# Defend Your Organization from Cyber-Thieves

## Don’t Be the Next Target

accelops

## Table of Contents

# Defend Your Organization from Cyber-Thieves: Don't Be the Next Target

In December 2013, just weeks before the year-end holidays, it was discovered that criminals hacked their way into the financial systems of Target, the well-known retail chain. Cyber-thieves gained access to approximately 40 million credit and debit card accounts and got away with the personal and financial information of up to 70 million shoppers. Target acknowledged that the criminals appeared to have first entered its system in early November, more than a month before company investigators became aware that an infringement had occurred.

The massive security breach, which could be one of the largest in U.S. retail history, has put Target in a tailspin. The company faces a number of government investigations and more than 80 lawsuits. Target incurred $61 million in costs associated directly with the incident, and when the dust settles, the total expense to the company is estimated to reach between $500 million and $1 billion — and that's on top of any sales lost as a result of customers avoiding its stores after the breach. Indeed, Target experienced a 46 percent drop in profits in the fourth quarter of 2013 and continues to experience weaker than expected sales. The company acknowledges that the greatest risk it faces is the negative impact on its reputation and loss of confidence of its customers. Target's CEO lost his job as a result of the incident.

***Headline news stories confirm concerns of researchers who warn that the risks of cyber-attack are growing.***

## Organizations under Attack

Target's data breach is one of several data thefts that have come to light in recent months. In March 2014, Michaels, the nation's largest arts and crafts chain, suffered a similar breach; criminals targeted payment systems and point-of-sale machines and gained access to credit/debit card account information of nearly 3 million customers. At Neiman Marcus, hackers raided 1.1 million customer accounts in a data breach that continued unnoticed in the company's computers for more than eight months. Meanwhile, AOL disclosed in April 2014 that it is investigating a security incident involving unauthorized access to a "significant number" of user accounts, and Microsoft discovered a flaw in Internet Explorer that prompted the U.S. Department of Homeland Security to issue an advisory warning businesses not to use the browser because cyber-attacks could "lead to the complete compromise of an affected system."

## Cyber Risks on the Rise

News stories confirm concerns of researchers who have been warning that the risks of cyber-attack are growing. According to a 2013 study conducted by Technology Business Research,[1] the number of cyber-attacks is on the rise, as is the cleverness and sophistication of the attacks. Criminals are focusing their efforts primarily on large organizations, but researchers say that breaches are occurring more frequently for organizations of all sizes and across all markets and industries. The study uncovered that nearly half (46 percent) of the organizations participating believe that they were targeted by cyber-attacks more frequently in 2013 compared to 2012 -- 18 percent said that breach attempts were significantly more frequent. Organizations in aerospace and defense, manufacturing, construction and transportation

reported the greatest increase. However, consumer-related industries also report increasingly sophisticated and frequent attacks.

## SANS Top 20 Critical Security Controls

Security professionals face the challenge of staying ahead of the rising rate of attacks and the increasing sophistication with which they occur. Organizations must design and adopt ever more advanced threat protection solutions and strategies that leverage new technologies and approaches to detect and block attacks. But with all of the available solutions and approaches from which to choose, how do you know which one will work best for you?

One way is to implement the SANS Top 20 Critical Security Controls in your IT security evaluation and planning. The SANS Institute is the largest cooperative research and education organization for information security training, certification and research. The SANS Top 20 lists essential security controls that help define and guide strategies and solutions for effective cyber-defense. It is a valuable checklist that security and IT managers can use to evaluate how systems and strategies address major threats and vulnerabilities. The SANS Top 20 Critical Security Controls have become an accepted standard for developing security controls and functions that are effective against the latest cyber-threats.

## Meeting the Demands of the SANS Top 20 Critical Security Controls

The SANS Top 20 Critical Security Controls are a valuable structure upon which to build your organization's readiness to counter cyber-attacks, but it can be difficult to meet the demands of all 20 controls without holistic command over the environment. As the high-profile breaches at companies such as Target and Neiman Marcus demonstrate, even organizations with advanced security systems and adequate staffing find it difficult, if not impossible, to effectively fend off cyber-criminals without processes to control the discovery and management of security blind spots.

