

Technology Brief

New Demands for Real-time Threat Management

Date: June 2011 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: *Many organizations are evaluating a new security model based upon IT risk management best practices. This is a good idea, but not enough for today's dynamic and malevolent threat landscape. To keep up with IT changes and external threats, large organizations need to embrace two new security practices: Real-time Risk Management for day-to-day security adjustments and Real-time Threat Management to detect and remediate sophisticated, stealthy, and damaging security breaches (i.e., Advanced Persistent Threats or APTs).*

Overview

Enterprise security management has undergone a series of profound changes over the past few years. Circa 2005, information security became inexorably linked to government and industry regulations like FISMA, HIPAA, GLBA, and PCI DSS. During this timeframe, security management was driven by one objective: passing compliance audits. Once organizations established processes and controls for these audits, they simply moved on to making these activities more efficient.

Somewhere around 2009, CISOs came to an alarming conclusion as they realized that passing security audits created a ton of work for security staff but this effort didn't necessarily equate to strong security. In fact, many CISOs working in the U.S. federal government observed that their agencies were spending inordinate amounts of time and money preparing for FISMA audits while experiencing a growing number of security incidents.

Clearly, security management focus on regulatory compliance was no longer enough. This led to a second security management transition from a regulatory compliance focus to one of IT risk management.

With IT risk management, threats and vulnerabilities are assessed on an asset-by-asset basis. Risk management decisions are then made depending upon an IT asset's level of exposure (e.g., threats and vulnerabilities) as well as its value (e.g., the relative significance each asset delivers in overall business operations). Armed with these metrics, organizations can make qualitative and quantitative risk management decisions such as risk acceptance, risk assignment or transfer (e.g., transferring potential risk to a third party such as an insurance company) or risk reduction (e.g., mitigating risk by implementing security controls, policies, and procedures). In this case, a control is defined as a mechanism used to restrain, regulate, or reduce vulnerabilities.

The Rise of Real-time Risk Management

IT risk management is a step in the right direction because it is based upon thorough IT assessments, established metrics, and intelligent cooperative decisions among business, security, and IT executives. Given today's dynamic threat landscape and constantly changing IT infrastructure, CISOs must go beyond periodic assessments and basic practices and embrace sound risk management practices designed to deal with their dynamic environments. ESG calls this advanced practice "Real-time Risk Management" (RTRM). RTRM is based upon:

- **Instantaneous threat and vulnerability knowledge.** The ever-changing nature of both IT and the threat landscape demand that asset changes, vulnerability assessments, and threat data must be available in real-time. Security tools must correlate this information and immediately report on new types or levels of risks. Security practitioners must be trained to digest these inputs, present them to business managers, and expedite risk management mitigation without delay.
- **Comprehensive visibility and coverage.** IT is made up of a multitude of assets like hardware devices, databases, business applications, and virtual appliances all interacting with one another. It is no longer enough to understand a sub-segment of the entire IT portfolio alone or adopt a piecemeal view of the entire

IT infrastructure through a potpourri of tools; to keep up with assets and their associated vulnerabilities, CIOs need consistent data, visibility, and alerts across the entire IT spectrum.

- **Constant controls assessment and adjustment.** Security controls don't fit into the "set-it-and-forget-it" category. Rather, controls need persistent assessment to ensure they adequately address new or changing risks.

Building on an RTRM Foundation

As the name suggests, real-time risk management is dedicated to providing CISOs with up-to-the-minute security information so they can analyze the current status of their environment, detect malicious activities as quickly as possible, and minimize damage. RTRM must be extremely flexible in order to provide security executives with granular intelligence about new and evolving threats at all times, but this is easier said than done. Why? The latest extremely sophisticated, stealthy, targeted attacks (often referred to as Advanced Persistent Threats, or APTs) are purposefully designed to avoid exposure. For example, APTs use "social engineering" tactics to fool users into downloading seemingly harmless files chock full of malware. APT malware is often propagated through trusted channels with hackers assuming familiar identities such as Facebook "friends." Once installed, APT malware silently gathers user names and passwords, covertly scans network address spaces, and slowly penetrates other systems on the network. After weeks or months of these activities, distant hackers usually find something of value like credit card numbers, software source code, or other types of intellectual property. Finally, the APT malware receives clandestine command-and-control instructions to copy precious data files, encrypt them, and send them to remote hacker-controlled drop servers.

New Threats Demand Real-Time Threat Management

Do APTs render real-time risk management obsolete? Not at all. The objective of real-time risk management is to proactively "harden" IT assets, protecting them from all types of attacks including APTs. For example, APTs may persuade organizations to turn on advanced features in endpoint security software or more closely monitor activities around copying and storing sensitive data. Unfortunately this is no longer enough. Recently, security breaches at organizations such as Google, Lockheed Martin, and RSA Security demonstrate that APTs demand security adjustments and new defenses.

Dealing with APTs demands a philosophical change within organizations. While risk management and incident preventions should remain top priorities, CISOs, CIOs, and executive managers should work under the assumption that their organizations will be compromised. This means that RTRM must be complemented with the right processes and tools for emergency response—like getting support from executive management, establishing a team, developing and communicating emergency response processes, and testing emergency response effectiveness.¹

Remember that the primary objective of any emergency response effort is fairly simple: minimize the impact of a security attack. To achieve this goal, large organizations need to be able to detect sophisticated targeted attacks as quickly as possible. This begs an obvious question: How can the security team detect these attacks when APTs are designed for undetectable "low-and-slow" attacks?

ESG believes that defending against APT-like attacks is difficult, but not impossible. To accomplish this, RTRM must be aligned with a new complementary service: Real-time Threat Management (RTTM). RTTM goes beyond basic situational awareness about vulnerabilities and traditional malware threats. Rather, it looks at network behavior across a multitude of devices looking for anomalous traffic patterns, connections, and flows within the corporate network and at network ingress/egress points. When real-time threat management detects suspicious content or network activities, it can automatically take immediate preventative actions such as quarantining malicious files and executables, blocking command-and-control traffic, or automatically "cleaning" infected endpoints. To accomplish these goals, RTTM depends upon:

¹ The CERT Coordination Center provides a good set of emergency guidelines at <http://www.cert.org/csirts/Creating-A-CSIRT.html>.

- **Improved network monitoring.** Real-time threat management goes beyond inspection of network logs and flow data alone. How? By looking at network traffic up to the application layer with special attention given to packet payloads, protocols, destination addresses, and APT communications patterns.
- **Event detection designed for sophisticated threats.** RTTM is designed with APTs in mind, carrying specific filtering rules and correlation engines. Network traffic is analyzed in multitude of ways, looking for specific behavior that may be indicative of a sophisticated threat.
- **Immediate remediation and policy enforcement.** Once an organization has discovered the presence of a sophisticated threat, it is often too late—sensitive data has already been stolen. Given this type of exposure, RTTM MUST go beyond detection to hands-on prevention and remediation. When RTTM detects command-and-control communications or other malicious traffic, it begins a sequence of alerting and remediation events. For example, RTTM can alert security staff and automatically remediate infected systems. Based upon an organization’s security and business policies, RTTM may also take proactive in-line actions like updating perimeter security device rules or isolating infected systems.
- **Network intelligence services.** Since APTs constantly mutate and evolve, RTTM must be equally as agile. To remain current, tools must be backed up with leading-edge actionable security research and new enforcement rules. The goal here is to match hacker brain power and tricks with a superior force of white hats and PhDs.

Trend Micro Threat Management System

While existing security defenses like firewalls, IDS/IPS, and endpoint security tools can be tuned to better address advanced threats, RTTM technologies should be viewed as an effective supplemental layer of defense against attackers seeking customer data, intellectual property, or highly sensitive internal documents. Many security vendors are exploiting APT fears to sell existing products that offer little incremental protection; others have developed specific new solutions that truly can make a difference. [Trend Micro’s](#) Threat Management System (TMS) is just such a product.

TMS provides an architectural approach to APT detection, remediation, and reporting. The solution consists of:

- **Threat Discovery Appliance.** A network-based out-of-band device that monitors network traffic, behavior, and protocols and is designed and tuned for sophisticated attack detection.
- **Threat Mitigator.** A network-resident system that provides automated real-time remediation (clean-up) of endpoint malware infections identified by the Threat Discovery Appliance.
- **Dynamic Threat Analysis System.** A malware identification and analysis platform that uses sandboxing and other advanced methods to provide detection, detailed exploration, simulation, and full forensic analysis of suspected malware captured by TMS or submitted directly by a security specialist.
- **Threat Management Portal.** A hosted or on-premises dashboard providing visibility, analysis, alarms, and multi-level reporting of threat activity and root cause analysis including source IP address, point of network entry, and details about malware characteristics.

For organizations that need further assistance identifying and reacting to advanced threats, Trend Micro backs TMS with its risk management services offering. Customers who choose this option are provided with ongoing help with threat analysis and alerts, risk posture, proactive monitoring, and strategic security planning. This service offering leverages Trend’s threat analyst expertise and Smart Protection Network intelligence, a cloud-based infrastructure powered by a global network of threat sensors.

What makes Trend Micro TMS more effective at detecting APTs than an IDS/IPS, next-generation firewall, or other network analyzer? Malware generally plays a key role in APT and advanced attacks. TMS focuses on detecting malware and the traces of its activity with specialized threat detection engines and event correlation that is continually updated with new threat relevance rules.

TMS uses an array of specialized threat engines that include signature-based scanning, document exploit examination, heuristic behavior-based analysis, reputation-based ratings, sandboxing, and more. Packets, streams, and full sessions are analyzed at layers 2-7 for real-time detection, and then later undergo an additional layer of correlation analysis to discover “low and slow” and other evasive activities discernable only over an extended period. The high detection rate

coupled with deep forensic analysis tools can clearly help reduce the risk of initial APT intrusion and speed discovery and containment of any actual attack.

The Bigger Truth

An evolutionary cycle is happening in enterprise security. Large organizations are moving beyond compliance-centric security and beginning to embrace an IT risk management approach focused on threats, vulnerabilities, and asset value. This is a sound foundation, but today's dynamic threat landscape demands a flexible risk management model that can keep up with constant change.

Real-time risk management provides a foundation for keeping up with changes to assets, networks, and vulnerabilities. With the onset of sophisticated APT-like attacks, real-time risk management now requires a sister service, real-time threat management. RTTM essentially expands the scope of RTRM with specific threat intelligence, detection, and remediation capabilities. The goal? React immediately to new types of threats to prevent or minimize damages.

Trend Micro Threat Management System is a good example of a RTTM solution. Built and deployed as an architecture, TMS detects and blocks APT malware, detects and remediates stealthy behavior associated with a sophisticated attack in progress, and offers the security team specific intelligence associated with sophisticated threats and anomalous network behavior. Given these capabilities, enterprise organizations should evaluate TMS capabilities to see if it is a fit for their environments. Organizations with strong security skills may find that TMS provides an effective security layer for defense-in-depth and firms with security skill deficits may find that TMS products and Trend Micro services can replace or augment existing security controls while supplementing internal security knowledge.