SOLUTION BRIEF

VECTRA™
Security that thinks.™

Detecting Cyber Attacks in a Mobile and BYOD Organization

Explore the challenges, understand the needs, evaluate mobile device management as an approach to detecting attacks and offer a flexible and high efficacy solution for detecting any phase of an ongoing attack on mobile devices regardless of device type, operating system or applications installed.

Mobile devices – laptops, tablets and smartphones – have been part of the information technology culture for some time. Enabling employees and contractors to bring their own devices to work has become a way of life for many organizations and may soon become the norm.

Many organizations understand that traditional perimeter security defenses are not effective at identifying attacks on mobile devices. This solution brief sets out to explore the challenges, understand the needs, evaluate mobile device management as an approach to detecting attacks and offer a flexible and high efficacy solution for detecting any phase of an ongoing attack on mobile devices regardless of device type, operating system or applications installed.

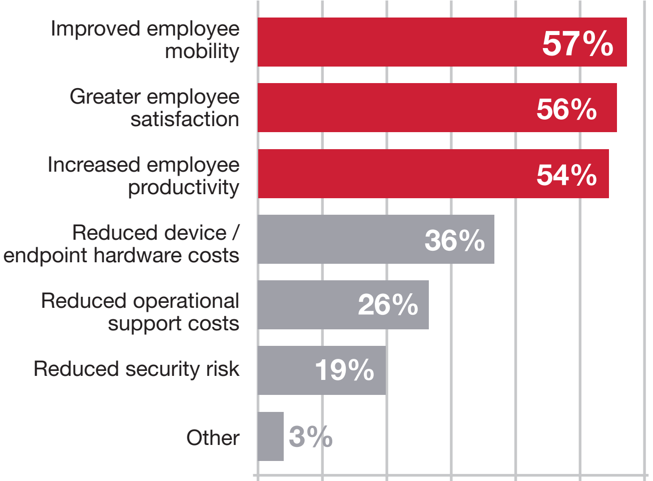
Personalization vs. Security – Clashes in a Changing Culture

Over the past several years, organizations have begun adopting "bring your own device" (BYOD) policies to create the kind of work environment that attracts and retains the best talent. The old days of standard-issue Windows PCs for new employees are over. College students no longer trek to the computer lab on campus and very often are choosing to use Windows PC alternatives such as MacBooks, Chromebooks, and iOS and Android tablets and smartphones for their scholastic and personal computing needs. Similarly, these alternatives are commonly the preference in high schools. These students-turned-new-employees frown at the idea of being told which device they must use at work and seek out employers whose computing culture aligns with their own.

A recent survey about BYOD and Mobile Security by the Information Security Group on LinkedIn shows that the primary benefits of BYOD programs are improved employee mobility (57%), greater employee satisfaction (56%) and improved productivity (54%). The same survey indicates the biggest security concerns are loss of company or client data (67%), unauthorized access to company data and systems (57%) and user downloaded apps or content with embedded security exploits (47%)[1].

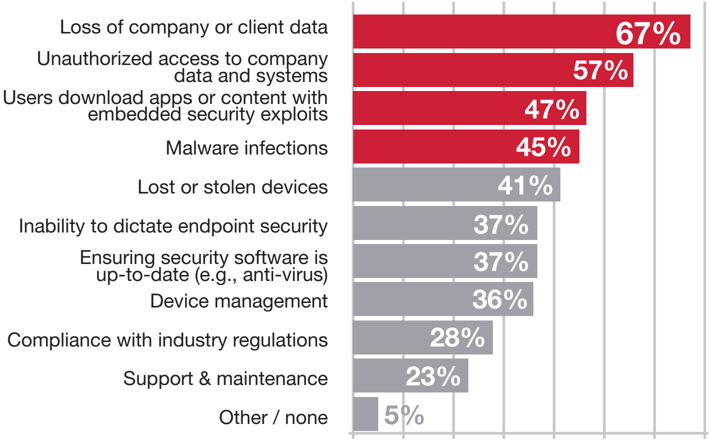
[1] 2014 BYOD & Mobile Security Survey, LinkedIn Information Security Group

BYOD Benefits



BYOD personalization freedom increases productivity.

BYOD Security Risks



BYOD is the new malware vector.

