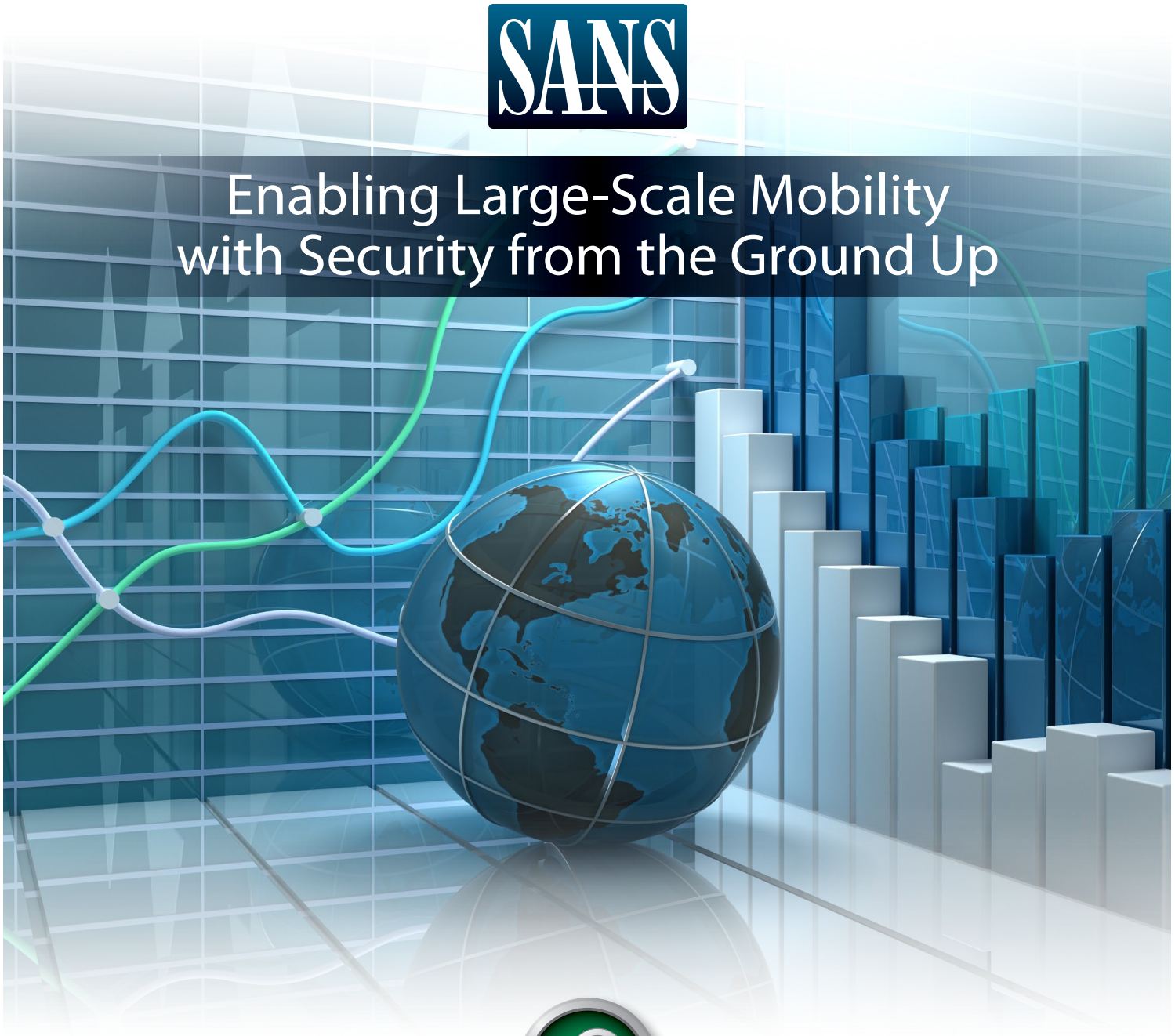
Interested in learning more about security?

SANS Institute InfoSec Reading Room

Enabling Large-Scale Mobility with Security from the Ground Up

A SANS Analyst Program whitepaper written by Jaikumar Vijayan and advised by SANS Analyst G. Mark Hardy. It discusses the state of enterprise mobility and the challenges posed to information technology groups by the massive influx of personal and corporate-owned mobile devices in the workplace in recent years.



Enabling Large-Scale Mobility with Security from the Ground Up

A SANS Whitepaper

Written by Jaikumar Vijayan

Advisor: Lee Neely

March 2015

Sponsored by
Symantec

Summary

The adoption of so-called "bring your own device" (BYOD) programs has raised new tensions between IT departments and workers over employer access to personally owned mobile devices. BYOD programs have opened the gates to a range of consumer devices in the workplace, raising concerns over data security and nonstandard access to enterprise applications and data. Meanwhile, employees using personal smartphones and tablets to access line-of-business applications have a tendency to view corporate risk management policies and security controls as restrictive, intrusive and counterproductive .

IT administrators responsible for managing BYOD strategies are under increasing pressure to accommodate user concerns over privacy and access, while implementing a risk mitigation strategy that is fully responsive to the array of threats posed by personally owned consumer devices. The challenge for organizations is to find a way to improve visibility and control over the mobile environment, while enabling the flexibility and freedom needed for users to harness the productivity and other perceived benefits of personally owned mobile technologies.

This whitepaper provides an overview of the state of enterprise mobility and the challenges posed to information technology groups by the massive influx of personal and corporate-owned mobile devices in the workplace in the past few years. Readers will get specific tips and action items to develop and implement an effective mobility management strategy.

How We Got Here

Historically, IT groups managed and controlled enterprise mobility initiatives. Organizations seeking to harness the productivity and operational efficiencies promised by mobile technologies would simply provision corporate-owned BlackBerrys or Palm Treos to the workforce and manage the devices as they did any other corporate assets.

The arrival of the first iPhone in 2007 and the first Android-powered smartphones a year later turned that model on its head. For the first time, consumers had access to technology that in many ways was more powerful, versatile and full-featured than the devices that IT departments offered. The features of these new devices, such as touch-screen keyboards, predictive-text software, web browser interfaces and access to email, social media and countless other applications, quickly transformed mobile phone use. Apple sold 5.4 million iPhones in its first year, and the company sold seven times as many devices just in the fourth quarter of 2014, illustrating the stupendous growth of the smartphone market in the intervening years.[1]

The always-on Internet connectivity offered by modern mobile devices has blurred the lines between work and play. An ever-growing number of workers bring their personal devices to work and use them to connect to enterprise applications and data, often without the IT organization's sanction or even its knowledge. Line-of-business owners have actively encouraged the BYOD trend, enamored of the prospect of their workers having "anywhere, anytime access" to the enterprise. For many companies, BYOD promises a way to boost employee productivity and connectivity with little to no capital expenditure.

By mid-2012 Gartner had begun describing the BYOD phenomenon as the "single most radical shift in the economics of client computing for businesses since PCs invaded the workplace."[2] The new devices were extremely powerful, relatively affordable, and in Gartner's opinion came with service pricing terms that often matched the best deals that an enterprise could get for its users. "An organization may better keep up with mobile technology advancements by aligning to the consumer, rather than the much slower pace of business technology adoption, with its long cycle of detailed requirements analysis, established refresh rates, and centralized procurement heritage," Gartner argued.

[1] "Global Apple iPhone sales from 3rd quarter 2007 to 1st quarter 2015"; Statista.com, retrieved Feb. 10, 2015; www.statista.com/statistics/263401/global-apple-iphone-sales-since-3rd-quarter-2007

[2] "Gartner Says Bring Your Own Device Programs Herald the Most Radical Shift in Enterprise Client Computing Since the Introduction of the PC," August 28, 2012; www.gartner.com/newsroom/id/2136615

The continuing influx of personally owned iPhones, iPads and Android smartphones and tablets in the workplace has overwhelmed IT's ability to manage them. Top-down attempts at imposing some control over the BYOD environment via acceptable-use policies, access-control strategies and mobile device management (MDM) have proved largely inadequate.

The second SANS survey of BYOD security policies and practices found in late 2013 that "despite a business commitment to adopt BYOD, organizations are concerned about the security risks associated with mobile device use." In that survey, 90 percent of respondents indicated that corporate email and intranet services were available to their BYOD workforce, while 85 percent expressed concern about the risk of BYOD to their businesses.[3]

The need for manageability and visibility and the lack of controls for mobile devices were among the top concerns the report noted:

> *Organizations are not confident in their existing policy and enforcement mechanisms for stemming the threat from mobile devices. Security controls such as VPN and mobile device network isolation remain the predominant protective mechanisms used, and fewer organizations leverage the more granular and sophisticated mobile enterprise security tools.*

One can gauge the scale of the problem by taking as an example the ScarePakage ransomware that hit Android devices in August 2014; in one 30-day period, it compromised *900,000* devices.[4]

Not surprisingly, many companies, especially in regulated sectors, have begun looking beyond BYOD at other mobile enablement strategies, including:

- Choose your own device (CYOD)
- Corporate-owned, personally enabled (COPE)
- Corporate-owned, business only (COBO)

All of these deployment options offer more granular control over mobile device use in the business compared to MDM. With the exception of COBO, these other mobile deployment strategies accommodate both personal and business use on the same device, just like a BYOD policy.

[3] "Fear and Loathing in BYOD," December 2013; www.sans.org/reading-room/whitepapers/analyst/fear-loathing-byod-34815

[4] "Android Phones Hit by 'Ransomware'," Bits Blog (The New York Times), August 22, 2014; http://bits.blogs.nytimes.com/2014/08/22/android-phones-hit-by-ransomware

Regardless of the operational model, mobile device use in the enterprise presents several risks, as shown in Figure 1.

Figure 1. Risks Associated with Mobile Devices

Let's examine these points in detail:

- **Data Leakage and Loss.** Mobile devices exacerbate the risk of data loss. A lost, misplaced or stolen smartphone or tablet can expose business-critical data and sensitive customer information. A mobile device that is not properly secured via a PIN or passcode could provide an unauthorized person with access to corporate email and other network services. Cloud-based storage and file sync-and-share applications for mobile devices are another source for data leakage. Data loss risks are especially severe for companies in regulated sectors such as health care, financial services and the energy industry.
- **Rogue Access Points.** Rogue devices can create an unsecured access point behind the firewall that attackers can use to gain unauthorized access to corporate data. This is something that can happen when employees use their mobile phones in the office with the Wi-Fi turned on and with no password to control access to it. Rogue access points can result in sensitive data being exfiltrated from the network in completely undetectable fashion.

- **Malware Infections.** Smartphones and tablets are just as susceptible to malware threats as PCs and other computing devices. Just as they have done with PCs and web applications, malware authors have developed data-stealing Trojans, keyloggers and spambots that they deliver to mobile devices via rogue emails, SMS, text messages and malicious advertisements. A study released in September 2014 by Alcatel-Lucent's Motive Security Labs (then known as Kindsight) estimated that 15 million mobile devices were infected with malware, with more than 60 percent of the infected devices running Android. The survey also found that the use of spyware on compromised devices was rising sharply: of the five "new" entries to survey's list of the 20 most frequently detected Android malware, four fell into the category of mobile spyware.[5]
- **Insecure Applications.** Poorly written third-party applications pose a security risk when used to access enterprise applications and data. Gartner estimates that more than 75 percent of mobile apps will fail basic security tests.[6] The risk is particularly high in the case of mobile devices that have been jailbroken or rooted to allow application downloads from untrusted application stores and download sites. (Third-party application stores are a common way for malware authors to deliver malicious code.) Insecure applications can allow hostile actors to take control of mobile devices to steal data or launch attacks against the corporate network and its data stores.

IT Challenges

The security and data loss risks posed by the BYOD phenomenon raise new challenges for enterprise IT groups. Unlike corporate-owned technology assets, personally owned mobile devices are subject to little direct control by IT groups. In most cases, they are not directly responsible for the hardware purchase, the OS choice or the applications installed on a personal smartphone or tablet, while upgrades and updates to OSes and applications happen on the schedule of the manufacturer, carrier or user; IT departments are often completely out of this loop. Employees across the board have proved adamant about personal device use in the workplace and have tended to resist IT attempts to impose control. Business groups and top management at many companies want BYOD and expect IT organizations to enable such use in a secure manner. By 2017, Gartner believes that half of all employers will actually require employees to bring their own devices to work.[7]

[5] "Kindsight Security Labs Malware Report – H1 2014," September 4, 2014; http://resources.alcatel-lucent.com/?cid=180437

[6] "Gartner Says More than 75 Percent of Mobile Applications will Fail Basic Security Tests Through 2015," September 14, 2014; www.gartner.com/newsroom/id/2846017

[7] "Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes," May 1, 2013; www.gartner.com/newsroom/id/2466615

The conflicting needs have presented several challenges for IT organizations. From a technology standpoint they fall into broad categories outlined in Figure 2.

Figure 2. Challenges BYOD Presents to IT Organizations

To expand on each point:

- **Device Visibility.** The massive influx of personal smartphones and tablets in the workplace has made it very hard for technology groups to monitor all the devices connecting to corporate networks and data. In order to manage a BYOD environment securely, IT departments need to have tools that offer visibility into both authorized and unauthorized devices on their networks and also the applications and services these devices are accessing on the network.
- **Device Onboarding and Access Revocation.** Organizations need to have a way to securely bring in, or onboard, new personally owned devices to the network. In order to do that, they need to implement a variety of new capabilities including remote configuration and security management of mobile devices, remote enablement of the appropriate wireless connectivity settings, remote enablement of application access and network permissions. They also need to the ability to revoke access to the network for devices that are lost, stolen or belong to employees who no longer work with the company.

- **Data Loss Prevention.** Mobile devices exacerbate risk of data loss. Organizations need a way to prevent unauthorized access to data on a misplaced, lost or stolen smartphone or tablet or a device belonging to an employee who is no longer with the company. This means having the ability to do things like remotely locking, unlocking or resetting a device and remotely wiping data on the device. Because personal devices combine business and consumer applications, organizations need a way to separate the two environments and ensure that personal use of the device does not compromise sensitive data. Because personally owned devices can create rogue access points behind the firewalls, or be used to secretly photograph or record audio or video of sensitive conversations or documents, companies need to have a way to restrict the manner in which personal devices are used in a business setting.
- **Policy Enforcement.** Organizations need a way to ensure that users of personally owned mobile devices behave in a manner consistent with usage policy. Workers who use the same device for personal and work tasks need policies for managing how the device is used to access, store and share corporate data securely. Different policies may be needed for how a personally owned smartphone or tablet accesses the Internet and cloud applications at work and how it behaves during personal use. In certain situations, workplace restrictions on devices, such as preventing camera use or restricting cut-and-paste functions, may be required as a way to protect sensitive data from unauthorized access. In some cases, organizations will have to strictly limit devices—or access via personal devices—for ultra-sensitive roles or data.
- **Secure Application Management.** Poorly designed and insecure applications pose a major security risk for organizations, so IT groups need the ability to control and manage the applications that are used to access services and data. This may involve the creation of an internal application store for enabling secure downloads of both custom and third-party applications. Securing applications also means having the ability to authenticate users, establishing controls for data sharing and implementing data encryption at the application level.
- **Threat Remediation.** The growing use of personal devices in the workplace has created a need for technologies that can detect and block unauthorized device use in the enterprise network, spot and stop mobile malware threats and mitigate data loss in the event of a mobile security breach.

User Considerations

Figure 3.
Employee Concerns to Consider

Employees using personal smartphones and tablets at work have balked at efforts to impose security and management controls on their devices, seeing them as intrusive and restrictive. Several of the employee concerns that could slow BYOD adoption, and therefore need to be factored when developing a mobility management strategy, appear in Figure 3.

To discuss these points further:

- **Device Privacy.** Many employees fear loss of privacy in letting employers put management controls on their personal smartphones, tablets and notebooks. Their concerns center on employers snooping on personal information, photos and private correspondence stored on employee-owned iPhones, iPads and Android devices, the *Indianapolis Business Journal* (IBJ) noted in an article on the growing tension between employers and workers over BYOD issues.[8]
- **Location Tracking.** Many smartphone and tablet owners are wary of letting employers install any management tools on their devices for fear of being monitored.
- **Personal Data Loss.** The insistence by most employees that they be the ones to wipe corporate data from devices that are no longer authorized to store that data is another stumbling block for users. The big concern for many employees is that such remote wiping of data could result in valuable personal information also vanishing from their devices.
- **Restricted Functionality and Access.** Employees wishing to harness the full capabilities of their mobile devices dislike IT controls because of fears of degraded device functionality and user experience. Many users also hesitate to let IT install management agents or other tools on their devices because they fear losing control. Tools that carve out an encrypted container for corporate apps and data may provide a solution to this conundrum.[9]

[8] "'Bring your own device' creates privacy issues for employees," IBJ.com, August 24, 2014; www.ibj.com/articles/49128-bring-your-own-device-creates-privacy-issues-for-employees

[9] "Best BYOD management: Containment is your friend," *Computerworld*, August 29, 2012; www.computerworld.com/article/2506111/byod/best-byod-management--containment-is-your-friend.html

Organizations seeking to better manage the BYOD environment need to address valid security and device management issues while also accommodating employee concerns over privacy and overly restrictive security and access controls. Much of the early effort around BYOD management focused on MDM tools that allowed companies to effectively lock down devices if they wanted to. However, such approaches are just a starting point; managing user-provided devices effectively means going beyond MDM and incorporating sound practices and tools for mobile application management and mobile content management. The measures that companies should take to exercise greater control over their BYOD environment will vary with organizational needs.

Managing Hardware

Controls need to be implemented at the device level to ensure that IT organizations have the ability to quickly enroll devices, configure them, provision applications and services, and update software and settings, and to do all of this over the air. All smartphones and tablets with access to corporate data have to be password-protected, and policies need to force a device password or passcode when accessing the enterprise network or data. IT organizations also need to ensure parity of hardware and OS with corporate device requirements. Users of personally owned devices may not always update their hardware or OS, thereby putting the devices out of compliance with corporate device requirements.

Application whitelisting and blacklisting can limit devices to installing and running only known-good applications. A whitelist provides a list of applications that the employer approves for use on a personally owned device, while a blacklist offers a list of applications that IT specifically prohibits in the protected environment. Both approaches have their benefits and downsides, and IT groups need to decide based on risk tolerance levels and user acceptance.

Remote device wiping is essential to preventing unauthorized access to business data stored on a device that may be misplaced, lost or stolen. Wiping the device ensures that no data can be retrieved from the device. Even though mobile application management (MAM) and device management tools allow IT to remotely wipe only corporate data and applications on a mobile device while leaving personal data intact, employees can still be hesitant to allow IT departments access to such features on their personally owned devices. In such a situation, requiring BYOD participants to remotely wipe the device themselves may be a good compromise.

Being able to update security settings over the air, without requiring connection to a computer or other location-specific services, is critical. This capability is critical for near-real-time updates of security and other policy settings as well as providing assurance to auditors that mobile devices are well managed.

Managing Applications and Content

MAM tools allow enterprises a way to exercise control over the manner in which applications are distributed to, and consumed by, mobile users. MAM controls are less restrictive than the all-or-nothing MDM controls. They enable the creation of an internal application storefront where authorized mobile users can download approved internally developed and third-party applications.

These tools are vital to ensuring separation between private applications and business applications on a personally owned mobile device. They facilitate content management and content security by enabling corporate applications and data to be stored in secure virtual "containers" in an encrypted space on the device operating system to prevent unauthorized access.

Finally, MAM tools are essential to provisioning applications to mobile devices based on the user's role and access rights within the organization. They can deliver applications on demand when users enroll on the network for the first time. They enable IT to create custom application settings for different groups of people based on their roles, facilitate easier software updates and security fixes, and restrict risky native applications from running on mobile devices under certain conditions. Application management tools are critical to implementing strong user authentication, data backup and encryption requirements with business-critical applications and data.

Threat Protection

Consider centralizing mobile security application distribution and management to mitigate malware threats on personally owned mobile devices in the workplace. Being able to detect mobile malware, phishing threats, "grayware" and leaky applications on mobile devices from a centralized console can significantly improve malware detection and response. Threat protection tools are essential to reduce malware-related disruptions, mobile spam and identifying at-risk and noncompliant devices.

Conclusions

The problems created by the proliferation of personal mobile devices in the organization should not detract from the productivity and operational benefits of mobile technology. In trying to develop a mobility management strategy for BYOD, organizations should resist the temptation to revert to age-old IT models of controls and restrictions. Such "iron fist" methods are more likely to result in defiance than compliance. Instead, the effort should be to enable the secure use of mobile devices in a manner that addresses legitimate security concerns while also accommodating user interests.

IT's best strategy, says Gartner, is to address the challenge with a combination of policy, infrastructure controls and software. IT departments need to work with their legal and HR teams to understand all the tax, labor and liability issues associated with personal device use in the workplace. IT policymakers should draft a standard policy for acceptable use with the help or legal and HR, and then customize the policy as needed. IT security teams can harness numerous, device, application, content and threat management tools to enforce this policy.

Smartphones and tablets are only the start of the BYOD phenomenon, as Gartner notes. It's far too late think about turning back this tide, so the key is to be prepared for it, by deploying appropriate policies and effective management tools.

About the Advisor

Lee Neely is a senior IT and security professional at Lawrence Livermore National Laboratory with more than 25 years of experience. Lee has worked with securing information systems since he installed his first firewall in 1989. As part of his employer's cybersecurity program, he leads the laboratory's new technology group, working with programs to develop secure implementations of new technology. Lee was instrumental in developing the secure configurations, risk assessments and policy updates required for iOS, Android, BlackBerry and Windows Mobile devices and has worked to evolve solutions for both corporate and BYOD requirements. Lee worked with the SANS SCORE project to develop the iOS Step-by-Step configuration guide as well as the Mobile Device Configuration Checklist (included in the SEC 575 course). Lee has a BS in computer science from California State University-Hayward and holds several security certifications, including GMOB, CISSP, CISA, CISM and CRISC. He is also the technology director for the ISC2 EastBay Chapter.

About the Author

Jai Vijayan is a seasoned technology writer with nearly 25 years of IT trade journalism experience. He most recently was a senior editor at *Computerworld*, where he covered information security and data privacy topics. Vijayan currently writes for the *Christian Science Monitor*, *InformationWeek*, *Dark Reading*, *eWEEK* and *Datamation*.

Sponsor

SANS would like to thank its sponsor:

Symantec™

Last Updated: March 18th, 2018

Upcoming SANS Training

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

SANS Munich March 2018	Munich, DE	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Pen Test Austin 2018	Austin, TXUS	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, AU	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Boston Spring 2018	Boston, MAUS	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS 2018	Orlando, FLUS	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Abu Dhabi 2018	Abu Dhabi, AE	Apr 07, 2018 - Apr 12, 2018	Live Event
Pre-RSA® Conference Training	San Francisco, CAUS	Apr 11, 2018 - Apr 16, 2018	Live Event
SANS Zurich 2018	Zurich, CH	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS London April 2018	London, GB	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MDUS	Apr 21, 2018 - Apr 28, 2018	Live Event
Blue Team Summit & Training 2018	Louisville, KYUS	Apr 23, 2018 - Apr 30, 2018	Live Event
SANS Seattle Spring 2018	Seattle, WAUS	Apr 23, 2018 - Apr 28, 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 Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
SEC487: Open-Source Intel Beta One	OnlineVAUS	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced