4 Actionable Ways to

Simplify

Your Security

WatchGuard®

Table of Contents

Introduction

As cyber threats continue to grow in sophistication and complexity, it's only natural that businesses are consequently seeking more powerful and complex cyber defenses. The problem with scaling security by way of complexity? Your resources – time and staffing principal among them – don't automatically scale as well.

A fully loaded tool box is not much use without someone to swing the hammer – likewise, even the most robust security infrastructure cannot manage itself. Unfortunately, IT department staffing shortages are an industry-wide challenge and show no signs of slowing down – **a staggering 53% of IT professionals worldwide are struggling with a critical deficiency of cyber security skills within their business**[1]**.** Those roles that are aptly filled within the department are spread thin, struggling to fulfill daily responsibilities while juggling constant alerts and support tickets.

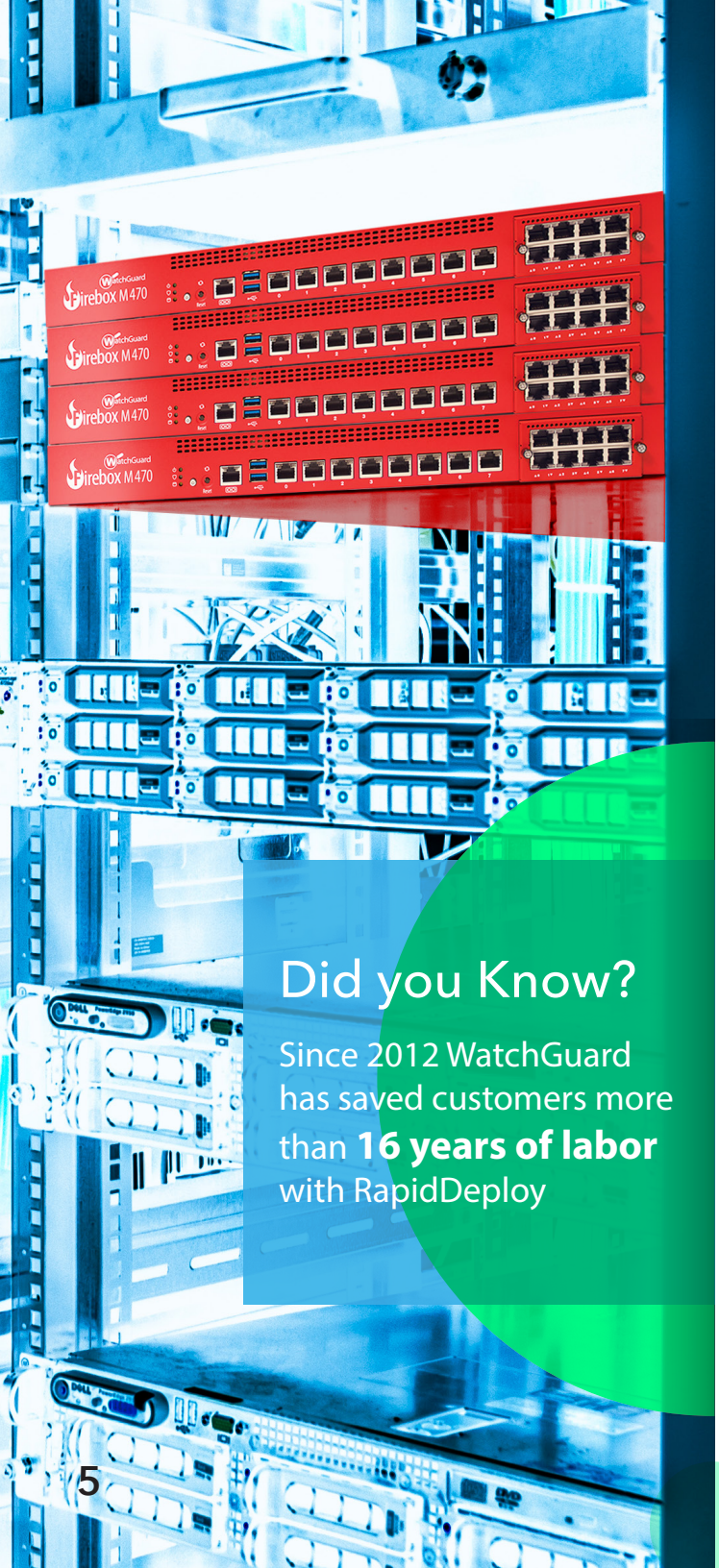
If this all sounds a little too familiar and simplified security is feeling out of reach at your organization, read on for four actionable ways to simplify your cyber security.

Complicated

Managing disparate, single-point solutions:

It's early on Monday morning and you receive a support ticket from Marketing: "Can't access business-critical document on file-hosting site. PLEASE FIX ASAP." You sigh, take a sip of coffee, (then another) and prepare to spend the next half hour navigating your configuration, plodding through five different screens in order to complete a simple URL exception. With growing collections of settings, commands, and disparate tools to manage, this scenario plays out all too often for many network admins, consuming far too much valuable time.

Think of it this way: if you have three or so email accounts (a work address, a personal address, and maybe an address dedicated to spam) it's probably easy enough to maintain your inboxes and parse-out the important messages ("Grandma's 80th birthday!", a note from the CEO, etc.) from the junk. Now imagine you have 100 accounts to monitor, all of which could hold critical communications at any point in time. Not so easy anymore.



Did you Know?

Since 2012 WatchGuard has saved customers more than **16 years of labor** with RapidDeploy

Simple

Centralized Management:

Invest in easy-to-configure, -deploy, and -manage products

The solution: You have enough on your plate without adding constant alerts to manage and a small army of screens to monitor. Look for network security products that enable ongoing management from a single, intuitive UI. WatchGuard Firebox appliances are not only easy to initially configure and deploy, they are also designed with an emphasis on centralized management from one console, making ongoing policy and network management simple and straightforward.

Easy to configure: Make one-touch configuration or firmware updates to all managed WatchGuard appliances to save time and ensure policies are synchronized across a distributed organization. Create policy templates from anywhere and quickly push them to multiple appliances using role-based tenants.

Easy to deploy: WatchGuard RapidDeploy is a powerful, Cloud-based deployment and configuration tool that comes standard with WatchGuard Firebox appliances. All you have to do is power up the appliance and connect it to the Internet – the rest can be taken care of remotely from any location.

Easy to manage: Manage one Firebox appliance or hundreds from one easy-to-use console, maximizing efficiency and streamlining network administration. A clear, visually driven interface and plain-language log messages keep the guesswork out of building and maintaining a strong security and compliance posture.

Complicated

Manually parsing through oceans of data

As our IT infrastructures grow in size and complexity, granular visibility into activity across the network is crucial – enabling IT teams to recognize patterns, threats, and security gaps, and to respond before damage occurs. This data is invaluable, however – it's of little consequence if key insights aren't readily available and actionable for your security team.

Many network visibility solutions on the market today deliver on large volumes of data – but with little consideration for priority ranking. This approach is overwhelming for most security teams, tasked with constant and seemingly never-ending queues of security alerts – which simply cannot all be investigated or prioritized. A truly effective visibility product will recognize the bandwidth limitations inherent to many IT teams and effectively spotlight the most critical events in order to maintain the health of the network.

Did you Know?

38% of IT and networking professionals feel they cannot proactively identify network performance issues[2]

Simple

Actionable Data:

Utilize automated visibility and reporting solutions

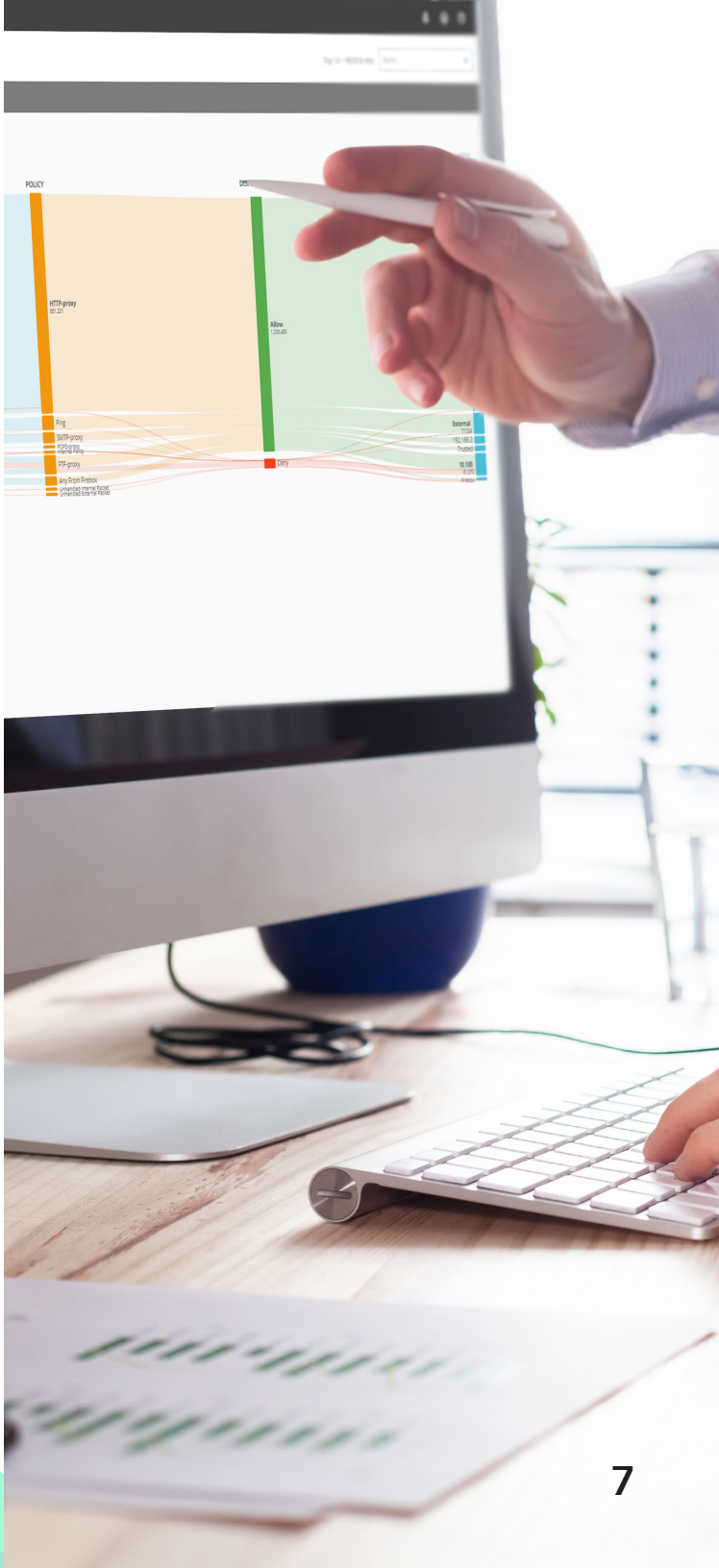
The solution? An automated, intuitive reporting dashboard will help prevent your IT team from wasting time and resources on low-risk events. WatchGuard Cloud Visibility offers swift, reliable, and actionable insights so that IT teams can quickly spot patterns and make informed decisions. With built-in dashboards and reporting features you can rapidly gather information on security events, compliance audits, and patterns on the network. As a Cloud platform, you can monitor and gain critical insights about your network security in real time, from anywhere, and at any time. Better yet – there's no hardware infrastructure required. How easy is that?

WatchGuard Cloud Visibility provides executive-level insights on your network, such as:

- Top users
- Top destinations
- Top applications
- Top domains

View your latest Firebox security information, such as:

- Top blocked botnet sites
- Top blocked clients and destinations
- Top blocked advanced malware attacks
- Intrusion preventions



Complicated

Unsecured, poor-performing Wi-Fi

For all of the efficiencies Wi-Fi access offers modern businesses – from Bring Your Own Device (BYOD) programs to mobile workforces – it also invites significant security concerns into your corporate network. The web now offers a virtual cornucopia of Wi-Fi hacking resources – including step-by-step "how-to" videos on YouTube – arming even the most novice of cyber criminals, and helping to propagate the six known Wi-Fi threat categories.

With many IT teams already dedicating considerable resources to Wi-Fi-related issues – forgotten passwords on mobile applications, email syncing, and difficulty accessing wireless networks to name a few – most do not have the bandwidth to deploy multiple solutions to protect against each of the six wi-fi threat categories – let alone maintain them. You need a single solution – both easy to deploy and manage – that not only supports the performance requirements of your unique environment, but also protects simultaneously against each of the Wi-Fi threat categories.

Did you Know?

The average global BYOD (Bring Your Own Device) user saves 37 minutes at work per week by using their mobile device.[3]

Simple

Stronger, Safer Wi-Fi:
Offer a Trusted Wireless Environment

The solution: Efficient, secure Wi-Fi connectivity doesn't have to be complicated. WatchGuard is the only company that offers a Miercom-verified framework for building a complete Wi-Fi network that is high-performing, simple to manage, and proven to defend against the six known Wi-Fi threat categories. Better still, WatchGuard Secure Cloud Wi-Fi-managed environments benefit from WatchGuard Discover, an application within the Wi-Fi Cloud that offers valuable insight into performance and health within the network. A complete set of actionable visibility, troubleshooting, and network health features are included with Discover, such as:

Client Journey: a live snapshot across all your locations to quickly see clients experiencing association, authentication, or network failures unrelated to Wi-Fi but still impacting their experience on the network.

Network Baselining: every client and AP within range of your networks is tracked for performance, connectivity, and application experience to establish what's normal and abnormal. When an anomaly is detected, Discover provides full visibility to identify the root cause, leading you to recommendations to resolve network problems, even those unrelated to Wi-Fi.

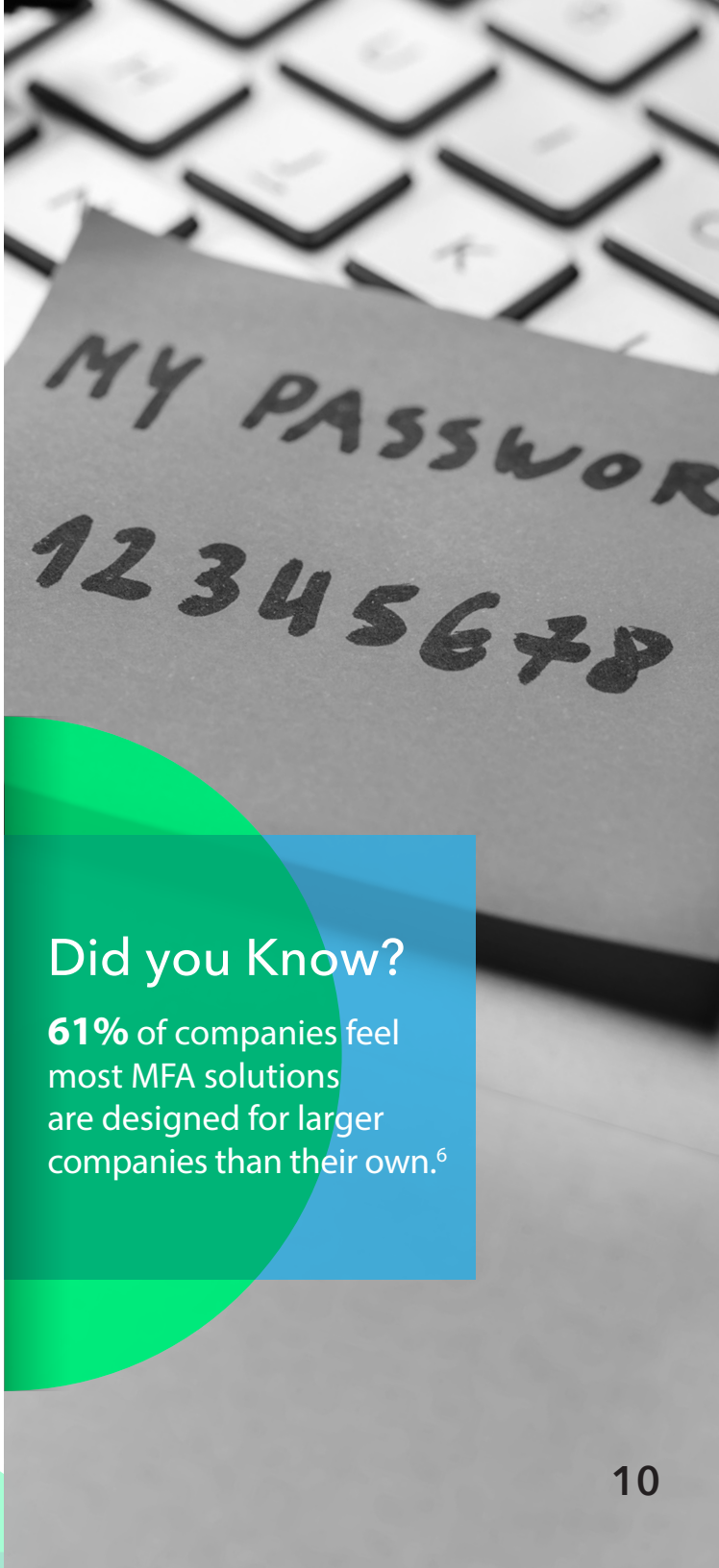
Alerts: maintaining Service Level Agreements (SLAs) is a breeze using the Alerts feature within Discover. Keep your Wi-Fi, wired, and application network resources running smooth.

Complicated

Resource-intensive MFA rollouts

Password security is one of the biggest challenges facing organizations today, with a staggering **81% of data breaches caused by weak or stolen passwords**[4]. Subsequently, businesses are evaluating multi-factor authentication (MFA) products for additional layers of security around access to corporate resources.

Unfortunately, many MFA products have proven difficult for IT teams to manage. Traditional hardware-based MFA rollouts consume time and resources, making it difficult to balance the implementation with existing priorities – let alone incoming service tickets. Many MFA rollouts also require significant training commitments from your IT team and staff alike, as one of the most common complaints with traditional solutions is usability (or lack thereof.) **In fact, 24% of companies that aren't using an MFA solution note difficulty with implementing, maintaining, and supporting it as their gating factors to adoption**[5]**.**



Did you Know?

61% of companies feel most MFA solutions are designed for larger companies than their own.[6]

Simple

Cloud-based MFA:

Enjoy hardware-free, user-friendly identity verification

The solution? MFA that's not only easy and cost-effective to deploy, but intuitive and user-friendly for all employees, regardless of technical savvy. WatchGuard's AuthPoint provides multi-factor authentication (MFA) on an easy-to-use, Cloud-based platform. Since it's based in the Cloud, there's no hardware to deploy and access can be managed from anywhere. The mobile app makes each login attempt visible and easy for users to approve or deny logins. AuthPoint also features many 3rd party integrations, including popular Cloud applications, web services, VPNs, and networks.

Simple

Delegation:

Partner with an MSSP (Managed Security Services Provider)

All WatchGuard products are designed with simplicity in mind to help give you back time in your day. However, if managing your business's security simply isn't an item you have room for on your to-do list, working with one of our IT solution providers can take that burden totally off your plate. A WatchGuard solution provider can work as an extension of your business to fill any IT security gaps through managed service offerings such as deployment, ongoing maintenance, reporting, and more.

Connecting with an MSSP couldn't be easier with WatchGuard's Partner Finder tool, available through watchguard.com/findapartner. Search by location, then filter your results by distance or specialization to find the WatchGuard-certified partner that best fits your business's needs.

Conclusion

Limited time and resources can make managing your organization's IT security feel beyond reach. Luckily, WatchGuard solutions are designed with an emphasis on simplicity: in configuration, deployment, and ongoing management. Your network is complex enough – your security doesn't have to be.

Network Security

In addition to delivering enterprise-grade security, our platform is designed from the ground up to focus on ease of deployment, use, and ongoing management, making WatchGuard the ideal solution for SMB, midsize, and distributed enterprise organizations worldwide.

Secure Wi-Fi

WatchGuard's Secure Wi-Fi Solution, a true game-changer in today's market, is engineered to provide a safe, protected airspace for Wi-Fi environments, while eliminating administrative headaches and greatly reducing costs. With expansive engagement tools and visibility into business analytics, it delivers the competitive advantage businesses need to succeed.

Multi-Factor Authentication

WatchGuard AuthPoint® is the right solution to close the password-driven security gap that leaves companies vulnerable to a breach. It provides multi-factor authentication on an easy-to-use Cloud platform. Our unique approach adds "mobile phone DNA" as an identifying factor to ensure that only the correct individual is granted access to sensitive networks and Cloud applications.

Find a Partner >

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Pacific, and Latin America. To learn more, visit WatchGuard.com.

[1] StationX, "Predictions for 2019: Cybersecurity skills shortages are getting worse", January 2019
[2] APM Digest, "Here's why IT teams spend too much time on network troubleshooting", March 2019
[3] Information Age, "The relationship between Wi-Fi and BYOD culture", April 2017
[4] CSO, "Hacked passwords cause 81% of data breaches", May 2017
[5] WatchGuard, "Passwords have failed, so what's next?", May 2018
[6] WatchGuard, "Passwords have failed, so what's next?", May 2018

WatchGuard

North America Sales: 1.800.734.9905 • International Sales: 1.206.613.0895 • Web: www.watchguard.com