Interested in learning more about security?

SANS Institute InfoSec Reading Room

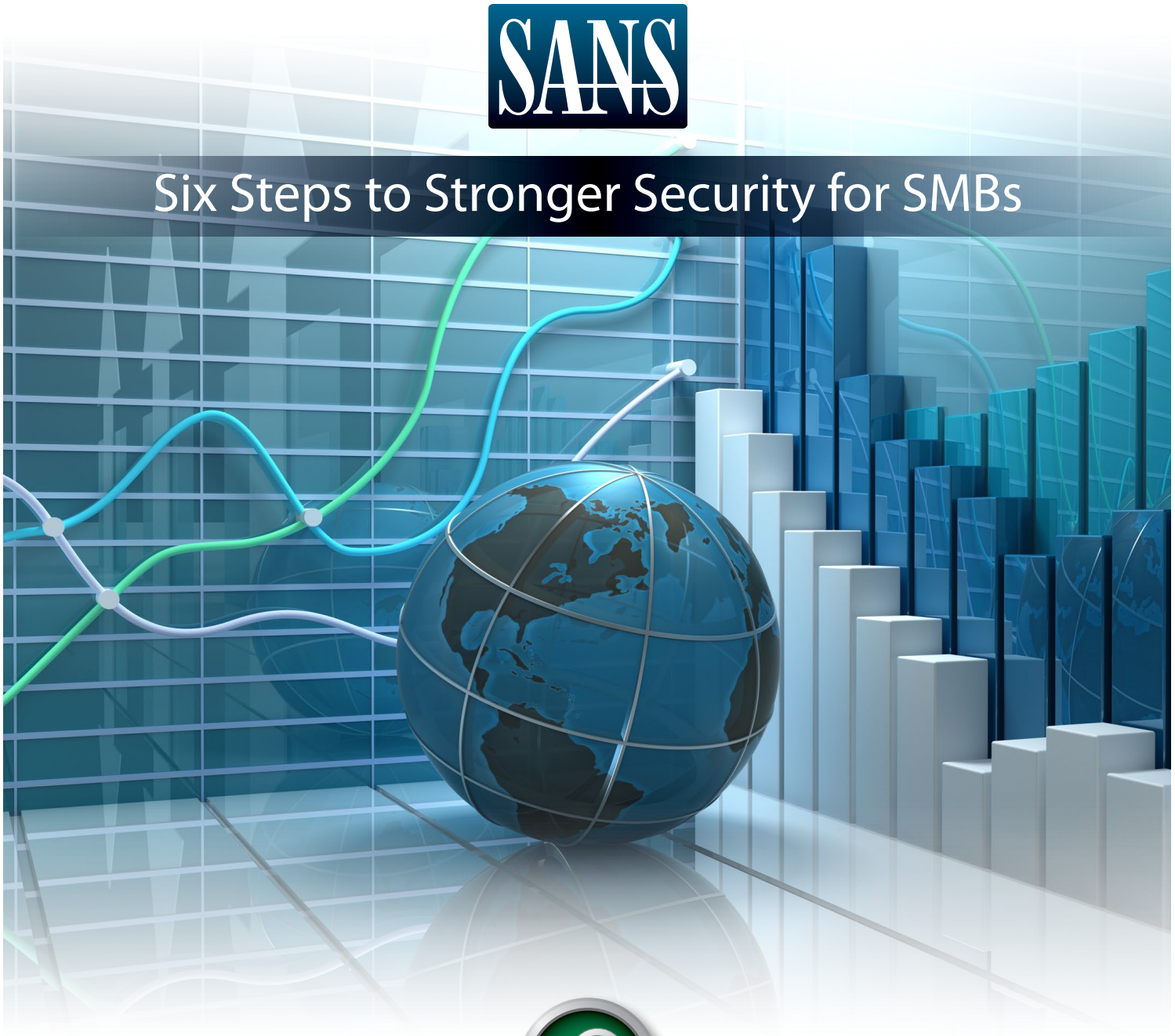
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Six Steps to Stronger Security for SMBs

An Analyst Program whitepaper by Dr. Eric Cole. It describes a six-step approach that small and medium-size businesses can use as a template for enhancing their overall security posture.

Copyright SANS Institute

Author Retains Full Rights



Six Steps to Stronger Security for SMBs

A SANS Whitepaper

Written by Eric Cole, PhD

June 2015

Sponsored by
Qualys

©2015 SANS™ Institute

Getting Started

Attackers target companies of all sizes; no matter how obscure you think you may be, you should expect to be eventually attacked. Big companies devote lots of money and staff to fighting attacks—and even then, breaches still occur far too often. Small to medium-size businesses (SMBs) face a tougher challenge. Your security budget is tiny by comparison. As for the security "team"—well, often it's just one or two people on the battle line. Because you must do more with less, it's crucial to be smart about defensive choices and focus on what matters most: Six Steps to Stronger Security.

Six Steps to Stronger Security

1. **Keep an accurate hardware inventory**
2. **Keep an accurate software inventory**
3. **Actively manage configurations**
4. **Remediate vulnerabilities quickly**
5. **Automate endpoint defenses**
6. **Control administrative access**

Stakeholders in the security industry provide many resources to solve this challenge. The problem for SMBs is lack of time and resources to sift through and apply all of the advice, so the Six Steps strategy focuses on the most likely threats, to fix the vulnerabilities that will cause the biggest impact to your organization.

Going for Quick Wins

When your security team and budget is small, you won't be able to do everything told by the experts. Think of your challenge as fighting a guerrilla war. As a guerrilla warrior, you can be highly effective with pinpoint application of security controls that give you quick wins. Always seek quick wins for your efforts. Here are four things you can do right away to shut down a huge percentage of potential attacks:

- **Whitelist applications.** Use a network application that allows launching only of approved applications. This limits the risk of damage caused by users who click on a Trojan embedded in an email phishing attack or from another attack vector.
- **Use standard configurations.** These ensure secure settings for workstations, laptops and other devices and avoid vulnerabilities created by mistakes in configurations.
- **Patch quickly.** Apply system and application patches within 48 hours for critical systems to eliminate potential attacks.
- **Control administrative privileges.** Make sure administrative privileges are inactive when using email or web browsers.

The Six Steps to Stronger Security can be easier and less expensive to implement than you might think. The rest of this guide will help you identify the highest-risk areas in order to focus your remediation efforts for strong security.

Step One: Keep an Accurate Hardware Inventory

Begin by creating an accurate hardware inventory. It's impossible to protect assets you don't know you have. This hardware inventory—when combined with an associated software inventory and managed configurations—will be the foundation for all of your other security efforts. Look for cost-effective tools that can easily perform this task. For example, many vulnerability scanners can automatically build and maintain an accurate asset inventory database that covers hardware and software.

Keep It Simple

Use the least number of tools to accomplish as many steps as possible. When done correctly, one may be able to address the first four steps outlined in this paper with a single tool that provides integrated results. This is critical for SMBs because they have limited budgets, which means they have limited tools. Few SMBs will be able to solve the problem by writing a check, but using one tool, in an integrated manner, can improve the scalability of device identification for resource-challenged entities.

The hardware inventory is essential to a solid network-based defense. Knowing which devices are authorized and which are not is vital for security because unknown devices are often conduits for an attack. It's important to inventory *all* devices on your network, whether it is a server, client, printer, switch or other device, and without regard to its ownership. This includes smartphones, tablets or notebook computers that employees use to access corporate resources. The inventory should also include point-of-sale terminals if your company is a retailer; this will help you comply with PCI requirements for protecting cardholder data.

It's vital that your hardware inventory be continuously updated. Vulnerabilities are constantly changing, and your scanner will need an accurate inventory to correctly assess the risks of a breach. Automation will help you achieve an accurate inventory without requiring any manual effort. With automation, your inventory will update when a device appears on the network.

If you can invest in hardware inventory software, look for tools that automate inventory management and asset tagging, while easily identifying, categorizing and managing assets. Such tools should automatically discover unknown devices and enable dynamic selection of assets for scanning or reporting. The main idea of automation is to require your personal engagement only when there is a problem.

Your tool for automating hardware inventory should do the following:

- Identify all unauthorized devices, as well as authorized devices.
- Scan on a regular basis to identify rogue devices.
- Integrate the hardware inventory database with software and configuration records.
- List *all* networked devices, including routers, switches and firewalls.
- Implement 802.1X (when supported by hardware and where appropriate) to allow only authorized devices on wireless as well as wired networks.

The first four items on this list are imperative for a meaningful hardware inventory.

Step Two: Keep an Accurate Software Inventory

Software is as critical to inventory as hardware because it's usually the point of compromise. Attackers exploit vulnerabilities in software that open the door to control of hardware. The goal is to identify the software required on a given system and permit use only of that software. A natural starting point is to scan existing systems to identify what is installed. A good vulnerability scanning tool can do this.

Consider implementing a labeling scheme that includes categories of systems (e.g., infrastructure servers, engineering workstations and business laptops) and creating a list of allowed software for each category. Your tool will automatically trigger an alarm when a user tries to install any software that is not on the approved list. Be sure to keep detailed logs of failed installations because such failures can be early indicators that someone is trying to compromise a system. Most attackers need to install software (usually disguised as a legitimate application or service) to set up launching points on the network for the next phase of an attack to cripple operational systems or breach sensitive data.

Your software inventory tool should do the following:

- Create a list of all authorized software.
- Scan on a regular basis to identify any unauthorized software.
- Integrate the software inventory database with hardware and configuration inventories.
- List software on *all* devices (e.g., network hardware, as well as endpoints).
- Implement application whitelisting to prevent unauthorized software from execution or installation.
- Check logs for failed software installations that could indicate an attack.

As with hardware inventory tools, the first four items are imperative for a useful software inventory.

Step Three: Actively Manage Configurations

Understanding and controlling device configurations is a key component of overall security. Improper configurations—whether deliberate or accidental—can trigger vulnerabilities. That's why developing and actively managing secure configuration baselines for all devices will help create stronger security. A tool for controlling these will enforce the use of authorized configurations and block unauthorized changes.

All changes to configurations should go through a standard change control process. Although such processes have some manual aspects, you can automate most of this with the help of a comprehensive asset database. Regular scanning will detect all configuration changes. If a change is unauthorized, the tool will generate an alert.

A tool for active management of configurations should do the following:

- Create a secure configuration for all devices.
- Scan on a regular basis to identify any unauthorized configuration changes.
- Integrate the configuration database with hardware and software inventories.
- Ensure that configurations are tracked for network hardware, as well as endpoints.
- Implement integrity checks and security templates to alert of and/or prevent unauthorized configuration changes.
- Implement a robust change control process in which all changes are reviewed before being applied to production systems.

The first five items on this list are must-haves for meaningful configuration monitoring.

Step Four: Remediate Vulnerabilities Quickly

Vulnerabilities are the gateways for attacks. New vulnerabilities turn up continuously, and it is critical that you identify them with scanning and fix them in a timely manner. The main idea about remediation is to reduce your network's attack surface and minimize the points where a criminal might create a breach.

The quickest way to reduce your attack surface is to close unneeded services and protocol ports. If you don't need them now, shut them down immediately. Remediation also entails fixing bad configurations, including version control of OSes and applications. That process that should occur automatically as described in Step Three.

Patching is the other major component of remediation. Patching is an onerous manual process without automation. Because quick patching of vulnerabilities is vital, you should use an automated tool to speed this process. Most OSes have free and automated patching tools, although the manageability of those tools varies. For that reason, look into using a robust tool that will automate all of your patching requirements.

Note that you should patch *all* software, even when it is disabled, and apply all available patches to any newly installed or re-enabled service.

A tool for active management of configurations should do the following:

- Run vulnerability scans on a regular basis to identify any anomalies.
- Categorize known vulnerabilities based on a risk-rating scheme.
- Utilize threat intelligence services to rate risks against active, real-world attacks.
- Remove any services not needed and close any protocol ports that are not required.
- Patch any services installed on the system, whether enabled or not.

Effective vulnerability remediation requires all of those.

Step Five: Automate Endpoint Defenses

Criminals often target endpoints, so protecting your network must include an endpoint security suite. Tools should include antivirus, endpoint protection, intrusion prevention and a personal firewall. In addition, your tool should block incoming executables while controlling and limiting the use of HTML content embedded in email. Email—through attachments and web links embedded in the body of a message—is a common point of compromise.

Here are five configuration tips for automating your endpoint protection:

- Enable OS auto-update features on each device so equipped.
- Turn on Windows AppLocker, and give no users admin privileges.
- Consider the use of a managed security service provider (MSSP) to manage and/or monitor next-generation firewalls or unified threat management appliances. Either of those can automatically provide network-based anti-malware protection.
- Implement cloud-based web security gateway services to limit inbound web malware and keep users (especially mobile users) away from dangerous websites.
- Take advantage of ISP offerings that block DNS resolution to known bad sites, or look at free and/or inexpensive services.

