PROTECTION BUILT FOR YOUR BUDGET AND STAFF:

Security Solutions for the Midsize and Distributed Enterprise

WatchGuard®

INTRO

Technology has changed every aspect of our lives. From the way we communicate and socialize to how we do business, advancements like the Cloud and machine learning have impacted us in more ways than we can count.

Today, most businesses have to worry about offices, employees and data living and working outside of the confines of the headquarters.

As a midsize or distributed enterprise organization with operations and employees spread out across cities, states, even countries, there are innate challenges that your IT teams must overcome. Your business faces unique challenges and cookie-cutter enterprise solutions don't provide the protection, management or price tag that your business requires.

Unique challenges require a unique solution. Let's take a closer look at the challenges your business is facing and the specific ways you can address them, ensuring that you're able to keep company resources protected, without adding to your cost and complexity?

63%

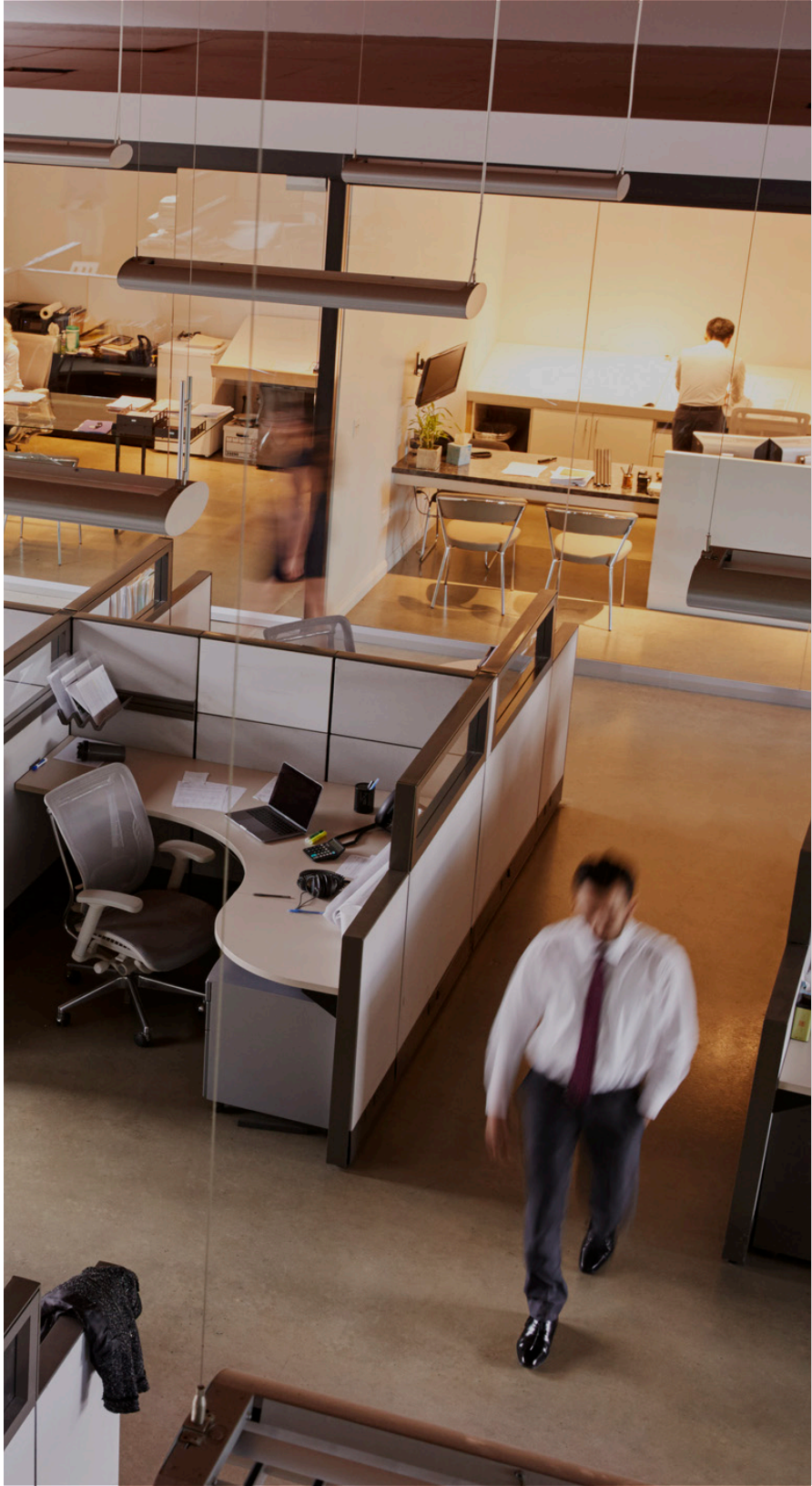
of companies have people within their organization who spend a portion of their time working remotely.

Upwork

SECURITY

Midsize and distributed enterprise organizations are struggling to find the right fit between "good enough" security and the security solutions they really need, but often can't afford or manage. As the threat landscape continues to evolve, organizations of all sizes require solutions that will advance to keep up with the next generation of attacks.

The natural distribution of business operations and employees also presents unique security challenges. It's critical for these organizations to have consistent security protection for every part of their business to ensure that they aren't a victim of the next big breach. Remote sites and employees generate an entire new level of risk, and hackers are using them as an easy entry point into the main hub of data.



24%

of midsize enterprises cite the lack of necessary IT skills as one of their top three challenges

Gartner

STAFFING

It is increasingly challenging to find skilled IT resources – and it's even harder to keep them. 21% of midsize enterprise organizations report that security is the biggest skills gap in their IT department.

Additionally, because skilled IT resources are so hard to come by there's a lot of competition to keep these valuable employees. In their annual "State of IT" report, Spiceworks reports that 36% of IT pros are expecting to get a raise in 2019, while 26% are planning to find new job in IT in the coming years. With CIO reporting that by 2020 there will be 1 million unfilled job openings in the tech sector while universities are only graduating 400,000 computer science students, around 60% of tech jobs are expected to go unfilled.

BUDGET

Midsize and distributed enterprise organizations often face the same challenges and risks as their larger counterparts, but without the enterprise-sized budgets. In fact, 34% of these businesses list a relatively smaller budget as a one of their top 3 challenges for 2019.

And while 45% of business with between 500 and 5,000 employees expect an IT budget increase for 2019, it certainly won't be enough to meet all of their budget needs (Spiceworks). From updating hardware to deploying new Cloud services to ensure the right security solution to protect from a breach, there are many different ways that increased budget could be prioritized.

SO, WHAT ARE SOME OF THE CORE CHALLENGES THAT MIDSIZE AND DISTRIBUTED ENTERPRISE ORGANIZATIONS OFTEN FACE?

Let's take a closer look at the top three.

CHALLENGE #1:

REMOTE SITES, BRANCH OFFICES, FRANCHISE LOCATIONS – OH MY!

Whether you're a retail organization with stores across the country, a regional bank with branch offices throughout the area, or a community college with buildings across campus, you need a way to protect the locations that fall outside the boundaries of your main firewall. This can be particularly important as these remote sites are often connected to the headquarters through shared network drives, making them an entry point for hackers trying to make their way into your main source of data.

You know you need to set up security protections at these locations, but that ultimately adds to your cost and complexity.

Cost of Deployment: Like most distributed enterprise organizations, you don't have an IT resource based at each of these sites. So, your option is to send out one of your limited team members to set up the new solutions OR configure them at your HQ, ship them out, and then walk through a likely long and tedious remote set-up. Neither of these is really a great option and can end up costing you time and money.

Cost for Performance: Any business with multiple locations needs to make sure that each site has the performance necessary to make effective use of VoIP, video and other business critical applications. But bills from Internet service providers (ISPs) and multiprotocol label switching (MPLS) services can escalate out of control. You need a solution that keeps costs at bay, while providing the high network performance for every location.

Complexity: Whichever deployment route you choose, you're now faced with the new challenge of figuring out how they're going to be managed. You know it's important to keep up with what's happening at each location, but you also need visibility into your security as a whole. Do you have to log into to multiple dashboards to keep an eye on each site individually? Will you need to implement a SIEM solution just to have deep visibility into your security? This can all make managing the security for your overall business increasingly complicated.

SOLUTION #1:

REMOTE DEPLOYMENT & CENTRALIZED MANAGEMENT

Savings on Deployment: What if I told you there was a way to deploy solutions to remote sites from the comfort of your own cozy office? With WatchGuard RapidDeploy, you can pre-configure any Firebox appliances from HQ and then ship them out to your remote site, wherever it may be. Once the appliance gets to the site, plugged in and connected to the Internet, configurations are automatically downloaded and the Firebox is ready to go!

The same is true for our Secure Cloud Wi-Fi platform. Simply log into the Cloud management platform and set pre-configurations for things like Wi-Fi settings, security policy, scheduled reports, and anything else that is important for your business. Then, once the access point reaches its final destination, it just needs to be plugged in and the configurations are downloaded to the AP just as you've set them.

Our WatchGuard AuthPoint solution leverages a mobile app-based token, saving cost and time in getting employees, even those outside of the headquarters, set up on the multi-factor authentication (MFA) platform. All they need to do is download the app, receive the activation email, scan the QR code and they're in.

Savings on Performance: SD-WAN solutions offer dynamic WAN selection to ensure high performance experience for every site while stabilizing Internet service costs at the same time. SD-WAN comes standard with each Firebox network security appliance – no additional purchases are required. Our appliances measure the performance – including jitter, latency and packet loss – of multiple WAN options to automatically select the optimal Internet connection for each type of office location.

Simplicity: WatchGuard offers Cloud-management options for all of our security platforms making it possible for you not only gain visibility into your organization's security as a whole, but to drill down into the data for remote locations as well.

With WatchGuard Dimension, included with every Firebox purchase, have clear visibility into network security threats, issues and trends across all locations around the world. Our WatchGuard Wi-Fi Cloud provides intelligent visibility into the threats and devices connected to your wireless network, making it easy for you to answer, "Why isn't the Wi-Fi working?!" Last but not least, our multi-factor authentication solution, AuthPoint, is entirely Cloud-managed and makes it easy to provision licensing, monitor declined authentication requests, and manage SSO portals and integrations.

CHALLENGE #2:

THE REMOTE EMPLOYEE INVITING UNWANTED RISK

As complicated as securing a remote site can be, protecting the remote employee can be even more challenging – they're rarely behind a firewall and often connecting to public, unsecure Wi-Fi networks. They can often be more susceptible to malware attacks as well if they're only protected by whatever AV is on their device. As these remote employees make stops in the office and connect to the network, whatever "computer illnesses" they've caught in the field can make their way to your network.

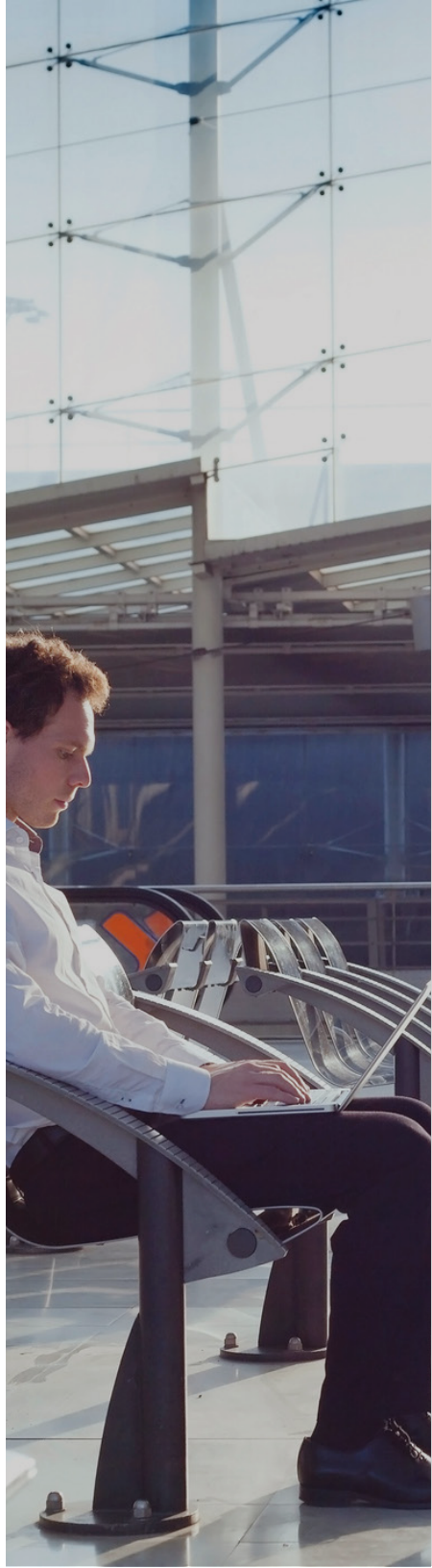
As the number of employees in your organization operating outside of the office continues to grow, you need a way to keep them secure that decreases the friction of adoption and cause you to incur too much additional cost.

Additional Risk: Protecting remote employees can be particularly difficult as they're often more susceptible to ransomware threats and phishing attacks as they're not operating behind the firewall. You need a way to offer these employees additional protection without increasing your bottom line.

Adoption: One way that organizations often try to protect remote employees is by requiring them to leverage VPN to access and share data when they're not connected to the network. While this can help improve security, it can also be challenging for end users as these connections often drop and need to be restarted regularly.

In general, deploying new solutions or setting new security policies can be difficult to implement and enforce for remote employees. Even if remote employees attend training sessions or seem to be following instructions, it can be challenging to truly enforce security best practices to those at your headquarters, let alone those outside of it.

Additional Cost: Managing the budget for your headquarters and remote offices is one thing but keeping up with the cost for every employee working outside of it can be challenging. Solutions like multi-factor authentication that require hardware tokens per user can really start to add up. You need to consider the solutions that not only decrease user friction but keep costs low through your ENTIRE deployment.



SOLUTION #2:

PROTECTION OFF-PREMISES, EASY TO USE AND COST EFFECTIVE

Extra Protection: WatchGuard Total Security Suite offers a variety of protection for off-premises employees including Host Ransomware Prevention, which tracks behaviors and blocks threats before file encryption takes place.

Simple and Easy to Use: If security solutions are too complicated to use or create too much additional work for your employees, they aren't likely to use them. You can continue to push policies at them, but you'll still have outliers that can't seem to get onboard. WatchGuard solutions are designed with ease of use in mind. From our IPSec VPN client that makes connecting with a VPN a breeze, to our phishing protection service, DNSWatch, which provides on-the-spot education at the time of an attack, our solutions help to protect your employees wherever they are.

Cost-Effective: Our AuthPoint solution leverages a mobile app, easily downloaded from an app store and set up using a QR code scan. No need to carry key fobs or thumb drives; instead employees use the phone that's already in their hand. Not only is this more convenient for your employees, it cuts down on your cost as well!

CHALLENGE #3:

REGULATORY COMPLIANCE CAUSING HEADACHES

Regardless of the business you're in, it's likely there's at least one compliance regulation that's always on your mind. Whether you're studying up on the latest changes to HIPAA and PCI DSS or you're catching up on the newest regulation like GDPR, there always seems to be some new security hoop your company needs to jump through. Maintaining regulatory compliance is just part of your job, but it can take a lot of your time.

Keeping up with compliance is also something that can add to your bottom line and distract your already-limited resources. With every update or change to a regulation, your team is stuck figuring out how to fit new technologies into the budget, and how to get them implemented without adding complexity to your already-disparate IT infrastructure.

Cost: When it comes to keeping up with compliance, you don't have a lot of options. It's either spend the money upfront to add in security solutions to meet the standard or face hefty fines after the fact. Either way isn't a great option and certainly doesn't help you manage your budget.

Complexity: As new regulations are rolled out, or changes are made to existing ones, you're tasked with making sure your infrastructure can keep up. But the more solutions you deploy to remote locations, the more challenging it can be to manage them effectively.

SOLUTION #3:

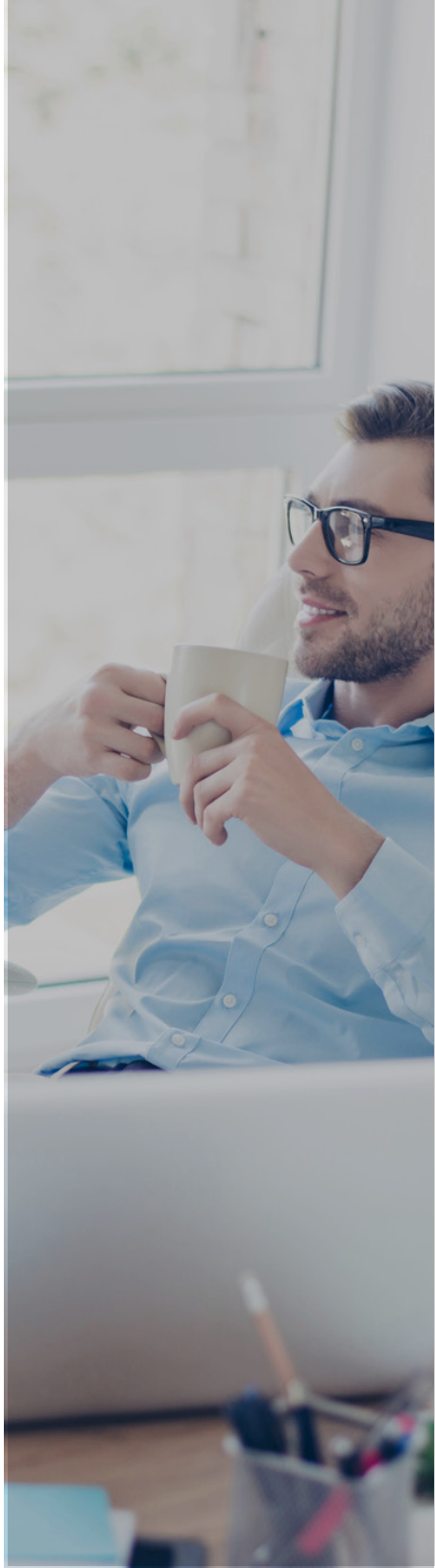
COMPLIANCE CHECKLIST AND CENTRALIZED MANAGEMENT

Compliance: You need a solution that enables you to check multiple boxes through one deployment. WatchGuard Total Security Suite offers 10+ security services through one license and one management platform, which means you can check off multiple compliance regulations with just one license.

WatchGuard also offers security solutions for Secure Wi-Fi and MFA which can help to check even more boxes on your compliance list, as technology protection for passwords and Wi-Fi is increasingly being added to compliance regulations. Working with one vendor gives you one place to go for anything you need – from resources and getting started guides to support and product assistance.

Simplification with Centralized Management: WatchGuard makes it easy to manage all of your sites and offices through our Cloud-managed platform. WatchGuard System Manager, available with every Firebox appliance is an out-of-the-box platform that enables you to centrally manage all the Firebox appliances in your network using one easy-to-use console. Leverage WSM monitoring and management tools to quickly apply configuration changes to your Firebox appliances in real time or as a scheduled task. Our Dimension Platform also offers out-of-the-box reporting for major regulations like PCI DSS and HIPAA.

Furthermore, our other security platforms, including Secure Wi-Fi and AuthPoint, are all managed through the Cloud, making it easy to deploy, administer and report on your security solutions wherever business takes you.



So, if we take another look at the core challenges facing midsize businesses and distributed enterprise organizations – Security, Staffing and Budget – it's easy to see how WatchGuard is the right solution for you!

Security: WatchGuard offers the security solutions you need without the enterprise-grade bells and whistles you don't want. Our Firebox appliances with Total Security Suite provide robust protection across your network against known, unknown, and even evasive threats. Our Secure Wi-Fi platform is the only solution in the market today that detects and prevents the six known Wi-Fi threat categories targeting your business. And last but not least, protect weak and mishandled passwords with WatchGuard's multi-factor authentication solution, AuthPoint, which is designed to meet the needs of YOUR business and not the large enterprise.

Staffing: All three of WatchGuard's security platforms are easy to deploy, use and manage. From pre-configuration of access points and Firebox appliances to web logins from anywhere in the world, you don't need a team of security experts to set up or manage our solutions. Our Cloud-based management solutions make your IT team look like a well-oiled machine with real-time visibility, actionable analytics, and pre-defined and customizable reporting templates. Want to work with a Managed Security Service Provider (MSSP)? WatchGuard's extensive partner network is sure to have the right MSSP for your business to make managing your IT even easier!

Budget: WatchGuard's products are designed, licensed and priced for the small business and midmarket. We're not going to make you pay enterprise prices to get the same level of security. We have the right package to meet the needs of your business – with nothing you don't need – with just one SKU per platform.

WHAT ARE YOU WAITING FOR?!

Learn more about why WatchGuard is the right fit for the midsize and distributed enterprise today!

PROTECT YOUR BUSINESS • PROTECT YOUR ASSETS • PROTECT YOUR PEOPLE

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, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

Global Headquarters
United States
Tel: +1.800.734.9905
Email: sales@watchguard.com

European Headquarters
The Netherlands
Tel: +31(0)70.711.20.85
Email: sales-benelux@watchguard.com

APAC & SEA Headquarters
Singapore
Tel: +65.3163.3992
Email: inquiry.sea@watchguard.com

©2018 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, AuthPoint, DNSWatch, Dimension and Firebox are trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners.
Part No. WGCE671405_010219