WatchGuard®

Eliminate Your Network Blind Spots with Complete Visibility

Table of Contents

An Evolving Threat Landscape

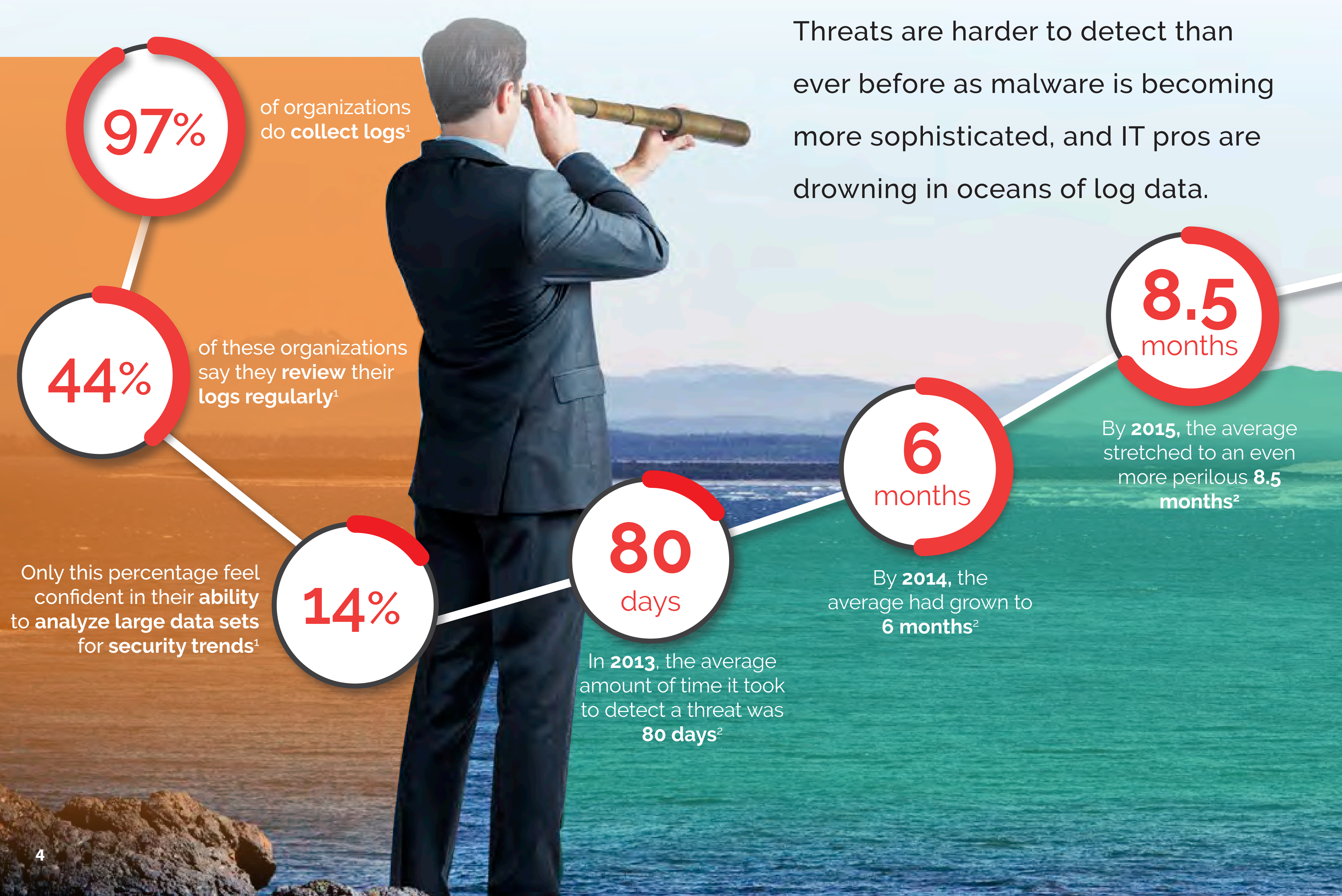
The number of worldwide cyber attacks is at an all-time high with no signs of slowing down, and the ability for IT admins to detect a breach is taking longer as they are drowning in an ever-growing amount of log data. To make matters worse, cyber criminals have turned their sights on small and midsize businesses, which they deem soft targets with inadequate security systems. Large corporations are well aware of this growing threat, employing teams of specialized security professionals to continuously monitor every corner of the network for malicious activity. Where does that leave smaller organizations that can't afford a dedicated IT security staff? How can SMBs stay ahead of the rapid evolution of data theft when they have no one to regularly monitor and investigate suspicious traffic? Is there a solution within reach of an SMB's modest budget and limited expertise?

The solution to this significant challenge is Visibility. One of the most important strategies for safeguarding an organization is to provide complete visibility into its network activity. Only when you can clearly see all network activity, connected devices, and users in real time can you consistently stay ahead of potential threats. Every organization needs comprehensive, clear insight into what is happening within their network.

> Data in itself is not valuable at all. The value is in the analysis done on that data and how the data is turned into information…
>
> *~ Mark van Rijmenam, Big Data Strategist*

Security Breaches are Becoming Harder to Detect

Threats are harder to detect than ever before as malware is becoming more sophisticated, and IT pros are drowning in oceans of log data.



97% of organizations do **collect logs**[1]

44% of these organizations say they **review** their **logs regularly**[1]

14% Only this percentage feel confident in their **ability** to **analyze large data sets** for **security trends**[1]

80 days In **2013**, the average amount of time it took to detect a threat was **80 days**[2]

6 months By **2014**, the average had grown to **6 months**[2]

8.5 months By **2015**, the average stretched to an even more perilous **8.5 months**[2]

Who Detected the Breach?

Security breaches are rarely detected by internal personnel, but rather by a third-party agency or law enforcement.

67%

A Third Party

16%

Law Enforcement

1%

Internal Personnel

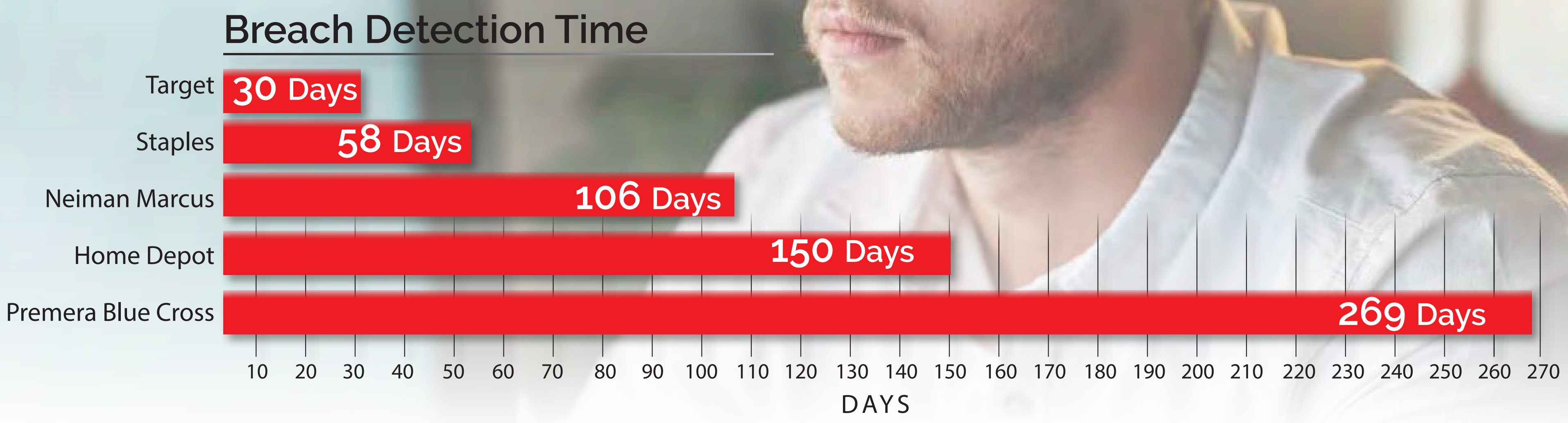
Three Key Areas of Visibility

Visibility Advances Security, Productivity, and Efficiency

If you can't identify the source of a problem, it's impossible to solve it. Poor network visibility is not only a big risk to an organization's security, it also threatens employee productivity, and makes it difficult to manage everyday nuisances like downtime and bottlenecks in the network. Businesses also need complete network visibility to accurately measure return on investment from their IT infrastructure.

1. Security Threats

Security breaches are becoming harder to detect every year in an increasingly unpredictable threat environment. Malware, backdoors, and data loss routinely go unnoticed for months, and in some cases years at a time. When the breach is finally discovered, it is usually reported by an external party and rarely through an internal review. Technologies and processes are failing to identify threats in an actionable way, and until organizations can tie security events back to users in real time, criminals will continue to steal valuable data.



2. Employee Productivity

Some employees spend too much time and resources downloading media, surfing the web, and ignoring their daily tasks. The cyber loafing will continue without proper visibility into user activity. With the introduction of technologies that monitor application usage, businesses can use throttling and traffic shaping to ensure business-critical applications have the proper amount of bandwidth while keeping employees focused on what is important.

3. Network Efficiency

Businesses may experience slow connection speeds around the same time every day. These bottlenecks typically occur when demands for resources are at their daily peak. This can cause users to become frustrated, while operations slow to a crawl. Without complete visibility into the physical layout of your network, you can't identify the source of the bottleneck, and the problems will only persist.

Problems Across Key Industries

Cyber Criminals Don't Discriminate

When it comes to stealing valuable data, cyber criminals don't discriminate. As long as a lucrative black market exists, organizations across all industries are at risk of a cyber attack. Among the most highly targeted sectors are **Education, Retail, Healthcare**, and **Hospitality**. It's imperative that businesses have full visibility into the most common threats and trends impacting their organization.

Education

Healthcare

Hospitality

Retail

Education

In the education sector, faculty and staff are not only responsible for protecting their networks from external threats, they are also responsible for protecting students from malicious and inappropriate content. Mobile devices are replacing textbooks in schools around the world. This trend has opened the door for malware to spread across campuses, leaving critical network systems vulnerable. To protect both students and the networks they depend on, schools need to monitor and filter the type of content being accessed by students.

> “With the WatchGuard platform, we’ve noticed that we have more visibility into the type of data that’s being sent out which enables us to make more informed decisions, maintain our compliance, and provide our school with a higher level of protection from inadvertent threat.”
>
> *~ Aaron Anderson, Vice President, Information Technology, Anthem College*

Principal

Providing my students and staff with fast, consistent, and secure Internet access is a must for my school. We understand that Internet access is essential for project research and as emerging learning aides, but we also understand that our students may attempt to visit inappropriate or illegal sites if left unmonitored.

Retail

Retailers exchange customer data with their corporate headquarters, and commonly offer guest Wi-Fi to encourage longer visits and repeat business. When a breach ultimately occurs, the retailer's limited IT staff needs an immediate, clear notification so that they can take the necessary steps to mitigate the issue. And while guest Wi-Fi certainly has its benefits, it presents a potential blind spot on the network. Customers streaming media or using other bandwidth-intensive applications can easily cause a decrease in transaction speed on the POS systems. IT pros need visibility into their guest environments to ensure the POS systems have enough bandwidth to quickly process transactions.

> "With a combination of WatchGuard's UTM and Dimension solutions, my team can view the entire network health in real time, investigate chokepoints and implement policies to solve the problem. All of this can be done in less than an hour."
>
> *~ Tony Sim, IT Manager, EpiCentre*

Business Owner

Guest Wi-Fi provides tremendous value for my business, but I can't let it affect my life-blood: POS transactions. I need an easy-to-mange, in-house solution that provides my small IT team with the insight they need to keep business operations on track and my customers happy.

Hospitality

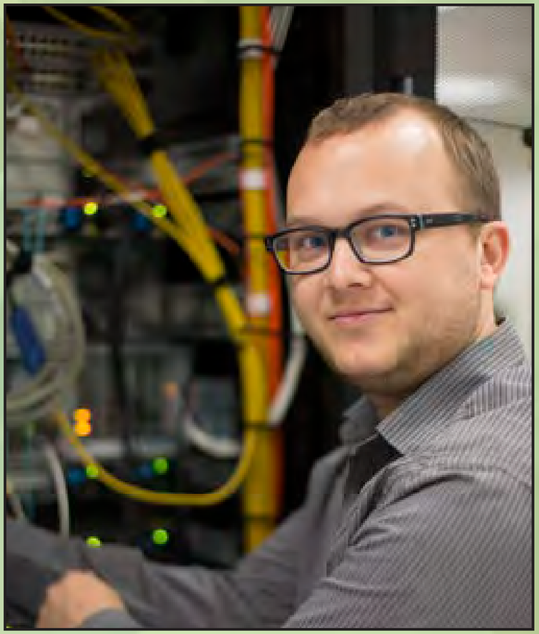
A Property Management System (PMS) is a software application used by hotels to automate and coordinate multiple business functions ranging from front office to back office operations, including management of credit card information. PMS systems also commonly integrate with POS and reservation systems, which results in a high-value target for cyber criminals. Many large hotel chains have been victimized because of a breach in the PMS or POS system, resulting in fines, lawsuits, and damage to their reputation. Without visibility into both the corporate and guest network, businesses in the hospitality sector are unable to respond to breaches and network downtime.

> “We now have the visibility to pinpoint very quickly where there is excessive traffic, by AP, Wi-Fi user, wired user, by protocol or port. Moreover, logging and viewing with Dimension was very easy to get operational without having to tweak or customize the process as is often the case with reporting systems.”
>
> *~ Fahyaz Khan, IT Manager, Kensington Close Hotel*

General Manager

I need all daily processes to run as smoothly as possible. Network downtime could mean unhappy customers, which in the age of Yelp, translates into bad reviews lost revenue. A data breach is even worse as the press will have potential guests looking elsewhere for room and board.

Healthcare



The healthcare industry has a unique set of security challenges brought on by the highly sensitive and valuable nature of the data being exchanged on their networks. The Health Insurance Portability and Accountability Act (HIPAA), along with similar global standards, require organizations that process patient data to adhere to a strict set of security practices. Various types of medical technologies have evolved to exchange data wirelessly, opening a new window of vulnerability. Healthcare organizations need total visibility into the health of their patients and network resources to ensure the best possible care while complying with the evolving data protection standards.

> “We now have a world-leading solution we can trust to deliver reliability, performance, and above all, secure access to sensitive patient information, whether that is from a PC or laptop device.”
>
> *~ Paul Freear, Head of IT Customer Services for Northern Lincolnshire*

Network Administrator

With a vast number of connected devices to account for on my network, I require complete visibility into each connection and the potential vulnerability that it presents. Accurate and comprehensive logging and reporting tools are also absolutely essential to maintaining HIPAA compliance – a non-negotiable for my healthcare organization.

Network Visibility Impacts a Wide Range of Functions

The need for complete network visibility extends beyond the IT office. With implications ranging from compliance to productivity, gains in visibility can benefit key roles across every type of organization.

Business Owner

Business Owners need to ensure that their technology investment is providing value to their business. Dashboards displaying the amount of traffic scanned and viruses blocked, as well as usage reports, provide this high-level insight into the value of IT systems.

IT Network Admin/IT Director

IT administrators are often responsible for managing multiple business technologies, making intuitive management and visibility resources highly valuable. As the first responders to security events, administrators rely on real-time alerts and granular details to quickly diagnose and mitigate threats.

CFO/Compliance Officer

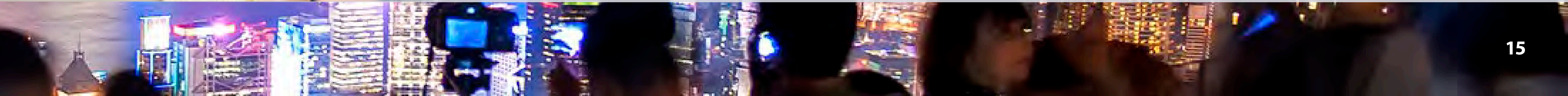
Financial officers constantly evaluate governance, risk, and compliance across their organizations. With little time to dive into detailed dashboard summaries, these individuals rely on summary reports tailored to their organization's specific compliance standards, including HIPAA and PCI.

CISO

C-level leadership desires a high-level overview of all network activity to develop and implement security strategies as well as monitor and enforce corporate policies. Automated summary reports provide the insight they need to stay on top of the security threats facing their organization.

Supervisors

Employees commonly use laptops, tablets, and other connected devices to complete daily tasks. While this technology provides huge gains in productivity, misuse can result in hours of waste. Managers rely on complete visibility, including dashboards and summary reports, to monitor network activity.



Eliminate Your Network Blind Spots

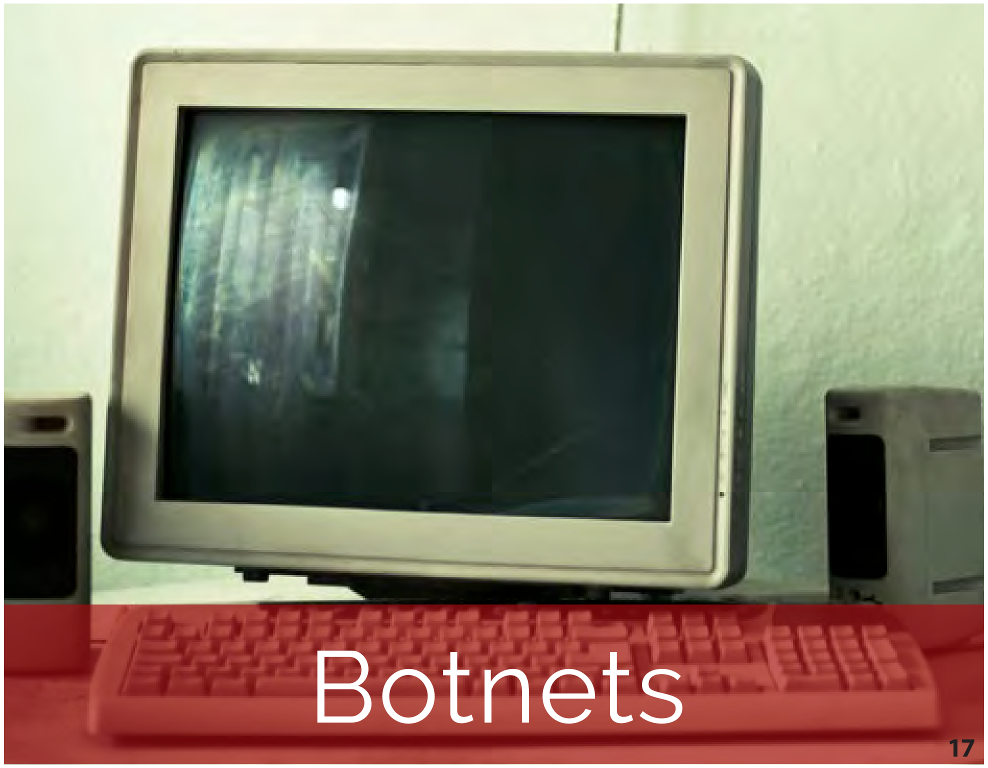
WatchGuard is light years ahead of the network security industry with a wealth of technologies that spotlight threats, illuminate trends, and stop potentially dangerous activity before it impacts your day-to-day operations.

Four Common Blind Spots

Network Activity

Connected Devices

Mobile Devices



Botnets

Blind Spot: Network Activity

Solution: WatchGuard Dimension

WatchGuard Dimension® is a cloud-ready security solution that provides complete visibility into all network activity. Distill information quickly with detailed reports and views of your network activity while instantly identifying security threats, issues, and trends before they become massive problems.

Dimension offers more than 100 comprehensive security dashboards and reports. From a high level, administrators can see who is consuming the most bandwidth, unusual traffic patterns, and which websites are visited the most often. You can then drill down to the individual log data for granular details.

Whether you are a C-level executive, IT director, compliance officer, or small business owner, reports can be tailored to your needs for complete network visibility.

Blind Spot: Network Activity

Solution: WatchGuard Dimension

Executive Dashboard

This high-level view provides a snapshot of what traffic has been allowed into the network including domains, applications, and the types of websites. From there, administrators can drill down and user data at a granular level.

Security Dashboard

The Security Dashboard shows all blocked traffic, including malware attacks and denied protocols and clients. It also tracks IPS activity, showing admins the latest detected threats at a glance. The associated IP addresses, domain names, and applications can then be added to the blocked sites list for automatic protection in the future.

FireWatch

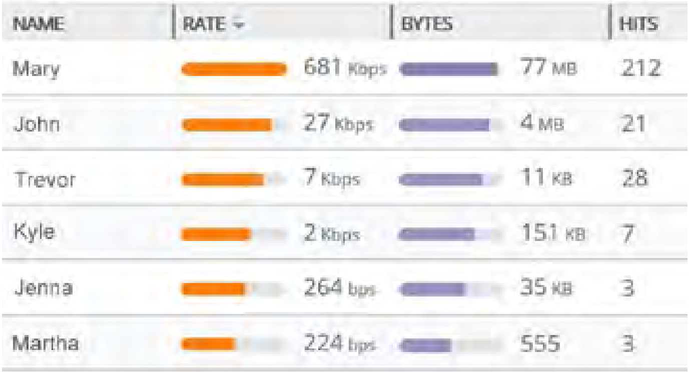
FireWatch is a real-time, interactive dashboard that filters traffic in a way that instantly brings the most critical information on active users and connections to the surface. FireWatch enables you to see what is using the most bandwidth and which sites and applications are most popular.

Health Reports

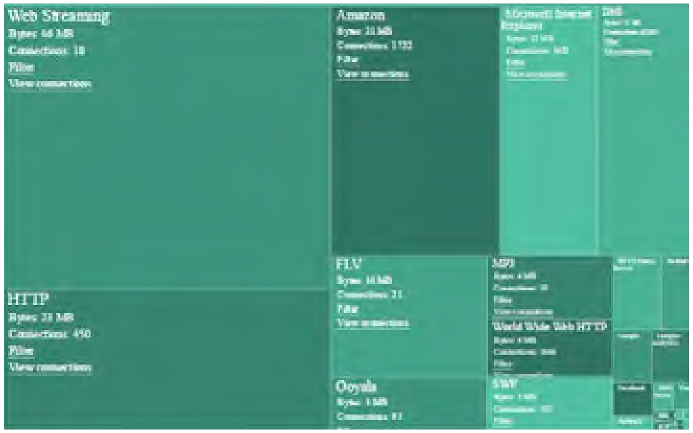
A preventative resource, Health Reports allow you to identify potential issues before they become real problems. CPU, memory, and physical interface usage are all critical factors in achieving maximum uptime. Without visibility into these health statistics, organizations are at risk of overloading and inadvertently disabling network equipment.

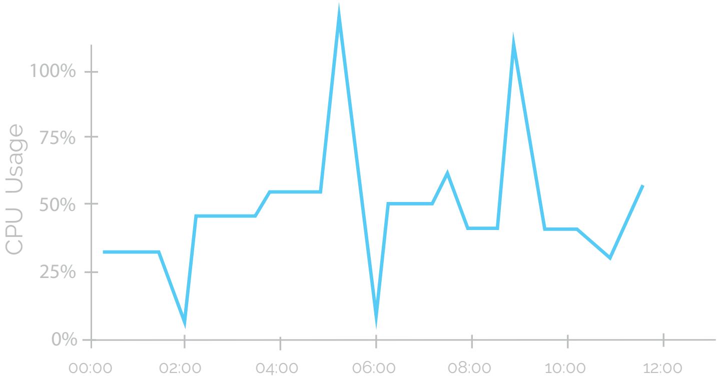
Policy Map

Policy Map displays a policy's impact across the network, making it easy to identify misconfigurations. Policy Map also displays the overall flow of network traffic, and it allows admins to filter and pivot data to reveal richer details.



NAME	RATE ▾	BYTES	HITS
Mary	681 Kbps	77 MB	212
John	27 Kbps	4 MB	21
Trevor	7 Kbps	11 KB	28
Kyle	2 Kbps	151 KB	7
Jenna	264 bps	35 KB	3
Martha	224 bps	555	3



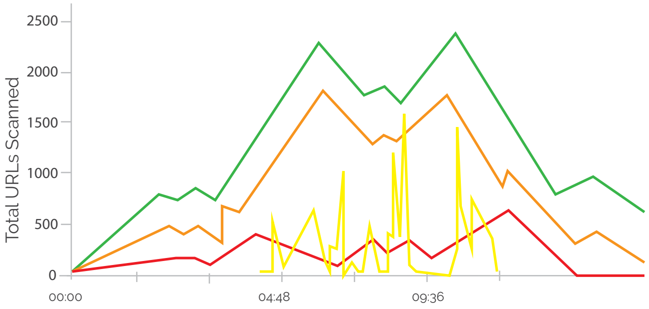


Blind Spot: Network Activity

Solution: WatchGuard Dimension

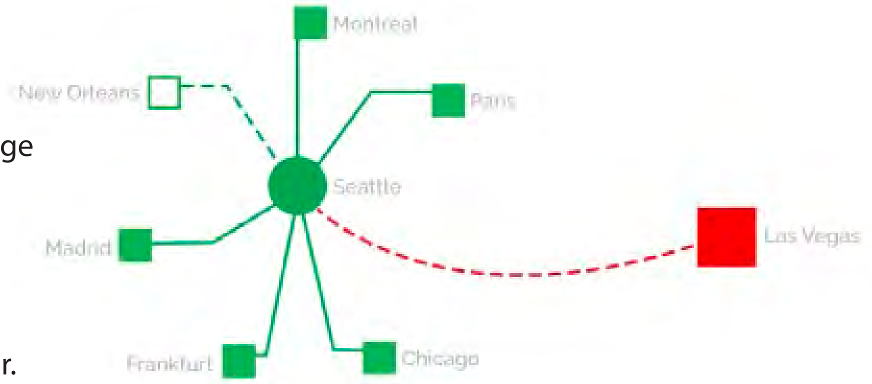
Subscription Services Dashboard

The Subscription Services Dashboard gives you a comprehensive performance summary with statistics that show the results of what has been scanned by a Firebox®. It also allows you to deliver that information in an easy-to-digest format for non-technical users.



Policy Usage Report

The Policy Usage Report provides valuable insight into how frequently policies are used. This report enables you to keep firewall policies current and eliminate those that are unnecessary. Unused policies present a security flaw as hackers may leverage them to infiltrate the network.

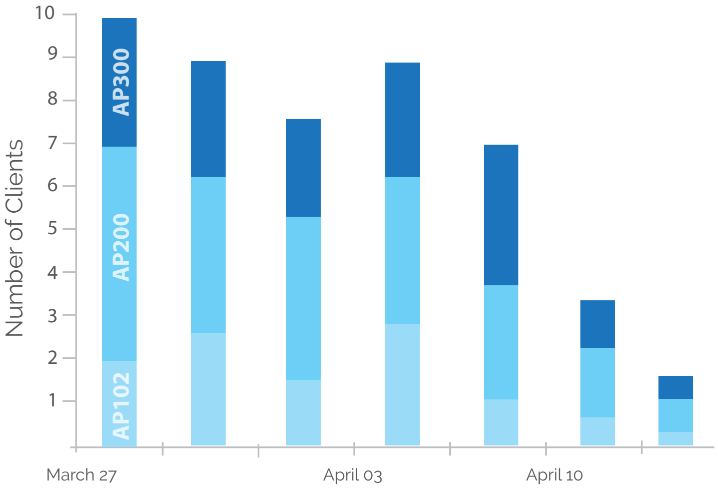


Hub & Spoke VPN

Monitoring the status of secure connections to branch offices has never been easier. Organizations can establish and manage VPN tunnels quickly and easily within Dimension's Hub & Spoke VPN builder.

Access Point Dashboard

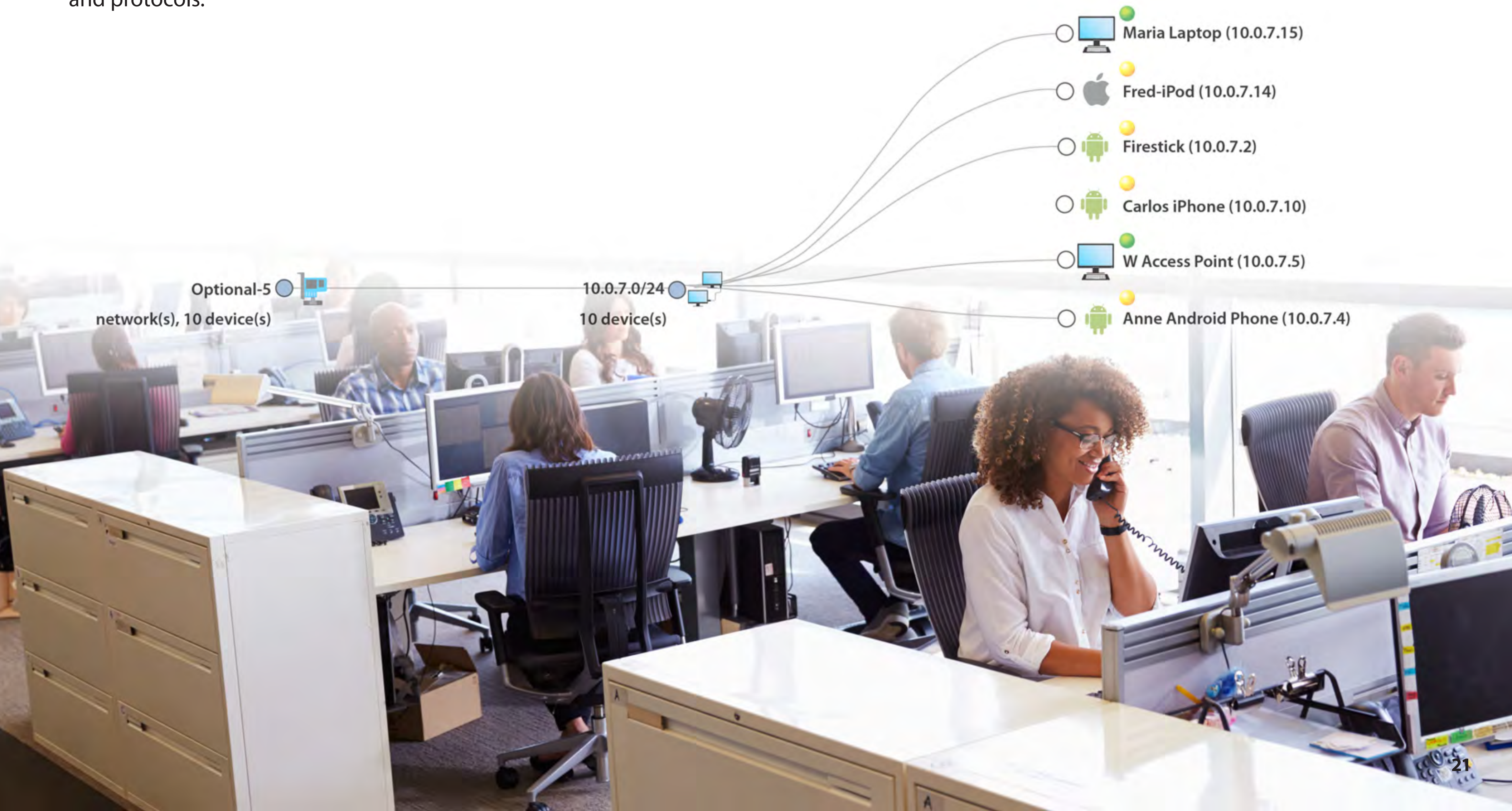
One of the most common security blind spots within an organization comes from its wireless network. The AP Dashboard displays valuable information for connected access points, including a chart with pivot options to see the number of bytes and clients on an AP device.



Blind Spot: Connected Devices

Solution: WatchGuard Network Discovery

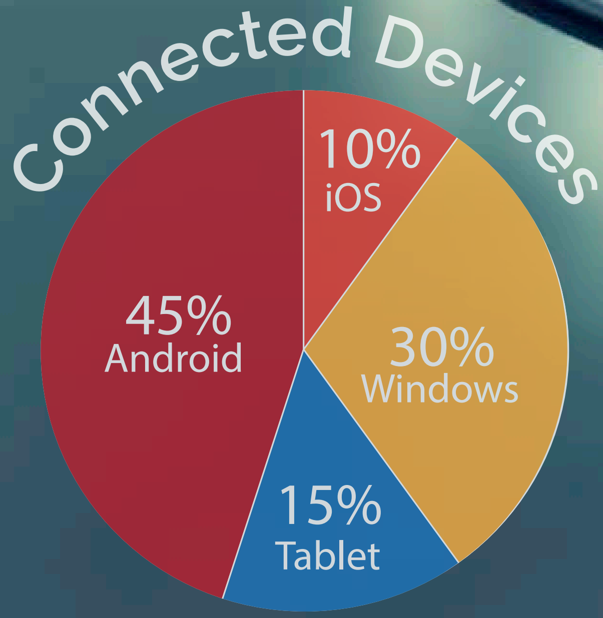
Scanning your network for unauthorized devices is a critical step in truly understanding your network. WatchGuard's Network Discovery subscription service preforms a complete network scan that generates a visual map of every connected device, providing you with total visibility into all connections. With Network Discovery, organizations can ensure only authorized devices are connected while detecting all open ports and protocols.

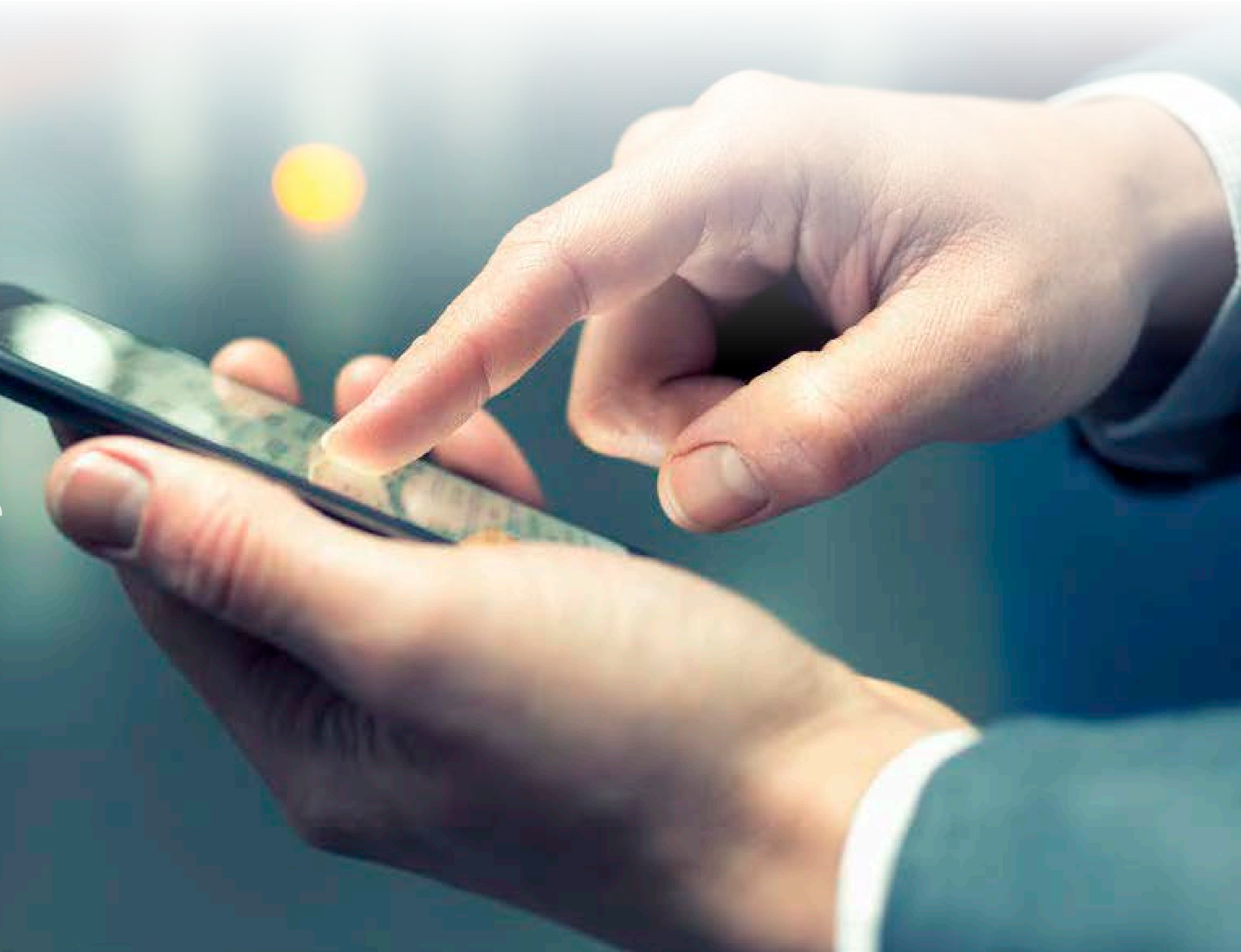


Blind Spot: Mobile Devices

Solution: WatchGuard Mobile Security

WatchGuard's Mobile Security subscription service delivers an additional layer of network visibility by enabling administrators to identify and audit mobile devices attempting to connect to their network. Prevent access to rooted or jailbroken devices’ and block those that download applications from unauthorized sources.

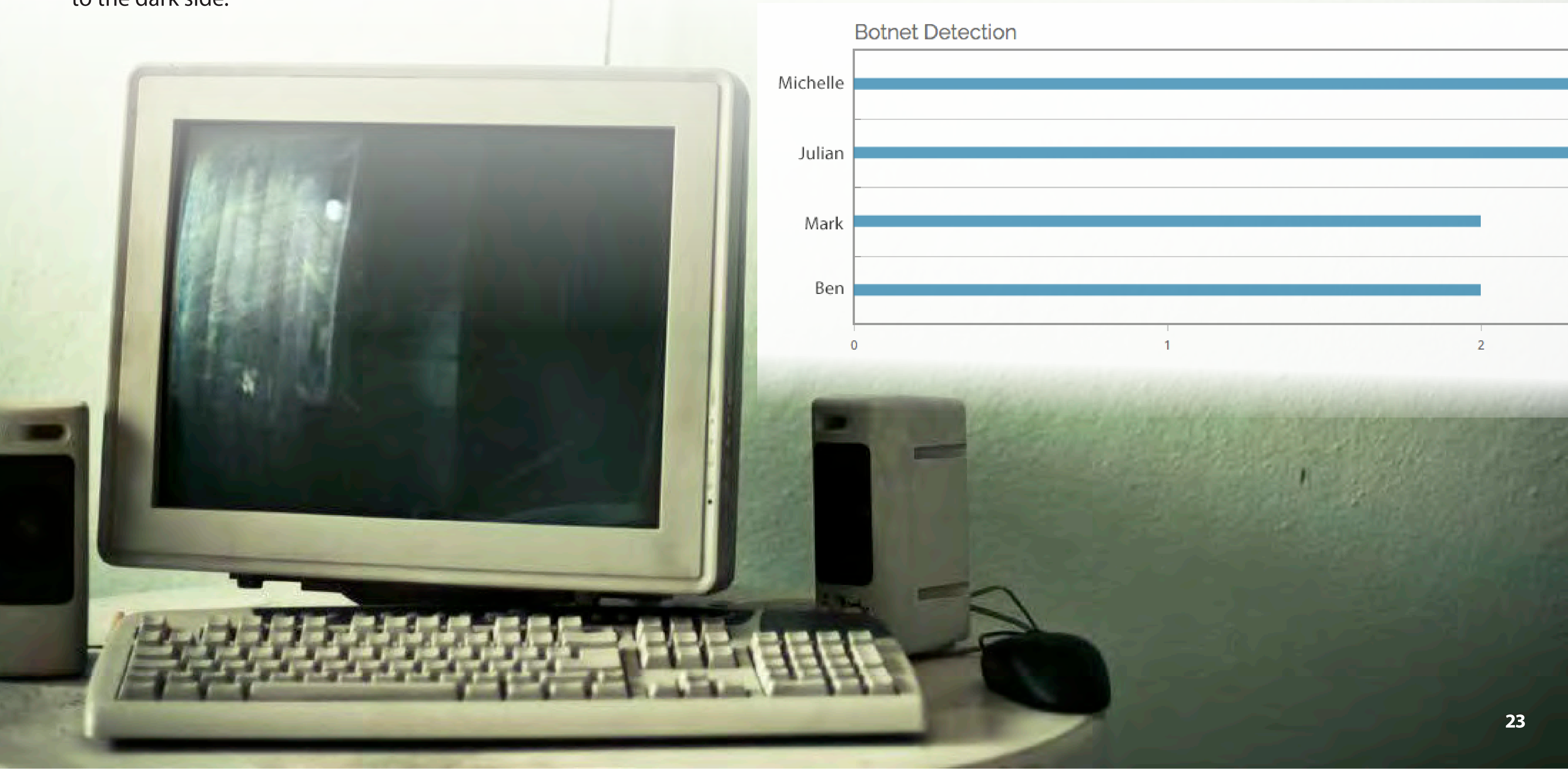




Blind Spot: Botnets

Solution: WatchGuard Reputation Enabled Defense (RED)

Networks of infected computers, known as a botnet, are used by cyber criminals to attack or infiltrate a specific target. Unsuspecting employees inadvertently join botnets after falling victim to a drive-by download or a cleverly crafted phishing email. As soon as the malicious code enters an employee's computer, the botnet master can use the compromised device as an additional soldier in their nefarious regime. Without visibility into this web of fallen machines, you are unknowingly supporting soldiers on a campaign of terror. With WatchGuard's integration of Botnet Detection into the Reputation Enabled Defense service, organizations gain real-time visibility into infected clients and the sites which beckon them to the dark side.



WatchGuard®

"We talk about visibility as the missing layer of information security, but really, it's more like night vision goggles. It allows you to see into areas that were previously just a shadowy void. No matter how good your security may be, the threat landscape will continue to evolve. Since you can't stop every attack, you need to have mechanisms that help you see, analyze, and respond to them before it's too late."

Corey Nachreiner, chief technology officer at WatchGuard

WatchGuard® Technologies, Inc. is a global leader of integrated, multi-function business security solutions that intelligently combine industry-standard hardware, best-in-class security features, and policy-based management tools. WatchGuard provides easy-to-use, but enterprise-grade protection to hundreds of thousands of businesses worldwide. To learn more, visit **WatchGuard.com/visibility**.

1. SANS Institute, "Ninth Log Management Survey Report", October 2014

2. Ponemon Institute, "The Post Breach Boom"

3. Ponemon Institute, "2014: A Year of Mega Breaches

4. Ponemon Institute, "2015 Cost of Data Breach Study: Global Analysis"

5. Verizon, "2014 Data Breach Investigations Report"