AccelOps is a virtual appliance that employs an automated discovery-driven approach that shortens the path to comprehensive IT monitoring and prevents future security blind spots. Customers have found that AccelOps is the most effective and comprehensive solution available to address the SANS Top 20 Critical Security Controls criteria and benefit from an advanced security monitoring platform that analyzes and automates the discovery of advanced cyber-threats and attacks. AccelOps allows security professionals and system administrators to implement and manage more inclusive and complete cyber-threat strategies across their entire organization, whether on-premise or in the cloud.

Here's how AccelOps approaches 17 of the SANS Top 20 Critical Security Controls.

# Managing the SANS Critical Security Controls

## SANS Critical Security Control 1: Inventory of Authorized and Unauthorized Devices

*The processes and tools used to track/control/prevent/correct network access by devices (computers, network components, printers, anything with IP addresses) based on an asset inventory of which devices are allowed to connect to the network.*

Criminals and cyber-attackers use sophisticated systems that continuously scan corporate networks for new and unprotected devices attached to the network. A variety of devices are subject to attack – everything from desktop computers and laptops, to routers, switches and firewalls, and a host of components and systems that utilize an IP address. This includes a growing number of mobile and tablet devices as well, and as more and more employees bring personal devices into the work environment and connect them to the network, the risks of cyber-attack become even more pressing. Criminals look to "hitch a ride" and exploit opportunities to install backdoor systems or malware. Even systems that are connected to a private network, without visibility from the Internet, can still be the target of an advanced adversary.

**Automated Discovery Enables Whitelists**

AccelOps automates the discovery of all hardware devices on the network. Whitelists can be created from the results of a discovery. The system actively monitors all the devices on your network and sends an alert if any unauthorized or unmanaged device attempts to gain access or exhibit any unusual behavior. Violations are flagged for immediate security review. The systems whitelist also grows dynamically to include devices that are added to the domain as part of an ongoing authorized process -- a mobile device that is authenticated, for example. All new and approved devices are automatically updated, eliminating a common gap in security. AccelOps continually monitors the environment, and any computer or device that is not part of the domain is automatically flagged as a suspect device and placed in a watch list. Any request for a DHCP address from a device that does not match your naming convention is flagged and placed in a watch list and rules monitor those devices for unusual behavior.

## SANS Critical Security Control 2: Inventory of Authorized and Unauthorized Software

*The processes and tools organizations use to track/control/prevent/correct installation and execution of software on computers based on an asset inventory of approved software.*

Computer attackers deploy a number of tactics that are designed to take advantage of poorly managed software. This includes scanning address spaces for software that can be remotely exploited and introducing malware through hyperlinks, file attachments and other methods that are designed to enter your network, gain access to a vulnerable system, and take long-term control. Many attackers install backdoor programs, "bots" and zero-day exploits that take advantage of previously unknown vulnerabilities for which no patch has yet been released by the software vendor. Once a single machine has been exploited, attackers often use it as a staging point, quickly turning one compromised machine into many.

**Automatically Inventory All Software on Your Network**

Organizations cannot properly secure their assets without proper knowledge of the software deployed throughout the enterprise. AccelOps provides the ability to automatically inventory which programs are installed and allowed (e.g., a whitelist) and which programs are known to present a threat (e.g., a watch list). This is done in part by virtue of AccelOps' automated analysis of networked computers and devices, since poorly controlled computers and devices are more likely to be running software that is unauthorized and have a higher potential to present potential security risk from malware and other cyber-attacks. AccelOps automatically inventories and tracks all software on your network and sends an immediate alert if it detects any unauthorized software or lack of security patch so security and network administrators can take immediate further action.