Getting started with automated protection can be as easy as configuring the anti-malware features in existing antivirus tools. If possible, configure these to send any alerts or events to your log server(s), then carefully review these logs for signs of system compromise and respond promptly. It's a good idea to review logs from critical assets every day. Also, ensure you configure malware defenses to check for regular updates and push those out to all protected devices.

When considering standalone anti-malware products or evaluating the anti-malware components within antivirus software, features to look for include the following:

- Ease of management and reporting (to promote visibility into the security landscape).
- Protection against zero-day attacks (to defend against currently undefined threats).
- Low overhead (to preserve application performance).
- Automation features enabled by default to minimize your learning curve.

A typical checklist for automating your defenses includes the following:

- Run an updated endpoint security software suite that automatically scans all critical files.
- Harden a system to turn off auto-run and auto-executable content.
- Scan executable attachments, run them in a sandbox and, if malicious, block them.
- Limit embedded HTML email content.

The first two items on this list are imperative for effective automation of defensive efforts.

Step Six: Control Administrative Access

The most damaging component of malicious code is the ability to run as the system administrator. If a system is infected but the damage can be controlled, the attack's impact is manageable. However, if malicious code has full administrative access, the damage can be extreme. Limiting and controlling administrative access is thus critical to security. In many SMBs, several people often have unnecessary administrative access. That's one of the most risky situations. You must monitor such access and control accounts holding administrative privileges. It is especially important to do the following:

- Inventory every account with elevated access, and review whether it is needed.
- Withdraw administrative privileges when someone leaves the organization or a person's job role changes.
- Encourage administrators to use different passwords for different types of systems, and enforce requirements that administrators use frequently changed, complex passwords.
- Find and disable default accounts on workstations and servers that attackers can easily penetrate.

A checklist for controlling administrative access includes the following:

- Audit and track anyone who has administrative access.
- Administrators should always log in with the access rights of an ordinary user and use privileged access only when necessary.
- Forbid the use of email or web browsers when logged in as a user with administrative access.
- Use complex and robust passwords.
- Use cloud-based multifactor authentication if possible.

Beware the challenge that privileged users often are unconvinced they are part of the problem. They may push back and say these rules shouldn't apply to them. Be firm to ensure controls are applied as appropriate.

Conclusion

Security does not have to be difficult or expensive for organizations using a risk-based approach to security. This paper provides actionable controls you can implement to increase security in a cost-effective manner by targeting well-known risk areas from the start. The most important points to consider:

- Automation is critical. Limited resources will always be a problem, so minimize manual efforts and use more automation.
- Prioritize by focusing on the areas that will provide quick wins with the best return.
- Risk-based security will ensure that the highest risk items are addressed first.
- Develop metrics to track compliance and identify gaps in security that need to be addressed.

By performing proper analysis and focusing on high-risk areas, SMBs that have limited budgets can still create strong security. Using the Six Steps will help you implement effective security that reduces risk.

About the Author

Eric Cole, PhD, is a SANS Faculty Fellow, course author and instructor who has served as CTO of McAfee and chief scientist at Lockheed Martin. He is credited on more than 20 patents, sits on several executive advisory boards and is a member of the President's Commission on Cyber Security. Eric's books include *Advanced Persistent Threat*, *Hackers Beware*, *Hiding in Plain Site*, *Network Security Bible* and *Insider Threat*. As founder of Secure Anchor Consulting, Eric puts his 20+ years of hands-on security experience to work to help customers build dynamic defenses against advanced threats.

Sponsor

SANS would like to thank its sponsor:

QUALYS®
CONTINUOUS SECURITY

Last Updated: April 21st, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Blue Team Summit & Training 2018	Louisville, KYUS	Apr 23, 2018 - Apr 30, 2018	Live Event
SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS Doha 2018	Doha, QA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
SANS Amsterdam May 2018	Amsterdam, NL	May 28, 2018 - Jun 02, 2018	Live Event
SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SEC487: Open-Source Intel Beta Two	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
Cloud INsecurity Summit - Washington DC	Crystal City, VAUS	Jun 08, 2018 - Jun 08, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
Cloud INsecurity Summit - Austin	Austin, TXUS	Jun 11, 2018 - Jun 11, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Cyber Defence Canberra 2018	Canberra, AU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, MY	Jul 16, 2018 - Jul 21, 2018	Live Event
SANS Seattle Spring 2018	OnlineWAUS	Apr 23, 2018 - Apr 28, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced