Trustwave®

White Paper

Keep Calm and Bring Your Own

How a cooperative and self-sealing technology ecosystem makes it safer to BYOD

Executive Summary

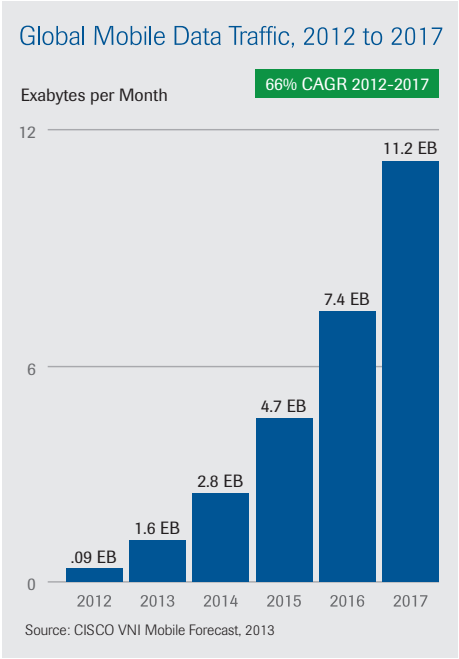
The consumerization of IT and the increasing popularity of bring-your-own-device (BYOD) initiatives that enable employees to use their personal devices for work activities are changing the way businesses operate, increasing productivity and cutting hardware costs. But at the same time, the phenomenon is creating significant security challenges. Mobile malware, policy violations, data loss, and unsupported and insecure applications that create security risk are all concerns that should be top of mind when organizations implement a BYOD program.

The proliferation of smartphones, tablets and other personal devices, along with an increasingly mobile workforce, has left enterprises grasping for better security and compliance for their devices, data and infrastructure. While many organizations have embraced mobile device management (MDM) to cover provisioning, configuration and tracking requirements, MDM often falls short when it comes to providing a mobile defense-in-depth security strategy — leaving enterprises exposed to network security and compliance risks.

How can organizations support the growing demand for BYOD and keep their users protected and productive without risk of compromising their sensitive data? This paper will explore the growing BYOD phenomenon, the increased malware risks that come with it, and how organizations can successfully implement security measures that empower the business to fully embrace the operational, cultural and performance benefits that come with mobile BYOD adoption.

The BYOD Phenomenon

The advent of smart-phones and tablets combined with mobile application (or "app") ecosystems has initiated a shift in Internet access and data usage from traditional personal computers and laptops to mobile devices. Increased mobile data access is notable across both consumer and corporate segments, and with the introduction of high quality, consumer products, such as the iPhone, iPad and Android-based devices, there has been ever-growing desire from employees to use their personal devices for work use as well.



This employee-driven mobility push for work-related use of personally owned devices, commonly referred to as bring your own device (BYOD) or "the consumerization of IT," evolved as employees resisted corporate security policies that barred access to social media, personal email and applications. In response, employees began bringing their own devices to work to gain access to these highly desired resources for both personal and work use — independent of the corporate policy. As a result, organizations found themselves with policies misaligned to actual employee access and usage, which has driven the need to adapt with corporate-sponsored BYOD programs and enhanced mobile data security solutions.

In fact, according to data from Gartner, three-quarters of companies allow employee-owned smartphones and/or tablets to be used at work and predict that number will rise to 90% by 2014. And according to Business Insider, 69% of IT leaders globally think the benefits of BYOD are positive. In addition, ZDNET data finds 75% of enterprises now have a "bring your own device" policy in place.

While initially perceived as a disruptive phenomenon, corporate BYOD adoption has substantially increased productivity by allowing employees to access business applications and data from virtually anywhere in the world. This ubiquity of data and application has led to faster communication, quicker decision making and more rapid transaction cycles, which are all factors that lead to increased sales revenue. A recent survey by Dell shows 70% of companies believe

BYOD can improve their work processes and help them work better in the future, while an estimated 59% believe they would be at a competitive disadvantage without BYOD. According to Intel's 2012-2013 IT Performance Report, their corporate BYOD program now includes 23,500 devices and has resulted in employee time savings of an average of 57 minutes daily, which equates to an annual productivity gain of about 5 million hours from BYOD in 2012 alone.

BYOD adds another dimension to organizational efficiency through decreased cost. By embracing BYOD, organizations not only accommodate employee preferences for device type but also dramatically decrease costs by eliminating capital expenditures of device hardware and operational expenses related to service charges by passing some or all of those costs on to their employees. A compelling example of the potential cost savings benefits can be seen with VMware, whose former CIO, Mark Egan, reported in February 2013 that the company saved $2 million by going "all-in" on BYOD.

However, with all of the notable BYOD benefits, it also poses real security challenges for CIOs. This shift from traditional platforms with well-established security and compliance tools and frameworks to emerging, mobile technologies exposes enterprises to a number of new threats and risks that cannot be mitigated with traditional security tools. With BYOD, organizations need to take a refreshed look at their governance, compliance, mobile device management and security strategies.

The looming security risk is further validated in Trustwave's 2013 Global Security Report, which quantifies the explosive growth in mobile malware. As organizations embrace mobility, mobile malware continues to be a problem for Android-based devices in particular, with Trustwave's malware collection for Android growing 400%, from 50,000 to over 200,000 samples in 2012. This growing body of malware targets personal devices for user credentials, valuable corporate confidential data and supports criminal and fraudulent attack vectors.

In addition to the insurgence of mobile malware, security of the apps and devices themselves are also factors for consideration. The apps combined with the physical device and Android or iOS constitute a bigger threat. In fact, 87.5% of mobile applications tested by Trustwave in 2012 had one or more flaws, including caching sensitive data on the device or transmitting sensitive data unknown to the user.

With all of the potential BYOD benefits and risks, the reality is that the rapid increase in the growth of smartphone and tablet driven data traffic means that organizations must establish new ways of assessing and mitigating security and compliance risks associated with these "new" mobile devices. Regardless of where an organization is at in their BYOD adoption lifecycle, analyzing the company's return on investment (ROI) is a useful starting point in quantifying the value in taking the next steps in the organization's BYOD maturity.

A broad ROI framework should consider the savings, costs and other indirect factors as seen in the example below.

BYOD – ROI Assessment*

Participating Employees: 1,000

SAVINGS	Year 1	Year 2
CapEx – Device Hardware Average $400 per device	$400,000	
OpEx – Annual Service Plans Average $1,000 per device	$1,000,000	$1,000,000
Employee Time Savings 57 minutes per day per employee = 237.5 hours gained per year X 1,000 employees X $40 average hourly wage	$9,500,000	$9,500,000
Total Savings	$10,900,000	$10,500,000

COSTS	Year 1	Year 2
BYOD Enterprise Security Technology and Tools Technology implementation + maintenance	$500,000	$85,000
Mobile Device Management Technology 1,000 devices x $30/month + $40,000 software implementation, licensing and subscriptions	$70,000	$60,000
Total Costs	$570,000	$145,000
Total Annual ROI	**$10,330,000**	**$10,355,000**

* The above figures are estimates. Organizations should apply their actual figures using the above ROI framework.

Common Challenges with Mobile Device Management

Often, organizations have turned to mobile device management (MDM) as an initial effort to develop and implement solutions for their BYOD risk management policy. While MDM solutions are a good start, they don't address the primary security issues inherent in enterprise BYOD adoption. Enterprise MDM is predominantly a provisioning, configuration and policy management tool for mobile handheld devices, such as tablets and smartphones. It aims to help organizations manage their migration to a more complex mobile computing and communications environment.

> "…just implementing MDM software won't solve IT's BYOD and mobile management headaches."
>
> Michael A. Davis
> Contributing Editor, InformationWeek

Still relatively new, the market and interest in MDM continues to grow. As noted by Gartner, MDM adoption growth is driven by the move from well-managed and secured BlackBerrys, to consumer-focused devices based on iOS and the Android OS. A recent Gartner survey showed that 58% of enterprises have or will make iOS their primary platform during the next 12 months, compared with 20% staying with BlackBerry and 9% on Android.

Although useful in its overall management functions, MDM does not effectively address other important enterprise mobile security and compliance issues. As noted by Michael A. Davis, InformationWeek Contributing Editor, "Employees need access to corporate data to do work while they're away from the office, and with that data access comes all kinds of security questions: who can access what data, why, when and where — and what happens when that device goes missing? But mobile data and mobile operating systems present a different security challenge from PCs, which is why just implementing MDM software won't solve IT's BYOD and mobile management headaches."

The first issue is the matter of ownership. Enterprises looking to take full advantage of the flexibility and efficiencies of BYOD support devices owned by their employees. In addition, employees use many devices, and they expect to use any device or application anytime, anywhere — for a blend of both personal and work related activities. Addressing the mobile security problem with the same processes used for laptops and PCs won't work. For example, if a device is infected or there is a data leak concern, as a security measure, if an organization wipes an entire device along with the employee's personal photos and other data, the company could potentially be liable for damages — or at minimum, have a disgruntled employee. That means security strategies need to evolve to accommodate for this new, blurred line between corporate and personal data on employee-owned devices.

The next limitation is device encryption, which is one of MDM's core security functions. While this is a valuable data protection measure it may not be effective for data at rest on the device if the encryption and decryption key are also stored on the device or the passcode can be snooped by malware. Physical access to a device gives the attacker great odds for successful compromise of that device and its data. Unless the application is protecting the data, itself, with a password-based encryption scheme that does not rely on a stored key, which can also be compromised by OS level malware, Trustwave SpiderLabs has verified that device encrypted data can be recovered. Combined with the growth in software-agnostic techniques for extracting data, memory scrapers have become popular in targeted attacks. According to Trustwave's 2013 Global Security Report, new samples that included memory-scraping functionality accounted for 32% of cases, and such activity was detected in 49% of all incident response cases for which the associated malware had identifiable data collection functionality.

Another important security requirement is the ability to protect the company's confidential data on employee's mobile devices not only when they're remote — outside the office — but also when they're inside the organization, which MDM does not support. This aspect is important in order to ensure systems accessing the corporate network from the inside are not introducing malware and that the corporate risk management policies are being followed.

Again, MDM does a credible job of provisioning and tracking devices outside the network but should not be considered a holistic BYOD security solution. User-owned devices present several security and management challenges, and the following three, most critical issues should be a minimum technology requirement for enabling BYOD enterprise security:

- ### Identification of BYOD Devices on Network

  Organizations embracing BYOD need to identify which devices, device types and users are on-network. Identification and aggregation allows organizations to profile and apply on-network policies without making configuration changes to employee-owned devices.

- ### Mitigation of Mobile Malware Propagation

  The rapid development and proliferation of mobile operating systems and apps has exponentially introduced new vulnerabilities and threats into the mobile enterprise ecosystem. BYOD exacerbates this further, and enterprises need a way to identify infected devices that are on network before they can propagate malware.

- ### Eliminating the Loss of Sensitive Data

  With BYOD, organizations are now challenged to monitor non-company owned devices for the presence and transmission of sensitive corporate data. Transmission of sensitive data can indicate anything from a user-generated mistake (e.g., accidentally sending the wrong data to the wrong place), an intentional breach or even the presence of active malware that is scraping the data and sending it back to the attacker.

The Trustwave BYOD Security Solution

At Trustwave, we understand companies need technologies and processes that can keep up with advanced malware and other threats to corporate data while enabling the business to go faster with the adoption of productivity platforms like mobile data and BYOD initiatives.

Trustwave BYOD Network Protection enhances an organization's mobility investments to address the core security issues inherent in a BYOD program, including the ability to apply security policies to devices on the network, rapidly identify and contain infected BYO devices before they can propagate malware and protect sensitive corporate data transmitted through mobile devices — even in scenarios where the device is jail broken or rooted.

Trustwave BYOD Network Protection leverages the integration of multiple, award-winning Trustwave security technologies, providing an end-to-end BYOD security solution that protects enterprise infrastructure, networks, data and users. Our mobile security approach is simple and powerful — actively detect and disrupt attacker methods and threats from mobile devices by applying intelligence with synergized and integrated technologies.

This defense-in-depth approach uses intelligence with automation among each Trustwave BYOD solution component: Trustwave Security Information and Event Management (SIEM), Network Access Control (NAC) and Secure Web Gateway (SWG) with integrated Data Loss Prevention (DLP). Each component shares information to gain a broader understanding of activity on the network. While one observation on its own might not appear suspicious, the shared information provides critical intelligence required for superior threat detection. This integrated approach serves as the cornerstone for an enterprise BYOD security strategy — providing detection and active control capabilities that enable response to evolving threats faster and smarter than alternative solutions.

How It Works

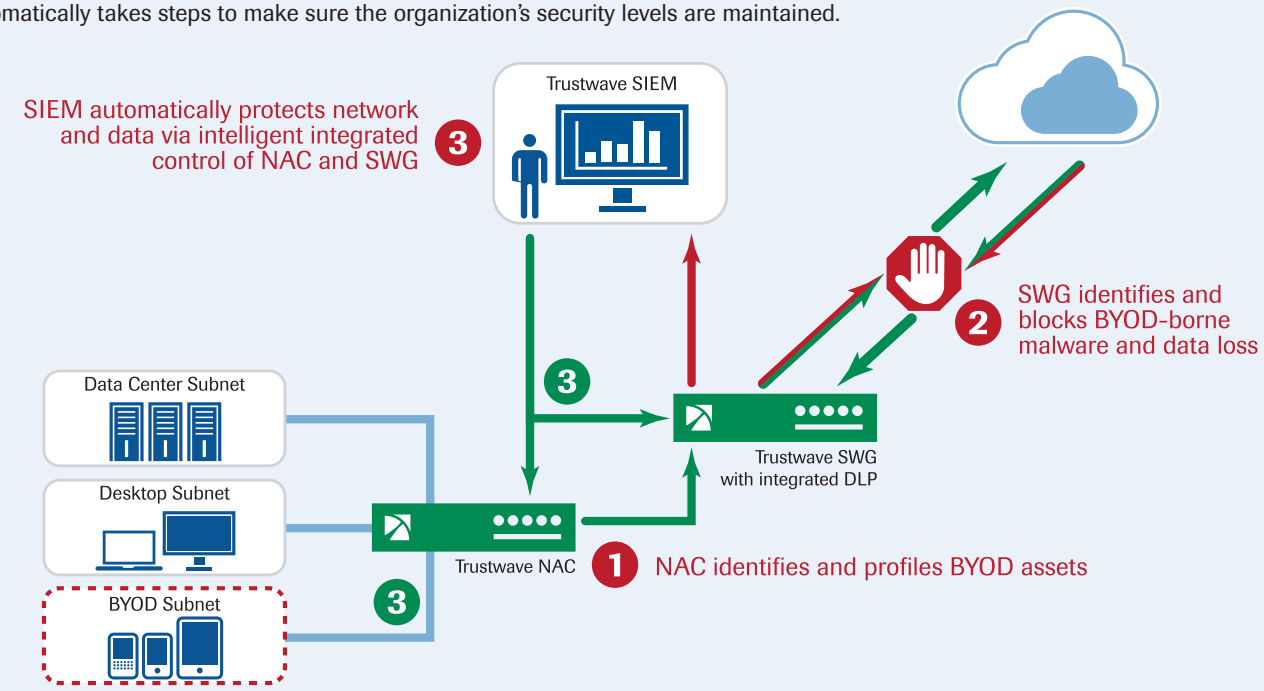
Native integration of Trustwave SIEM technology provides a unique advantage with an award-winning solution that serves as the monitoring and control nerve center by allowing each BYOD solution component to share intelligence and events that uncover threats that single security products — acting alone — miss.

