SOLARWINDS WHITEPAPER

IT Security Management Checklist

9 Key Recommendations to Keep Your Network Safe

Share:

solarwinds
Unexpected Simplicity™

Table of Contents

As we move ahead into 2013, we find more businesses preparing for new network threats and phenomena such as '*hacktivism*.' Identifying the right areas to improve security measures, employee training, and gearing up with the right technology is the key to success for IT security teams. In addition to the pressing demand for enhanced IT security, regulatory compliance is another business pressure of concern.

The gateway to new technology adoption also opens up the window for newer security incidents, or *zero-day* attacks. In addition, in 2013 organizations are likely to see more of private and hybrid cloud implementation, software-defined data center consolidation, bring your own device (BYOD), big data, HTML5, IPv6, and more. It's time to get prepared!

One great way to be prepared is to create a comprehensive IT security management checklist. Creating a comprehensive checklist will ensure that you are following the best practices for IT security. Below are 9 recommendations on how to set up your checklist.

Recommendation #1 — Log and Event Management

✓ Ensure that you have the right SIEM software in place for log collection, analysis, real-time correlation and automated response.

Does your organization have the technology to aggregate and correlate logs from multiple sources in real time? Logs may not be problem-solvers by themselves, but they are a substantial means to monitor problem occurrence, analyze the root cause, and then take corrective measures. All devices on the enterprise network have the ability to generate event logs. The wise option is to use the log data available to correlate and process them in real time for diagnosing and troubleshooting security issues.

Security Information and Event Management (SIEM) systems are the best solution for comprehensive log management. By being able to automate responsive actions in time of security incidents, IT security teams can ensure that many significant threats are prevented as, and when, they occur. Many IT security software and appliances on the enterprise network are vulnerable to malicious use and unauthorized access. Some of these include:

- Intrusion detection/prevention system
- Antivirus software
- Firewalls, routers and other network devices
- VPN, secure gateways and file transfer servers
- Application servers, Web servers, database servers
- Operating systems, virtual machines, and physical workstations serving as user end-points

Monitoring event logs from each of these entities is critical from an IT security standpoint.

SIEM tools—as a solution to address log management and IT security—integrate with your security appliances and help you interpret the circumstance of activities that are non-compliant with your organizational security policies. These tools can help you:

- Aggregate and analyze the event logs in real time
- Correlate the log instance with other network events
- Produce a meaningful and timely diagnosis for immediate threat prevention or remediation
- Provide automated responses following security best practices

Recommendation #2 — Firewall Security Management

✓ Ensure you have a firewall management system in place that can help manage your firewall activities to strengthen IT security and at the same time, support regulatory compliance.

Firewalls—being the gateway in and out of the secure enterprise network—will always remain an organization's primary network defense. Not paying heed to firewall security management is as good as welcoming network threats into the organization. Viruses, malware, application backdoors, email-bombs, redirect attacks, and DoS are some among the increasing and inventive hacking malpractices that are lurking around.

A Gartner research note from November 28, 2012 stated that "Through 2018, more than 95% of firewall breaches will be caused by firewall misconfigurations, not firewall flaws."

Firewall management is a critical but demanding activity that includes:

- Building and modifying firewall rulesets and managing them constantly to cover IT security rules and organizational Web access policies
- Testing the firewall rulesets before deploying them into the IT environment
- Cleaning up unnecessary and redundant firewall rules and objects
- Tracking and managing all firewall changes that are happening across the network
- Conducting periodic security audits to identify critical hosts exposed to dangerous services

Firewall management gets deeper and more technical as we go down to analyze the packet flow through the network and identify where blocks are—whether caused by network devices or by a wrong rule definition. With all these activities going on to ensure intact ***firewall security***, it's not as easy as just having rules executed. The wiser approach is to simulate the functions of the defined rules and objects on a test environment to assess their efficacy before executing them in your live network.

It's not a question of whether or not to have robust firewall management in place. In today's multi-vendor environment, the real question is *which* tool is going to enable your security admins to manage firewall rules, set IT security norms, and ensure compliance with federal and organizational policies most effectively.

Recommendation #3 — Network Change & Configuration Management

✓ Automate network configuration management to protect your network from security threats, maintain compliance, and avoid costly downtime.

Most network administrators would agree that the majority of network problems they experience can be traced back to a device configuration change, which typically falls under one of these three categories:

- Incorrect config change—due to manual errors
- Unauthorized config change—could be a mistaken change or security breach
- Non-compliant config change—deviated from organizational policies

Such changes, as evidenced by some well-publicized network disasters, can lead to a myriad of network problems—from exposure to dangerous security risks, to legal penalties for non-compliance, to costly business downtime.

So how can these potentially disastrous problems be avoided? The solution is simple—manage network configuration well. But how?

- Create standards based on IT security and user access policies.
- Implement standards through network administration teams.
- Enforce standards through continuous monitoring and auditing.
- Validate standards through ongoing data analysis.
- Maintain standards through regular reviews.

Obviously, these activities are difficult to implement manually, even in an SMB network. And, considering these ***network configuration and change management*** (NCCM) tasks are on-going, the only effective way to accomplish this is by automating the process.

	Top 5 Reasons to Automate NCCM	Benefit
1.	Automate real-time alerting when met with unauthorized and non-compliant config changes. Know when and where changes have been made, and by whom.	Quicker network troubleshooting and improved security.
2.	Automation gives you the power to perform deeper analysis of config data. You can archive config and backup history to deep-dive into config changes and policy violations.	Improved network forensics; historical config change data available any time for analysis.
3.	Automating NCCM also incorporates the automation of compliance reporting.	Ensure federal and internal corporate policies are complied with efficiently.
4.	Execution of bulk config changes is made easy with NCCM automation. Especially in a heterogeneous environment where thousands of device configs can be scheduled for bulk and uniform change.	Eliminate effort to change individual device configuration by standardizing config process.
5.	Automating NCCM allows you to schedule periodic network configuration scans to get a holistic view of all the changes in configuration and device settings.	Manual effort eliminated, time saved, and NCCM process optimized.

Remember, network configuration management is a daily operational activity, not a one-time task. As such, it's imperative to have the right standards and policies in place AND the right tools to enforce and maintain those standards—not just for increased network availability and performance, but for enhanced security and compliance.

Recommendation #4 — Endpoint Vulnerability Management

✓ Ensure you are equipped with centralized and automated patch manager software for comprehensive endpoint vulnerability management and compliance.

Workstations, as we have seen from so many security incidents in the past, are easy targets for hackers. We know many of the reasons: weak passwords, unencrypted hard drives, malware infection from the Web, and another important piece of the puzzle—"missing patches," including security patches that are out-of-date.

With the increasing number of new viruses and malware that plague workstations and servers, keeping your security software and system applications patches up-to-date is the most appropriate and secure option. What is needed as an IT security solution is pre-emptive system administration with reliable and fail-safe ***patch management***.

Proactive patch management calls for:

- Comprehensive audit trail of software on end-user workstations
- Customizable mass deployment options to patch applications uniformly
- Compliance reports that show the status of patched and unpatched desktops, servers, and VMs
- Automated scheduling of patch jobs to avoid manual errors and omissions

Leaving workstations and servers unpatched only increases their susceptibility to both internal and external incursion not just into a single endpoint but the enterprise network as a whole.

Recommendation #5 — Endpoint Data Loss Prevention

✓ Safeguard your corporate data from endpoint data loss and the introduction of malware with the appropriate USB detection and prevention system.

Endpoint data-loss prevention is an IT security mechanism that enables organizations to mitigate the risk of unintentional disclosure of confidential information from endpoints. One of the sources of endpoint data loss made famous by movies and TV is via USB drives. USBs are also notorious for their capability to spread malware. Let's face the facts:

- Owing to its compact size, there's a high possibility of your corporate data walking right through your door if endpoints are not protected from USB data theft.
- Not all organizations can deny every employee from connecting a USB stick to their workstation; It's required by some staff for valid business purposes.

The more effective way for IT security teams to deal with this internal threat is to institute an effective ***USB defender technology*** that can:

- Protect data and applications with real-time notifications when USB devices are detected
- Automatically disable user accounts, quarantine workstations, and reject USB devices

"Java was responsible for 50 percent of all cyberattacks last year in which hackers broke into computers by exploiting software bugs"

Kaspersky Lab

Security Information & Event Management (SIEM) systems are the best solution here as they have the technology to automate preventative actions to respond to endpoint data loss prevention threats in real time.

Recommendation #6 — Internet Data Security

✓ Ensure your email servers and file transfer servers are supporting (if not requiring) secure protocols, lockouts, and integration with AV/DLP, and that all components are being monitored by your SIEM solution.

Every organization uses email servers to exchange information with the outside world. Many also use ***file transfer servers*** using protocols as diverse as FTP, SFTP, and WebDAV. All of these "edge" servers need to be specially protected and monitored because they are the primary means for data and potentially malicious files to enter or leave your network.

Protections that should be implemented on these servers include:

- IP and user-level lockouts to defend against brute-force attacks from the Internet
- Secure protocols (e.g., SMTP with TLS, SFTP with SSH, or FTPS with TLS/SSL) to prevent unauthorized capture of credentials and data
- Anti-virus (AV) and data loss protection (DLP) software to prevent malicious use and the unauthorized passage of overly sensitive data
- Full logging of all connection, authentication, and data transfer activity to allow SIEM systems and NOC management to do their jobs

SIEM systems can be effective in monitoring in your edge servers, but only if logs have been enabled in your software, and your SIEM system and agents have been configured to collect and interpret them.

Recommendation #7 — Network Traffic Monitoring for Endpoints

✓ Monitor network traffic across your network to check for users connecting to insecure domains and websites.

Network traffic passing through workstations and other endpoints such as employee-owned personal devices (BYOD) is also a major area to be constantly monitored. This will ensure users are not getting into unsafe domains and websites that could, in turn, cause havoc by opening the company up to Web-based malware, spear fishing, or credential harvesting attacks.

With objectifying statistics from the recent Verizon 2012 Data Breach Investigations Report (DBIR)—a study conducted by the Verizon RISK Team with cooperation from various police and cybercrime handling organizations across the globe—it has been estimated that there have been a startling 855 incidents of data breach and 174 million compromised records.

Recommendation #8 — WLAN Monitoring

✓ Make sure to choose the right network monitoring software that supports both thin and thick access points and their associated clients for WLAN monitoring and rogue access point detection.

A rogue access point (AP) is a wireless access point that has gained access to a secure enterprise network without explicit authorization from the network administration team. This could be a standalone (aka thick) or controller-based (aka thin) access point. Unauthorized APs that could potentially open wireless backdoors into wired networks include:

- Unauthorized APs that exist in and around the airspace of your corporate firewall.
- Wi-Fi devices from employees who connect personal devices to the corporate WLAN and APs from neighboring concerns that may be accessible to your network because of proximity. These may not look potentially malicious but still they are unsecured and may turn out to be security threats later on.
- Rogue APs that pose potential security threats and by infringing into your corporate network.

While all of these malicious and non-malicious access points need to be monitored, it is the responsibility of the network administrator to ensure the malicious ones are contained and eliminated.

Network management software that extends capabilities to monitor the health and performance of all your network devices can also help identify rogue APs in your multi-vendor network environment by scanning wireless controllers and devices.

Recommendation #9 — User & Device Tracking

✓ Be prepared with a security system that helps recognize user connections to switch ports and identify unauthorized devices.

Network ***user and device tracking*** is becoming increasingly important to track and monitor which user connects to which switch port or Wi-Fi access points. Tracking and monitoring occurs by mapping the username and MAC address with the port number or SSID. For both wired and wireless devices, IT security and network administration teams must constantly be able to know:

- Which user and device connected to which port and when
- Historical data of users' connections to ports and Wi-Fi access points
- If an unauthorized or rogue device shows up on the network

IT Security Checklist

This checklist will help guide you in creating a comprehensive IT security plan. These crucial aspects of IT security management cannot afford to be missed. IT security preparedness is all about getting equipped with the right tools for the right problem at the right time. Threats are on the way.

Below, you can review each checklist item along with SolarWinds product recommendations that will ensure you're ready to take on comprehensive IT security management.

Recommendation #1 — Log and Event Management

✓ Ensure that you have the right SIEM software in place for log collection, analysis, real-time correlation and automated response.

SolarWinds Product Recommendation: Log & Event Manager

Recommendation #2 — Firewall Security Management

✓ Ensure you have a firewall management system in place that can help manage your firewall activities to strengthen IT security and at the same time, support regulatory compliance.

SolarWinds Product Recommendation: **Firewall Security Manager**

Recommendation #3 — Network Change & Config Management

✓ Automate network configuration management to protect your network from security threats, maintain compliance, and avoid costly downtime.

SolarWinds Product Recommendation: Network Configuration Manager

Recommendation #4 — Endpoint Vulnerability Management

✓ Ensure you are equipped with centralized and automated patch manager software for comprehensive endpoint vulnerability management and compliance.

SolarWinds Product Recommendation: Patch Manager

Recommendation #5 — Endpoint Data Loss Prevention

✓ Safeguard your corporate data from endpoint data loss and the introduction of malware with the appropriate USB detection and prevention system.

SolarWinds Product Recommendation: Log & Event Manager

Recommendation #6 — Internet Data Security

✓ Ensure your email servers and file transfer servers are supporting (if not requiring) secure protocols, lockouts, and integration with AV/DLP, and that all components are being monitored by your SIEM solution.

SolarWinds Product Recommendation: Serv-U FTP Server

Recommendation #7 — Network Traffic Monitoring for Endpoints

✓ Monitor network traffic across your network to check for users connecting to insecure domains and websites.

SolarWinds Product Recommendation: Network Traffic Analyzer

Recommendation #8 — WLAN Monitoring

✓ Make sure to choose the right network monitoring software that supports both thin and thick access points and their associated clients for WLAN monitoring and rogue access point detection.

SolarWinds Product Recommendation: Network Performance Monitor

Recommendation #9 — User & Device Tracking

✓ Be prepared with a security system that helps watch out for user connections to switch ports and identify unauthorized devices.

SolarWinds Product Recommendation: User Device Tracker

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide - from Fortune 500 enterprises to small businesses. The company works to put its users first and remove the obstacles that have become "status quo" in traditional enterprise software. SolarWinds products are downloadable, easy to use and maintain, and provide the power, scale, and flexibility needed to address users' management priorities. SolarWinds' online user community, http://thwack.com, is a gathering-place where tens of thousands of IT pros solve problems, share technology, and participate in product development for all of the company's products. Learn more today at ***http://www.solarwinds.com***.

For additional information, please contact **SolarWinds** at 866.530.8100 or e-mail ***sales@solarwinds.com***.

To locate an international reseller near you, visit ***http://www.solarwinds.com/partners/reseller_locator.aspx***