## SANS Critical Security Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

*The processes and tools organizations use to track/control/prevent/correct security weaknesses in the configurations of the hardware and software of mobile devices, laptops, workstations and servers based on a formal configuration management and change control process.*

Once criminals compromise a computer network, they use sophisticated attack programs to constantly search for systems that were configured with vulnerabilities they can exploit. For example, default configurations that are designed to make installation and deployment easy are rarely optimized for security and leave a number of extraneous services that are exploitable in their default state. Software that is installed as-is from manufacturers and resellers is also highly vulnerable to exploitation. Even seemingly innocuous software updates can introduce unknown weaknesses into a software configuration that make it newly vulnerable to zero-day exploits.

**Configurations Must Be Continually Managed**

To combat this threat, security professionals must establish and ensure the use of standard and secure configurations across the many devices and systems throughout their enterprise. This is a harrowingly difficult task that requires the analysis of potentially hundreds or thousands of devices, systems and addresses. Even after configurations are in place, they must be continually managed and monitored to ensure that new security vulnerabilities are addressed.

AccelOps changes all that with automated tools that inventory the configurations of all hardware and software attached to your network. AccelOps continually monitors the environment and provides security professionals and network administrators with the ability to implement a comprehensive configuration management and change control process that works to prevent attackers from exploiting vulnerable services and settings.

## SANS Critical Security Control 4: Continuous Vulnerability Assessment and Remediation

*The processes and tools used to detect/prevent/correct security vulnerabilities in the devices that are listed and approved in the asset inventory database.*

Today's cybersecurity must always be a forward-looking activity. Security professionals must continually and actively address the cyber-threat associated with a constant stream of new software versions, security patches and a variety of threat advisories. Cyber-criminals are also aware of these developments -- perhaps more aware – and are poised to take advantage of potential gaps between attention and remediation. Indeed, when a new vulnerability is discovered and reported by researchers, hackers often race to deploy an attack before developers can find a fix. Clearly, organizations that do not actively scan for vulnerabilities and proactively address discovered flaws face significantly higher likelihood of a damaging security breach.

**Automated Monitoring for Security Vulnerabilities**

Understanding and managing new and evolving security vulnerabilities takes time, resources and expertise, especially when scaled across an entire enterprise. AccelOps provides an automated system that continually monitors the vulnerabilities found by your vulnerability tools and audits from your logs based on prioritized lists of the most urgent and developing vulnerabilities on devices are documented in the configuration management database with severity level from 1 to 10 (10 being the highest). Assessments can be tied directly to intelligence services and databases that ensure activities are based on the most current and relevant warnings. AccelOps can feed patch management and software update tools that verify that the potential threats were successfully addressed and helps shorten the delay between the discovery and remediation of new vulnerabilities.

AccelOps is an effective tool to continuously assess and take action on new information, and to quickly identify vulnerabilities and minimize the window of opportunity for attackers.

## SANS Critical Security Control 5: Malware Defenses

*The processes and tools used to detect/prevent/correct installation and execution of malicious software on all devices.*

Malicious software, or malware, is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware can enter a system in a number of ways, including through email attachments, webpages and user devices. Malware includes computer viruses, worms, Trojan horses, spyware, and a growing variety of other malicious programs. The malicious code may tamper with the system's contents, capture sensitive data, and spread to other systems. It may even disable anti-virus and spyware tools running on the targeted systems to allow further cyber-attacks to take place. In the case of the high-profile data breach at Target, sophisticated malware was used that was previously unknown to investigators and analysts.

**Monitor for Malware**

AccelOps provides an automated platform that continually monitors all computers and devices on the network for malware. Each is dynamically monitored against a database of known malware threats that is continually updated through a subscription update service. In this way, the most current and emerging

threats are known and included. The system also uses a set of advanced behavioral rules -–– based on the way that malware works – that are designed to immediately notify administrators of potential malware threats. By virtue of automated discovery, AccelOps helps administrators more effectively understand and control the installation, spread and execution of malicious code at multiple points in the enterprise, while optimizing the use of additional automation tools to enable rapid updating of defense, data gathering and corrective action.

## SANS Critical Security Control 6: Application Software Security

*The processes and tools organizations use to detect/prevent/correct security weaknesses in the development and acquisition of software applications.*

Attacks against vulnerabilities in web-based and other application software are a top priority for cyber-criminals. The reason is that many in-house applications have coding mistakes and logic errors that increase their vulnerability to attack. Attentive hackers steal public and private information by virtue of these vulnerabilities and through a robust marketplace of tools and techniques to weaponize these vulnerabilities into full-scale attacks. Thieves inject specific exploits, including buffer overflows, SQL injection attacks, cross-site scripting, cross-site request forgery, and click-jacking of code to gain control over vulnerable machines. Both internally developed and third-party application software must be carefully and continually tested to avoid such attacks.

**Alerts for Vulnerable Software**

Through ongoing analysis, AccelOps provides greater understanding of all applications running on your system, including both in-house and third-party developed software. This helps security personnel be more fully aware of all applications and third-party software that may present a security weaknesses. AccelOps can process information from vulnerability assessment tools to flag software that is considered vulnerable to attack. Security administrators can review these incidents so they can take the appropriate action to eliminate the issue. Establishing effective software security is a complex and time-consuming activity that requires a complete enterprise-wide program. AccelOps provides a platform to monitor the results of vulnerability assessment tools to help with the security lifecycle of all in-house developed and acquired software to prevent, detect and correct security weaknesses.

## SANS Critical Security Control 7: Wireless Access Control

*The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points and wireless client systems.*

Wireless devices are a convenient and popular target for cyber-attackers looking to gain and maintain long-term access to your systems because they do not require direct physical connections. Thieves gain access from outside the physical building and bypass security perimeters by connecting wirelessly to access points inside the enterprise. The risk is high because smartphones, tablets and other wireless devices accompanying traveling employees and officials are commonly targeted for infection during air travel or in cyber-cafes. Cyber-criminals often install a backdoor entry when they are reconnected to

plant unauthorized wireless access points on the network. These remain hidden until activated at a later time, giving them unrestricted access to your internal network.

**Wireless Scanning, Detection and Discovery**

It is critical that organizations adopt and utilize wireless scanning, detection and discovery tools, as well as wireless intrusion detection systems, to protect their environment from attack. AccelOps automatically monitors the environment to detect and warn if a wireless access point comes on the network. DHCP fingerprinting detects the device and notifies AccelOps. Any access point that is not authorized generates an immediate alert. The system directly ties devices to users and authority to specific wireless access points. AccelOps helps administrators better understand and define what groups of devices or people are allowed to access the wireless network, as well as which groups of devices, data files or other assets are allowed.

## SANS Critical Security Control 10: Secure Configurations for Network Devices such as Firewalls, Routers and Switches

*The processes and tools used to track/control/prevent/correct security weaknesses in the configurations in network devices such as firewalls, routers, and switches based on formal configuration management and change control processes.*

Attackers often take advantage of the fact that network devices become less securely configured over time. Configurations change as users ask for exceptions for specific and temporary business needs. Often, that security risk is neither properly analyzed nor measured against the associated business need. And once those exceptions are deployed, they are often not removed or corrected once the business need is no longer applicable. As a result, attackers search for such vulnerabilities and use those to penetrate your defenses. Once in, criminals will redirect traffic to a malicious system masquerading as a trusted system, intercept and alter information while in transmission, and otherwise gain access to sensitive data.

**Configuration Monitoring is a Must**

AccelOps automatically inventories and monitors the configurations of all your network devices and compares those configurations to previous configurations on file. The environment is constantly monitored to evaluate what is installed and running and what is approved on any given network device. This includes firewalls, routers and switchers and any configuration not adhering to the standard prompts an immediate security alert. All revised configurations are automatically recognized and recorded in the configuration management system. AccelOps provides an automated platform to continually inventory and monitor the security configurations present in your network infrastructure to prevent attackers from exploiting vulnerable services and settings.

## SANS Critical Security Control 11: Limitation and Control of Network Ports, Protocols and Services

*The processes and tools used to track/control/prevent/correct use of ports, protocols and services on networked devices.*

Cyber-thieves are always looking for vulnerable points to attack and they often find opportunity by looking at the various network ports, protocols and services on targeted networks. These access points can be overlooked in the bigger picture of cybersecurity. Common vulnerabilities include services that are automatically installed by software packages, often without informing a user or administrator that the service has been enabled. While the installation of the main software package may be approved, these unnoticed ancillary services are often brought onboard without an established business need. Hackers look to exploit these services, often with the aim to obtain user IDs and passwords that will allow them further access.

**Track and Analyze Ports, Protocols and Services**

AccelOps ensures that only ports, protocols and services with a validated business need are allowed to run on your system. This is done against a template that is assigned to a device or groups of devices or applications, which defines the ports, protocols and services that should be seen. Anything detected that is not in the template is considered a threat and prompts an immediate alert. The system receives port information from router and firewall systems on a regular basis, allowing administrators to continually compare the environment against a known and approved baseline. Administrators then are more aware of the ports, protocols and services, thus increasing the agility of analysis and response. Using AccelOps, organizations can be more confident that the ongoing operational use of ports, protocols and services is continually tracked and analyzed for vulnerability to attack.

## SANS Critical Security Control 12: Controlled Use of Administrative Privileges

*The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

Cyber-criminals often target the misuse of administrative privileges as a primary method of attack. One way they take advantage of uncontrolled administrative privileges is when a workstation user, running as a privileged user, is fooled into opening a malicious e-mail attachment or tricked into downloading a file from a malicious website. The malevolent file delivers hidden executable code, and if the user has administrative privileges, the attacker gains further access, leaving them free to capture additional administrative passwords, steal sensitive data and establish a pivot point within the network to attack other systems. The risk is significantly higher in organizations where administrative privileges are loosely and widely distributed; the attacker has a much easier time gaining control of accounts that can act as entry points for further attack.

**Monitor Administrative Privileged Accounts**

AccelOps inventories all administrative accounts that have administrative privileges. This is done through a discovery process that tracks all events via a device, server or application that take place from that account. Any unauthorized access or activity is immediately flagged for security review and the activity log can be reviewed as needed for audit and discovery purposes. The system also monitors the age of account passwords and issues an alert if any account has not been used in a specified number of

days. Privileged account groups ensure that administrative accounts are used for system administration activities only. AccelOps automates the monitoring of administrative activities on all computers, networks and applications.

## SANS Critical Security Control 13: Boundary Defense

*The processes and tools used to detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.*

Cyber-thieves often look to exploit systems that can reach across the Internet, including perimeter networks, as well as computers and devices that pull content from the Internet through network boundaries. Architectural weaknesses found on perimeter systems, network devices and computers are used to gain initial access into an organization. From that base of operations, criminals then work to gain access deeper within the boundary to steal information and to position hackers for subsequent attacks. The risk is high between internal and external partner networks; attackers jump from one extranet to another to further exploit vulnerable systems and settings.

**Real-Time Alerts When Network Boundaries are Crossed**

AccelOps monitors the flow of information on your network so administrators can limit access only to trusted, whitelisted sites. The system immediately sends an alert if any attempted transmission is detected from a malicious IP address contained on a watch list. Since the boundary lines between networks are diminishing as a result of increased interconnectivity within and between organizations, as well as the rapid rise in deployment of wireless technologies, AccelOps automates the process to monitor the flow of traffic through network borders and enables a more dynamic and real-time process to uncover attacks and evidence of compromised machines. AccelOps gives security personnel dramatically increased ability to discover attackers who have devised methods to bypass boundary restrictions.

## SANS Critical Security Control 14: Maintenance, Monitoring and Analysis of Audit Logs

*The processes and tools used to detect/prevent/correct the use of systems and information based on audit logs of events that are considered significant or could impact the security of an organization.*

Security audit logs provide a wealth of vital information that can help protect your organization and systems from cyber-attack. However, flawed security logging and inattentive analysis allow attackers to hide their activities, often for weeks and months at a time. Even when a systems are known to have been compromised, a lack of comprehensive logging records often works to obscure the details of the attack and hide subsequent actions taken by the attackers. As a result, response to fix the breach is often too late to prevent the damage.

**Automatically Analyze Log Files**

Attackers rely on the likelihood that administrators rarely review audit records for potential threats. Breaches occur without anyone knowing that vital systems have been compromised, even though the

evidence of the attack was recorded in unexamined log files. AccelOps automates the log analysis processes of all network servers and equipment with a continual audit of the environment. Any anomalies are immediately flagged for security review. The system also includes advanced log analytic tools that allow for log aggregation and consolidation from multiple machines. Security administrators can more effectively focus on unusual activity, avoid false positives and more rapidly react to threats and anomalies. AccelOps ensures that organizations never miss events buried in audit logs that could help detect, understand and or recover from an attack.

## SANS Critical Security Control 15: Controlled Access Based on the Need to Know

*The processes and tools used to track/control/prevent/correct secure access to information according to the formal determination of which persons, computers and applications have a need and right to access information based on an approved classification.*

Cyber-thieves look for sensitive data wherever they can find it. Unfortunately, their job is often made easier because many organizations do not carefully identify and separate their most sensitive data from less sensitive, publicly available information available on their internal networks. In many environments, vetted internal users are able to gain access to all or most of the information on the network, and once that user and workstation have been compromised, attackers can access sensitive information with relatively little resistance; sensitive data is often stored on the same servers with the same level of access as far less important data.

**Set Limits on Querying and Viewing of Files**

To protect data from falling into the wrong hands, it's important that organizations identify and understand which users have access and why these users need access to sensitive systems and data. AccelOps uses an advanced role-based methodology to set limits on what users can query or view and the system regularly reviews access permissions to allow use of and access to sensitive data only where strictly necessary. Detailed audit logging monitors access based on the need-to-know principle as part of an overall data classification scheme for the organization. An immediate alert is issued when access to sensitive data appears broader than what is required for legitimate purposes. AccelOps automates the process to track and prevent access to sensitive data based unless strictly needed. This gives organizations more complete understanding of where sensitive information resides and who needs access to it.

## SANS Critical Security Control 16: Account Monitoring and Control

*The processes and tools used to track/control/prevent/correct the use of system and application accounts.*

Any large organization experiences employee turnover. Indeed, analysts predict that the average employee turnover in North America, across all industries, is expected to climb to 23 percent per year by 2018. Add to that the turnover of legitimate authorized contractors and partners, and the rate quickly rises above 30 percent. Hackers look to discover and exploit legitimate but inactive user accounts, and once a system has been compromised, they are able to impersonate legitimate users and operate

without being detected. Additionally, disgruntled former employees may log into accounts left behind available long after they have been terminated and access sensitive data for unauthorized and malicious purposes.

**Notifications of Unauthorized Account Activity**

AccelOps automates the process to manage, protect and review system and application accounts. The system sends an immediate alert and reports on any unauthorized account activity while monitoring account usage to uncover dormant accounts. If an account has not been used for a given period, such as 30 days, a notification is sent to administrators warning of the dormancy. After a longer period, such as 60 days, administrators may choose to have the account disabled and flagged for even further review. In most cases, organizations choose to invoke a process to immediately revoke access to accounts after a user leaves the organization unless documented business requirements permit an extended grace period in which departed users are allowed access. AccelOps actively monitors all system and application accounts, including their creation, use, dormancy and deletion to minimize opportunities for attackers to leverage them.

## SANS Critical Security Control 17: Data Protection

*The processes and tools used to track/control/prevent/correct data transmission and storage, based on the data's content and associated classification.*

Cyber-thieves have the ability to exfiltrate significant amounts of sensitive data from organizations of all shapes and sizes. As was the case with Target, and many other recently breached organizations, despite having advanced data security measures in place, the victims were unaware that their systems were compromised and that sensitive data was leaving their systems. This vulnerability could have been avoided if the targeted organizations actively monitored data outflows and more carefully scrutinized the movement of data across network boundaries.

**Detect Exfiltrated Data**

AccelOps detects exfiltrated data during network actions, data storage and the use of various digital endpoints. The system associates a single user or multiple users to a group, that group is then defined access to specific particular directories and or files on an end device. All access is actively monitored, including move, copy, delete, create and modify, and violations of predetermined explicit rights prompt an immediate alert and are reported to the system. AccelOps helps monitor sensitive data across an enterprise, and ensures the privacy and integrity of sensitive information.

## SANS Critical Security Control 18: Incident Response and Management

*The process and tools to make sure an organization has a properly tested plan with appropriate trained resources for dealing with any adverse events or threats of adverse events.*
*Note: This control has one or more sub-controls that must be validated manually.*

As recent news headlines show, data breaches and cyber-incidents can happen anytime, to even the most sophisticated and well-funded enterprises. It is difficult enough to defend against the rising frequency and complexity of attacks in the first place, but without an incident response plan, an organization may not discover and respond to an inevitable attack before it's too late. And once an attack is detected, without appropriate escalatory methods and procedures in place, it may be impossible to contain the damage and eradicate the attacker.

**Alerts in Real-Time**

AccelOps automates the discovery of potential threats by security personnel and administrators. Whenever an abnormality occurs or an alert is issued, the system has the ability to send an email message, an alert via SNMP-Trap or XML, or open a Help Desk ticket or run a script. This gives security administrators a better ability to establish effective escalation policies and procedures. The system passes critical discovery data to Help Desk systems that automate escalatory notifications in the event of an incident. In this way, AccelOps helps protect your organization and your information as a platform to feed critical information into an incident response infrastructure that allows you to quickly discover an attack and effectively focus on containing the damage and eliminating the attacker's presence on your network and systems.

### SANS Critical Security Control 19: Secure Network Engineering

*The process and tools used to build, update and validate a network infrastructure that can properly withstand attacks from advanced threats.*

Cyber-attacks are often designed to compromise systems and networks that are poorly designed and ineffectively monitored. Without a carefully planned and properly implemented network architecture, attackers can bypass security controls on certain systems and pivot through the network to gain further access. Attackers look for unneeded connections between systems, weak filtering and a lack of network separation.

**Comprehensive and Consistent Monitoring**

Security designers rarely get to start from scratch and build in all of the security features they might want in their systems and networks. AccelOps provides a much needed layer of capability that raises confidence that critical systems and sensitive data is being protected from attackers. Even the most sophisticated and secure systems are continually subject to new techniques and new technologies developed to defeat your organization's defenses. AccelOps, by virtue of comprehensive and consistent monitoring of the environment, helps organizations manage and react to the emergence of new threats even before they become known. With AccelOps, companies have much higher confidence that they have a network infrastructure in place that will effectively minimize risk from cyber-attacks.

## Moving Forward

As we observe throughout this paper, it is very difficult to build a network infrastructure that can withstand all attacks from advanced persistent cyber-threats. Criminals are becoming increasingly

ingenious and sophisticated, and attacks are now both more frequent and more complex. Indeed, as the high-profile data breaches at Target, Neiman Marcus, Michaels and AOL show, protecting against cyber-intrusion for organizations of all sizes is now a part of daily life and a critical part of doing business, no longer a luxury, but an absolute necessity. The question of a successful cyber-attack against an enterprise is not "if" but "when."

One way to ensure you are doing all you can to protect your organization and your sensitive data is to design and implement strategies and tactics that follow the framework provided by the SANS Top 20 Critical Security Controls.

AccelOps is the most effective and comprehensive solution available on the market today to address the SANS Top 20 Critical Security Controls criteria. Companies worldwide in virtually every industry use AccelOps to manage their security (SIEM), network performance and compliance requirements. AccelOps' virtual appliance features an automated discovery-driven approach that shortens the path to comprehensive monitoring and prevents future security blind spots. AccelOps provides unparalleled threat monitoring, prioritization and mitigation, and extends your monitoring reach across on-premise, off-premise, private, public and hybrid clouds.


2901 Tasman Dr., Suite 100
Santa Clara, CA 95054 USA
info@accelops.com
+1.408.490.0903
www.accelops.com

**FREE TRIAL DOWNLOAD**
www.accelops.com/free-trial

**Footnote:**

1. *Changing malware attack rates guide new strategies for security vendors*. April 2014. tbri.com