Trustwave NAC enables on-network management of user-owned BYOD devices through transparent policy enforcement, and Trustwave SWG, with market leading malware protection and integrated DLP, protects against malware downloads — intended or accidental — and the unauthorized transmission of sensitive data.

Working together, all Trustwave BYOD Network Protection components provide operational efficiency, automation, transparency and holistic protection for the enterprise. The end result is substantially reduced risk exposure with intelligent operational automation and cost savings.

Use Case

When an employee comes into the office with their device, Trustwave BYOD Network Protection automatically takes steps to make sure the organization's security levels are maintained.



1. An employee connects to the network with their device. NAC identifies and profiles the device, performs policy enforcement, assesses if it's a rogue or rooted device, assigns the malware-free device to the appropriate access group and keeps SIEM informed.

2. SIEM receives the information and passes the employee's device IP address to SWG. SWG applies the appropriate access policy to the IP address and sends all logs of the device's Internet access to SIEM. The employee then inadvertently accesses a malicious site, and SWG identifies and blocks the BYOD-borne malware and potential data loss.

3. SIEM sees the malicious behavior from SWG's logs and takes immediate action by leveraging the native NAC integration to quarantine the employee device in order to eliminate propagation of the malware to other parts of the enterprise network. Alternatively, the user's access to certain internal resources can be removed based on the violation and the organization's desired policy configuration.

As this example use case demonstrates, Trustwave BYOD Network Protection provides organizations with a closed loop, "self-healing" process to ensure and verify a threat has been identified, stopped and fully contained. This integrated BYOD security approach provides organizations with unparalleled, real-time protection and reduced risk using Trustwave's powerful technologies, working together, to identify and take action on the root cause that led to the attack in the first place. Through this unique, automated process organizations also gain significant cost savings with eliminated admin cycles in time traditionally spent manually assessing the threat and tracking down the device in question.

Conclusion

Embracing a BYOD culture undoubtedly offers organizations several benefits, including increased employee satisfaction and productivity along with lower overall capital and operational expenditures related to mobile devices. With all of the positive reasons for organizations to embrace BYOD, the introduction of employee-owned devices at work also creates challenges, such as managing non-standard, heterogeneous devices, personal and potentially rogue applications and the potential of introducing malware into the corporate network.

In an effort to address the BYOD challenges, many organizations have turned to MDM software. These solutions mainly focus on corporate-owned mobile devices and excel at provisioning, configuration and policy management; however, they lack the in-depth security protection organizations require for employee-owned devices on the corporate network.

Trustwave BYOD Network Protection puts control of BYOD back into the hands of IT and security administrators to ensure a secure, productive and compliant computing environment. Trustwave BYOD Network Protection is an integrated, end-to-end security solution that protects enterprise infrastructure, networks, data and users through a defense-in-depth strategy. As organizations take action to include BYOD implementation plans as part of their mobile strategy, Trustwave BYOD Network Protection should be included in the vendor short list.

Corporate Headquarters
70 West Madison St.
Suite 1050
Chicago, IL 60602 USA

P: 312.873.7500
F: 312.443.8028

EMEA Headquarters
Westminster Tower
3 Albert Embankment
London SE1 7SP UK

P: +44 (0) 845 456 9611
F: +44 (0) 845 456 9612

LAC Headquarters
Rua Cincinato Braga,
340 nº 71 Edificio Delta Plaza
Bairro Bela Vista - São Paulo - SP
CEP: 01333-010 - BRASIL

P: +55 (11) 4064-6101

APAC Headquarters
Level 7/Suite 3
100 Walker Street
North Sydney NSW 2060 Australia

P: +61 2 9466 5800
F: +61 2 9466 5899