Technology Brief

New Demands for Real-time Threat Management

Date: February 2012 **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 related 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 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 environments, 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 RTRM obsolete? Not at all. The objective of RTRM 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 examines 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:

- **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.

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

- **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 Deep Discovery

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 Deep Discovery is just such a product.

Deep Discovery focuses on detecting APTs and targeted attacks by indentifying malicious content, communications, and behavior across the stages of an attack sequence. Through detection and in-depth analysis of both advanced malware and evasive attacker behavior, the product provides the enterprise with a new level of visibility and intelligence to combat attacks. Key product attributes are:

- Deep Discovery detection based on multiple threat engines, sandboxing, event correlation, and intelligence from the Trend Micro Smart Protection Network and dedicated threat research teams
- A Deep Discovery Management Console that provides real-time threat visibility and analysis to allow security professionals to focus on the most severe risks, perform deep forensic analysis, and access the latest threat profile and containment information
- Integration with leading SIEM platforms, including HP ArcSight and IBM Q1 Labs, to provide SIEM customers with enterprise-wide threat detection based on network intelligence combined with the full range of events collected and analyzed by SIEM

For organizations that need further assistance identifying and reacting to advanced threats, Trend Micro backs Deep Discovery 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 also 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 Deep Discovery more effective at detecting ATPs than an IDS/IPS, next-generation firewall, or other network analyzers? Advanced malware and direct attacker manipulations are both used in APT and advanced attacks. Deep Discovery focuses on detecting that advanced malware and the traces of its activity, as well as malicious attacker activity, with specialized threat detection engines and event correlation continually updated with new threat relevance rules.

Deep Discovery uses a three-level detection scheme to perform initial detection, then simulation and correlation, and ultimately a final cross-correlation to discover "low and slow" and other evasive activities discernable only over an extended period. The result is a high detection rate, low false positives, and in-depth incident reporting information designed to speed the containment of an attack.

The Bigger Truth

An evolutionary cycle is occurring 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 damage.

Trend Micro Deep Discovery is a good example of a RTTM solution. Deep Discovery detects APT malware and 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 Deep Discovery's capabilities to see if it is a fit for their environments. Organizations with strong security skills may find that it provides an effective security layer for defense-in-depth, and firms with security skill deficits may find that Deep Discovery and Trend Micro services can replace or augment existing security controls while supplementing internal security knowledge.