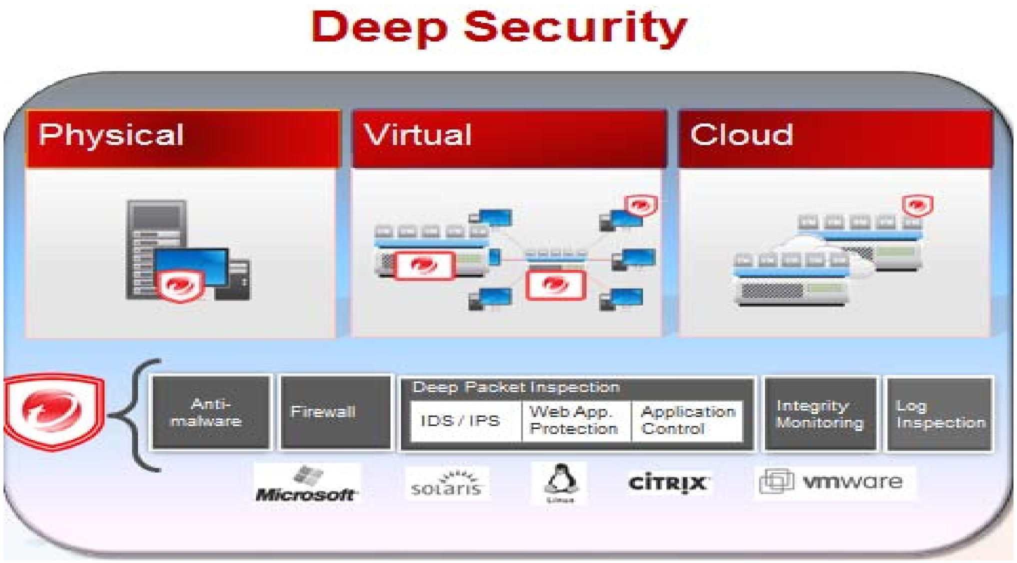
## RISK RANKING

With a data classification policy established, implementation of technologies that conveniently facilitate the categorization of assets into security and risk profiles is essential.  Assigning asset values allows computers and events to be filtered by risk importance. The risk profile then determines how security events are alerted and managed. When a rule is triggered on an asset, the severity values of the rules are multiplied by the asset value of the device. This risk score is used to rank events in order of importance. It also enables a calculated response to react, review, and remediate the risk, closing the loop of continuous monitoring.

Leveraging a risk ranking system is necessary to quantify the importance of security events and "see the forest through the trees." Rules are assigned a "Severity Level" (high, medium, low, etc.), and assets are assigned an "Asset Importance" level. Information assets should also be grouped into logical security profiles to more efficiently manage the entire IT environment.

The ranking system provides a way to quantify the importance of events. By assigning asset values to resources, and assigning severity or risk values to rules, the importance/rank of an event is calculated by multiplying the two values together. This allows you to filter security events by rank and relevance.

## KEY TECHNOLOGY VARIABLES



### Security Feedback Loop

Information sharing is key to continuous monitoring. Organizations that leverage continuous communication between technology assets and cutting edge threat research centers and technologies gain valuable information that can prepare them for attacks. Closed-loop security intelligence between centralized threat intelligence ecosystems and information assets allows for the foundation of a continuous improvement strategy.

As the threat landscape evolves, inputs from key security events can be analyzed, probabilities of concern ranked, and action can be taken to address concerns. Response to these global risk rankings is disseminated to the organization's assets, where the logical security profiles of the computing environment are prepared to remediate and prevent future attacks against "zero hour" vulnerabilities.

Reducing the threat cycle time down as much as possible requires a smart feedback loop where large amounts of threat data is shared and analyzed in real time. This interconnection enables Internet speed for identifying, analyzing, and stopping new threats – a level of responsiveness that addresses the thousands of new threats and threat variants daily. To improve their continuous monitoring and patch management strategy, organizations should leverage partnerships and technologies that have demonstrated world-class threat intelligence capabilities.

## Deep Packet Inspection/Host Intrusion Prevention System

Deep Packet Inspection (DPI) is the latest security technology that allows for visibility into many of the layers of the the Open Systems Inspection (OSI) model.  DPI technologies most often enable views into Layer 2-7 and help defend against traditional attacks as well as complicated Advanced Persistent Threats (APT's).  APTs are highly complex and target mainly web vulnerabilities and unpatched platforms via SQL injection techniques.  These attacks go undetected when continuous monitoring strategies and technologies like DPI/HIPS are not deployed across the organization.  It is essential to have a Host Intrusion Prevention System (HIPS) enabling self-defending assets for even greater protection compared with the traditional approach to outside-in information security protocols.

Vulnerabilities for custom or COTS applications may not be immediately addressable with a patch.  With integrated DPI/HIPS capability, you can create virtual patches/shields against your security profiles and assets to defend within hours of vulnerability acknowledgement. Additionally, as assets move from private cloud computing environments to public cloud ecosystems, you can extend your HIPS strategy and manage those security profiles across all platforms for consistent threat protection.

Virtualization and cloud environments create even greater challenges for traditional networking intrusion prevention systems.  It is important to implement a technology solution that can thoroughly analyze the virtual switches used in many of the leading virtualization technology hypervisors.  It is also important that the analysis does not significantly degrade performance across the computing infrastructure.  With virtualization and multi-tenancy, it is critical that HIPS technology views ALL traffic.  Agentless architecture is most definitely preferred.

## Integrity Monitoring

Integrity monitoring allows you to monitor specific elements on a computer for changes.
To monitor for changes, it is critical to create a "gold" standard and baseline profile for device classification.  The baseline establishes the appropriate standard for installed software, running services, processes, files, directories, listening ports, registry keys, and registry values. With standards in place, continuous monitoring is embedded and facilitates the alert and remediation process.

Integrity monitoring functions by performing a baseline scan of the elements on the computer specified in the assigned rules. The monitor periodically rescans those elements to look for variances that fall out of tolerance.

Organizations should look to partner with vendors that have industry standard, predefined rules to assist your continuous monitoring efforts.  Once assets are deployed into security profiles, they will be automatically analyzed against the baseline.  Ultimately, alerts from the platform are based on the aforementioned asset risk ranking protocol to eliminate noise within your continuous monitoring process.  As a result, you'll have better intelligence to react to and remediate alerts as they occur within your IT environments.

Performance is an important consideration –and adding another software agent will definitely impact performance.  To alleviate performance issues, look for technology solutions that integrate into the hypervisor to conduct critical aspects of continuous monitoring.

## Log Inspection

An integrated platform focused on continuous monitoring and functional compliance should consist of world-class malware protection, deep packet inspection, integrity monitoring, and log inspection.  Threat vectors are focused at the web and application tiers, which produce a tremendous amount of logs, can be too overwhelming to analyze, react and mitigate once miscreants target your environments. However, not paying attention to the logs is NOT an option.

Often organizations will leverage Security Information and Event Management (SIEM) systems to implement a centralized logging strategy.  Timely and ongoing log analysis is a huge pillar for the success of any continuous monitoring strategy.  A centralized logging strategy is typically based on several factors.  For example, the sheer amount of devices that organizations currently support is exponential, versus three to five years ago.  Virtualization technologies engineered to facilitate integration and migration to cloud computing platforms have caused this paradigm shift.  That being said, the number of devices that network, security and system administrators have to review for integrity are far too great for them to keep pace on a day-to-day basis.  The ratios simply are too large.

Log inspection and correlation is at the core of scaling your response to targeted attacks and continuous monitoring of your computing assets.  Technology platforms that simplify a cohesive log collection, protection, and inspection/remediation approach are of the utmost importance. Compliance for most sensitive data processing within the private or government sector relies on a solid log management process and technology solution set.

To streamline the log inspection process and support continuous monitoring, organizations should look for solutions that bundle the management of these capabilities into a single platform. A single platform allows you to more efficiently and continuously manage resources, react to security events, and defend your critical infrastructures across physical, virtual and cloud environments.

## CONCLUSION

As organizations continue to adopt mobile devices and a “Cloud First”/FedRAMP approach, we must be aware of new and emerging risks and stay committed to finding new methods to better protect our digital ecosystems. To tap into the power of web-based, mobile, and virtualization – and build stouter virtual castles in the sky – we must appreciate the evolution of blended threats from the simple virus of yesteryear to the virulent malware and organized cyber campaigns of 2012 and beyond.

For more information, visit http://blog.trendmicro.com

The stages of cyberintrusion dictates that we must also build dungeons within those castles. Rather than endorsing security models that drive us to construct additional defenses and filters that have an increasingly slim chance of stopping advanced threats, the focus within IT development and security must shift to emphasize more aggressive and proactive self-assessment. In other words, “offense can inform defense.”  Continuous monitoring is the first step in addressing the use of intelligent metrics to empower greater cyber-situational awareness within our government agencies. It represents a significant bridge between military-type assessment programs, civilian standards, and risk assessment paradigms.

The future of cybersecurity will be grounded in continuous monitoring and increasing the level of our adversaries’ discomfort so they no longer attack and/or remain persistent within our networks.

Trend Micro has developed a layered security platform that provides defense in depth and continuous monitoring of both traditional and virtual infrastructure: Deep Security.
To learn more, visit http://www.trendmicro.com/us/enterprise/cloud-solutions/deep-security/index.html

TREND MICRO™
Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site: www.trendmicro.com.

TREND MICRO INC.
U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax:+1408.257.2003

www.trendmicro.com.