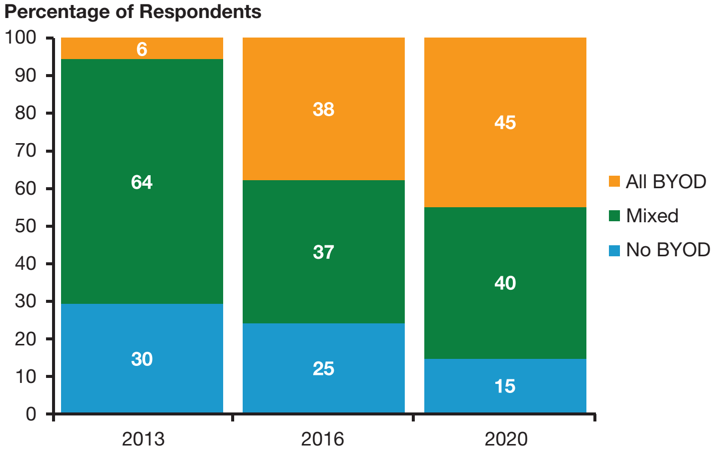
This survey data demonstrates the paradox of personalization and security for IT organizations embracing BYOD. A BYOD policy increases productivity and satisfaction, but creates new critical risks that are hard to mitigate when directly controlling the device is no longer possible.

Data from the same survey indicates the strong momentum with BYOD fully implemented by 31% of organizations and under evaluation by 20%. However, 21% of survey participants admit that personally owned devices are in wide use without official support of the organization.[2] This indicates that employees will find a way to use their own devices even when there isn't a program in place.

No Turning Back

Regardless of the friction caused by this paradox between the freedom to personalize and the restrictions necessary for security, the trend is irreversible. A Gartner strategic planning assumption indicates "by 2020, 85% of organizations will adopt BYOD in some form."[3]

Q: When will your organization cease to provide personal devices?



N = 2,206 worldwide

According to Gartner, enterprise device ownership will shift over a period of time.[4]

This strategic planning assumption represents a big shift from 2013 where only 6% of organizations surveyed were completely BYOD.

Defeating Your Own Perimeter

Many organizations' security implementations focus on the concept of a defensive perimeter, which includes firewalls, intrusion prevention systems and sandboxes as well as endpoint security products such as antivirus software. BYOD and mobile devices including laptops, smartphones and tablets defeat the goal of perimeter security, which is to block an attack at the entry to the organization. Employees, contractors and customers use these devices inside and outside the perimeter. If their devices are infected with malware outside the perimeter, the malware will be physically carried into the network past all the network perimeter defenses.

[2] "2014 BYOD & Mobile Security Survey," LinkedIn Information Security Group

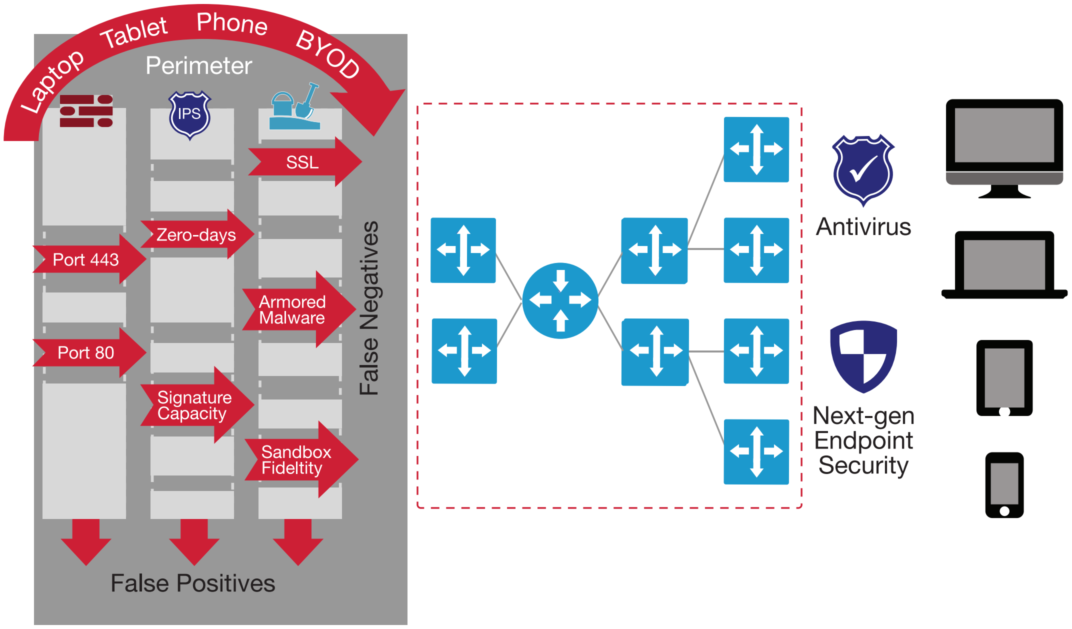
[3] "Defining BYOD Ownership and Support Expectations in Contracts Ensures Successful Implementation," by DD Mishra and David Edward Ackerman, April 25, 2014, ID G00261616, http://www.gartner.com/document/261616

[4] "Defining BYOD Ownership and Support Expectations in Contracts Ensures Successful Implementation," by DD Mishra and David Edward Ackerman, April 25, 2014, ID G00261616, http://www.gartner.com/document/261616

Perimeter defenses look for malicious traffic coming into the organization from the outside rather than assuming that the malware is already inside and they are generally ineffective at protecting against this attack vector.

For devices owned by employees, the IT department is often unable to require installation of endpoint security software, leaving this traditional security approach ineffective as well. As BYOD use increases, so does the lack of visibility and control over security.

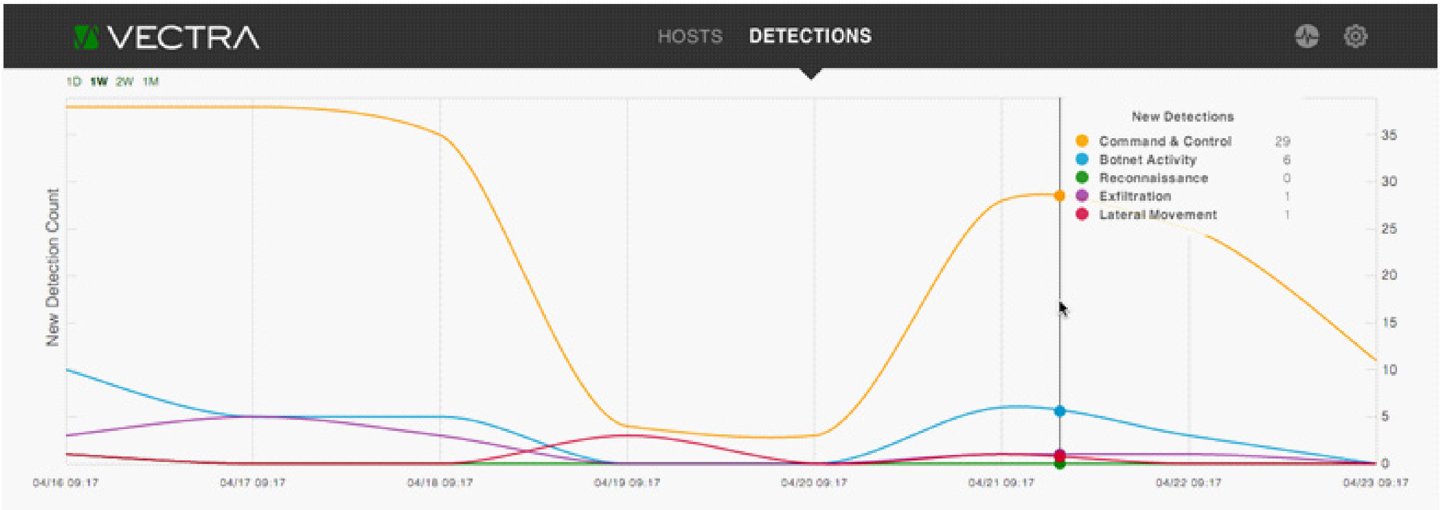
Porous perimeter and endpoint defenses



Malware on mobile devices circumvent perimeter defenses leaving the network exposed as BYOD become the norm.

Malware – it's not just for laptops anymore

Laptops are still the primary mobile devices used to physically carry malware into an organization. The detections graph below reinforces the reality that mobile laptops – regardless of their owner – are one of the largest sources of malware in an organization.



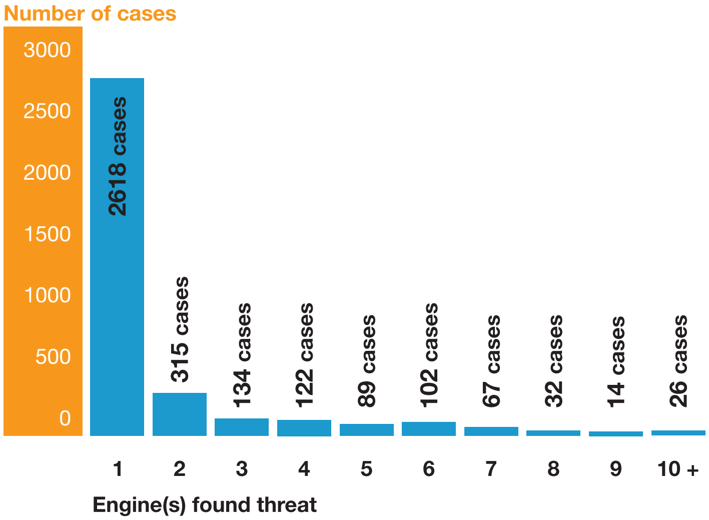
Detections report for a Vectra X-series Platform in a production network.

Note the orange line dropping from 35 command and control detections on Friday April 18 to less than 5 on Saturday, April 19, then rising back to nearly 30 on Monday April 21. This happened because employees closed their laptops and took them home for the weekend. In this customer deployment, over 85% of the command and control detections were for laptops.

Tablets and smartphones will quickly catch up to laptops for malware infections in organizations. Gartner published a strategic planning assumption that "by 2017, the focus of endpoint breaches will shift to tablets and smartphones."[5]

The trend is already visible. The first Android botnet was reported in June 2012 and the first Android botnet using The Onion Router (TOR) in February 2014. This TOR-enabled botnet can be rented for $500 per month plus a $1,000 one-time setup fee. In March 2014, WinSpy RAT became available for Windows and Android mobile devices. In July 2012, a grey-hat company called Hacking Team released the Da Vinci Remote Control Suite to Government organizations, enabling them to intercept content on Android, Windows and iOS mobile devices regardless of encryption, transparent to the user and with no discernible impact on battery life.

A collection of nearly 12,000 Androids application files from third-party sites (other than Google Play) were scanned using Metascan Online and nearly a third, or over 3,500 files, were flagged as having a potential threat by one of 40 malware engines. Two or more malware engines[6] flagged 919 of the 12,000 application files, which is 26% of the samples likely containing malicious software.



74% of the app files were flagged by a single malware engine. The remaining 26% flagged represent 8% of the nearly 12,000 app files scanned.

Similarly, Cisco reports that 97% of all mobile malware in 2013 targeted Android devices, while Android users also had the highest encounter rate (71%) with all forms of Web-delivered malware.[7]

Plugging the Gap with Mobility Device Management Solutions

To keep pace with both the employee expectations for BYOD and mobility and the organizations' requirements for security, IT departments have been deploying mobile device management (MDM) solutions.

MDM is often the preferred BYOD solution that requires employees to allow installation of security client software on their personal devices. This gets tricky when the devices aren't actually company-owned.

However, MDM software doesn't actually detect the presence of malware on a laptop, tablet or smartphone. MDM provisions and manages devices to ensure an employee-owned device inherits the user's enterprise persona, thus centralizing authorization for email access and blocking network access to jailbroken devices since they represent a significant vulnerability. MDM solutions can also attempt to manage access and use of applications from branded and third-party app stores as well as preventing a device from incurring international plan surcharges.

According to Gartner, "by 2016, 20% of enterprise BYOD programs will fail due to enterprise deployment of MDM measures that are too restrictive."[8] This is likely to occur if IT departments implement MDM with a similar level of control over employee-owned devices that they had on company-owned personal computers. At the same time, employees are increasingly aware that MDM provides IT organizations access to their personal information, such as personal email, photos and social media posts. Employees are demanding solutions that isolate personal content from business content and restrict the ability of the IT organization to access or change personal content and applications.

[5] "Predicts 2014: Mobile Security Won't Just Be About the Device," by Ray Wagner, Dionisio Zumerle, John Girard, Joseph Feiman, November 22, 2013, ID G00258488, http://www.gartner.com/document/258488

[6] OPSWAT study April 14, 2014, http://www.opswat.com/blog/scanning-malware-android-applications

[7] 2014 Annual Cisco Security Report, https://info.sourcefire.com/2014CiscoAnnualSecurityReportForm-SEM.html

[8] "Predicts 2014: Mobile and Wireless," by Ken Delaney, November 8, 2013, ID G00255829, http://www.gartner.com/document/255829

Adapting Your Security Architecture for BYOD & Mobility

According to Gartner, enterprises are overly dependent on blocking and prevention mechanisms that are decreasingly effective against advanced attacks.[9] Existing blocking and prevention capabilities are insufficient to protect against motivated, advanced attackers, but most organizations continue to be overly invested in prevention-only strategies. Information security doesn't have the continuous visibility it needs to detect advanced attacks when computers are company-owned and BYOD exacerbates the problem further.

What's needed is a solution that finds threats that evade and circumvent the limited protection that perimeter defenses provide against motivated, advanced attackers.

Vectra Networks provides detection capabilities to find attacks that have evaded perimeter security products deployed at the perimeter. The key benefit of Vectra Networks' detection capabilities is reduction of the length of time malware remains in the network, and the potential damage it can cause. Detection capabilities are critical in a mobile/BYOD environment where an organization must assume the network is already compromised because these devices are used outside the perimeter without any guarantee of endpoint protection technologies being present on the device.

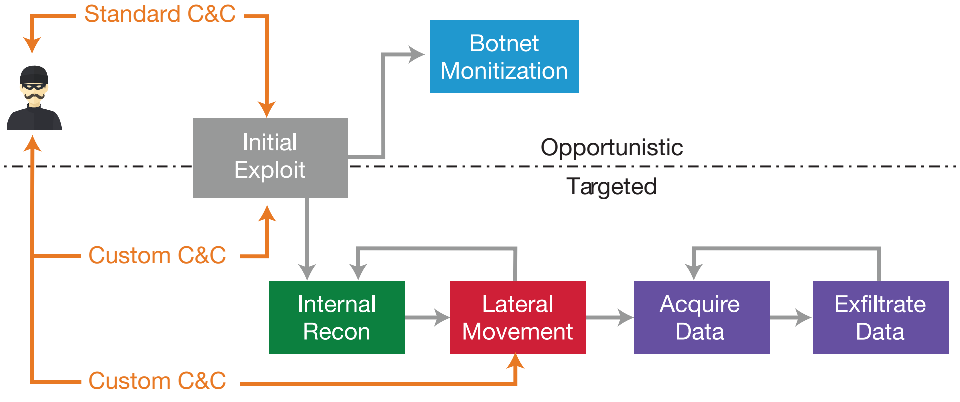
Vectra Networks' X-series platforms deliver detection capabilities by continuously listening, rather than periodically scanning. That means Vectra knows when an attack starts, morphs or subsides. And because it's deployed inside the network perimeter, Vectra can listen to users' traffic to both the Internet and the data center to detect anomalous behavior consistent with specific phases of an ongoing attack including command and control communications, botnet activity, reconnaissance, lateral movement or data exfiltration.

Vectra detects attacks involving all operating systems, applications, devices and browsers. Vectra learns the traffic patterns and behaviors that are typical to a network, and it remembers and correlates anomalous behaviors it has seen hours, days or even weeks before. This means Vectra can detect malware walked past perimeter defenses on all employee, contractor and visitor devices, including BYOD mobile devices. As a result, organizations don't need to put restrictions on the types of devices used or spend time ensuring that security solutions are up-to-date with changes in employee's chosen device models and mobile OS platforms.

Vectra preserves privacy and simplicity since it requires no software installation on BYOD laptops, tablets or smartphones. So employees can rest easy about their privacy while companies need not continually react to the introduction of new apps or devices.

In customer deployments, Vectra has detected threats that have evaded traditional network perimeter defenses like firewall, IPS and sandbox solutions as well as endpoint anti-virus products. For more information on customer deployments or how Vectra can help your organization move ahead with BYOD, please take advantage of the resources below.

- White Paper: Vectra X-series Platform
- Case Study Video: Riverbed Technologies
- Case Study: Aruba Networks
- Video: How Vectra Works



Vectra X-series platforms can detect any phase of an ongoing opportunistic or targeted cyber attack.

[9] "Designing an Adaptive Security Architecture for Protection From Advanced Attacks," by Neil MacDonald and Peter Firstbrook, 12 February 2014, ID G00259490, https://www.gartner.com/doc/2665515/