



## Dollars and Cyber-Sense: Your Finance Security Planner

[WWW.WATCHGUARD.COM](http://WWW.WATCHGUARD.COM)

# Table of Contents

Introduction. ....3

Partnering with FinTech to Support Digital Banking Experiences.....4

Pressure from Consumer Expectations and Compliance Regulations Alike.....6

Increased Risk from 3rd Parties.....9

# INTRODUCTION

Financial institutions have long employed tried and true – and reliably profitable – business models but are now experiencing competition from start-ups seeking to disrupt the market. Crowdfunding, mobile payments, Bitcoin, robo-advisers – today we’re seeing a wealth of “FinTech” (Financial Services Technology) innovations.

Considering these advancements, many financial institutions are eager to jump on the (mobile-optimized, naturally) bandwagon and delight customers with new banking options. But keeping pace with trends does not come without a cost, be it cyber-security ramification or regulatory standards, and many such challenges have fallen upon the IT department to resolve.

In this eBook we’ll address some of the most critical challenges impacting financial organizations today, but furthermore – the key steps that financial organizations of any budget, size, or complexity can take towards more robust cyber security.





# CHALLENGE

## Partnering with FinTech to Support Digital Banking Experiences

By and large, the days of waiting in line at the grocery store while patrons leisurely scribble checks – and provide the veritable rolodex of identification that went along with them – are gone. Today's transactions rarely need a signature, let alone an ID. Perhaps one of the most extreme examples of FinTech at its finest (and most convenient) is stores like Amazon Go – where not just the payment process has been streamlined, but the checkout lines themselves (hint: there aren't any.) Customers simply walk out the door and wait for AI to work its magic and charge their accounts.

Though the industry is rapidly evolving, it's clear that established financial institutions and new FinTech firms will need to work together to continue driving innovation and meeting consumer demand for tools that enable them to pay bills, get loans, receive financial advice, and manage their money online. In fact, data shows that **three-quarters of large financial firms recognize the importance of collaboration with FinTech.**<sup>1</sup> Conversely, where FinTechs are concerned, most need banks as partners to scale quickly enough to compete. One key factor impacting these partnerships, and potentially slowing down the rate of progress needed to remain competitive, however, is cyber security.

While the majority of banks see FinTech partnerships as necessary, **71 percent are also concerned with the cyber risks associated with these new firms.**<sup>2</sup> This is in part because young FinTech companies typically have fewer resources to spend on security or address other regulation requirements.



<sup>1</sup> ComputerWeekly.com, "Cyber security fears are a barrier" April 7, 2017  
<sup>2</sup> Ibid



# SOLUTIONS

FinTech largely relies on applications that can access users' financial profiles to perform transactions, which unfortunately are an increasingly common attack vector. Banks and FinTech must ensure that a robust application security infrastructure is deployed to protect user data – which should include a **firewall** enabled with current **threat intelligence** to identify and mitigate known and unknown threats.

**WatchGuard Firebox®** firewalls are uniquely architected to do just that, leveraging best-in-class security services from the industry's most respected brands, minus the cost and complexity of multiple single-point solutions.

**ThreatSync**, a key component of WatchGuard's Threat Detection & Response service, collects event data from a **WatchGuard Firebox, Host Sensor, and enterprise-grade threat intelligence feeds**, analyzes this data using a proprietary algorithm, and assigns a comprehensive threat score and rank. This powerful correlation engine enables Cloud-based threat prioritization for actionable insights that empower IT teams for quick responses to threats.

## Client related threats

Unauthorized Association	0 Devices	0 Instances
Mis-association	17 Devices	386 Instances
Banned Client	0 Devices	0 Instances

## Ad hoc Networks

0 Devices 0 Instances

## Bridging/ICS Client

0 Devices 0 Instances



# CHALLENGE

## Pressure from Consumer Expectations and Compliance Regulations Alike

Financial institutions face strict expectations from regulators and are subject to an ever-growing set of protocols, putting immense pressure on staff to comply with each requirement. Adhering to regulatory mandates has become a daily focus for financial institutions of all sizes and although meeting these standards is no small task, there is no other option – the cost of non-compliance is much too high. Whether it's steep fines or a debilitating hit to reputation, no company wants to be on the wrong side of regulatory compliance.

On the consumer side, customers expect more channels, more service, and greater capabilities from their online accounts — without compromising on the safekeeping of their data. This sets companies up for serious consequences if they let consumers down by suffering a data breach or by failing to innovate service offerings. Additionally, in the recent wake of what regulators deemed to be significant misconduct and manipulation by financial services providers, financial services companies are facing a renewed rigor to stringently adhere to regulations rather than face the reputational fallout of misconduct.



# SOLUTIONS

Just like any other business, financial organizations should regularly assess the effectiveness of their information security efforts. Often, it's helpful to bring in an outside expert who may be better able to spot potential risks, gaps in compliance, and areas where security could be improved. A **WatchGuard MSSP** (managed security service provider) can provide valuable guidance and may see vulnerable security gaps that your internal teams cannot. Take these findings seriously, escalating to management and ensuring that any underlying compliance issues are identified and addressed.

A monitoring and reporting option for your network is key to achieving – and maintaining – compliance. Visibility across all networks can be achieved with **WatchGuard Dimension**. This built-in tool, which comes standard with every WatchGuard Firebox appliance, provides intuitive reporting methods (such as real-time dashboards) that make it easier to identify threat activity for quick remediation.



# SOLUTIONS

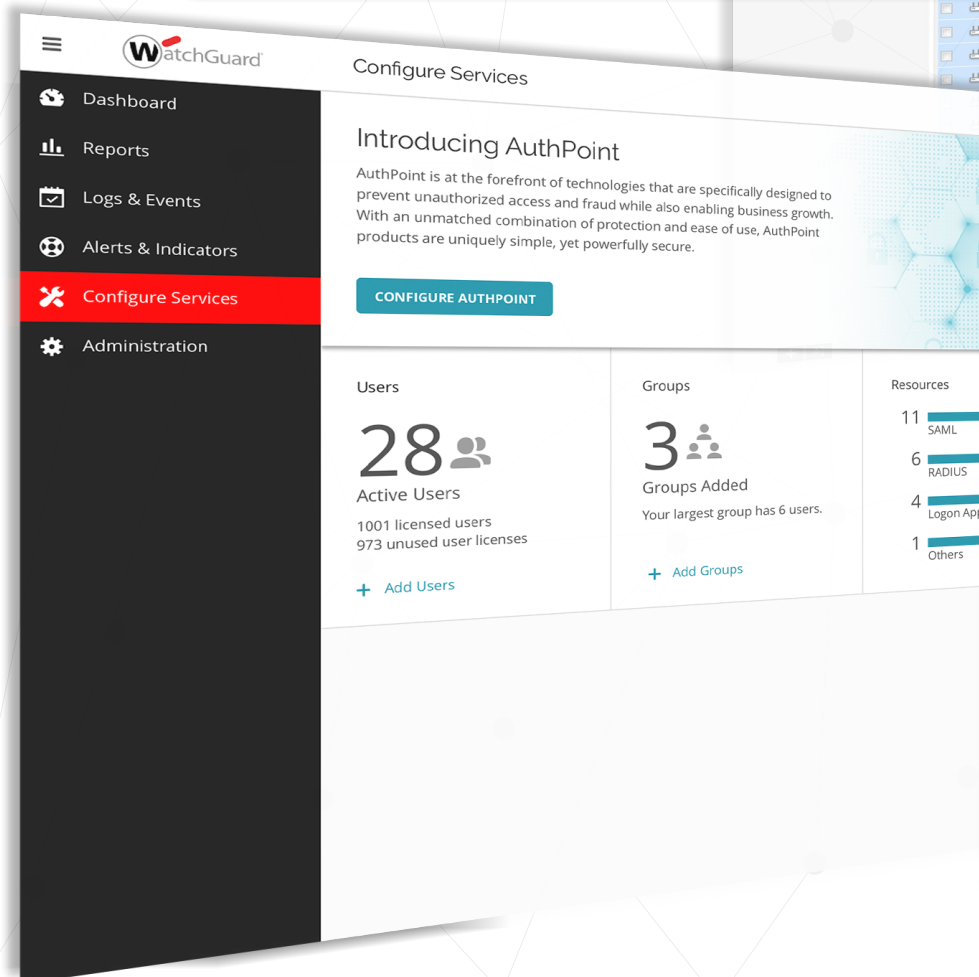
WatchGuard Cloud-managed access points can help address wireless-specific mandates included with regulations like PCI DSS. These appliances have built-in Wireless Intrusion Prevention System (WIPS) to ensure protection, extending and enhancing our security to wireless devices.

The screenshot shows the WatchGuard Monitoring dashboard with a table of detected wireless devices. The table includes columns for Name, MAC Address, Ch., Prot., Client, SSID, Security, Location, Network, and Up/Down Since. The devices are categorized by status: Authorized (green), Misconfigured (yellow), Rogue (red), External (blue), and Uncategorized (grey).

Name	MAC Address	Ch.	Prot.	Client	SSID	Security	Location	Network	Up/Down Since
Netgear_E8:72:99	2C:30:33:8B:72:99	7	802.11	0	NETGEAR31-5G	Open	//Locations/Unk	--	↑ Aug 12, 2016 1
Technicolor_39:D2:E8	8C:04:FF:39:D2:E8	8	b/g	802.11	HOME-D2EB	Open	//Locations/Unk	--	↑ Aug 12, 2016 1
4E:7A:8A:05:C9:4C	4E:7A:8A:05:C9:4C	6	b/g	802.11	xfinitywifi	Open	//Locations/Unk	--	↑ Aug 12, 2016 1
22:86:8C:79:1B:1E	22:86:8C:79:1B:1E	36	802.11	0	xfinitywifi	Open	//Locations/Unk	--	↑ Aug 12, 2016 1
6E:8F:E0:4D:63:12	6E:8F:E0:4D:63:12	1	b/g	802.11	xfinitywifi	Open	//Locations/Unk	--	↑ Aug 12, 2016 1
5E:8F:E0:DB:F4:4C	5E:8F:E0:DB:F4:4C	11	b/g	802.11	0	802.11	//Locations/Unk	--	↑ Aug 12, 2016 1
Cisco-Linksys_67:98:C6	00:25:9C:67:98:C6	1	b/g	802.11	Silvia	802.11	//Locations/Unk	--	↑ Aug 12, 2016 1
Pegatron_9A:D1:B2	00:71:C2:9A:D1:B2	1	b/g	802.11	xfinitywifi	Open	//Locations/Unk	--	↑ Aug 12, 2016 1
Pegatron_94:F1:C3	C0:7C:D1:94:F1:C3	6	b/g	802.11	LEEFAMILY	802.11	//Locations/Unk	--	↑ Aug 12, 2016 1
Pegatron-Corporation_72:99:00	DC:FE:07:72:99:00	44	802.11	0	HOME-F3A4-5	802.11	//Locations/Unk	--	↑ Aug 12, 2016 1
Arris-Group_DB:F4:4C	5C:8F:E0:DB:F4:4C	11	b/g	802.11	Wagner-2-4	802.11	//Locations/Unk	--	↑ Aug 12, 2016 1
84:00:2D:7D:CF:A1	84:00:2D:7D:CF:A1	36	802.11	0	xfinitywifi	Open	//Locations/Unk	--	↑ Aug 12, 2016 1
Pegatron_66:A3:EA	C0:7C:D1:66:A3:EA	11	b/g	802.11	xfinitywifi	Open	//Locations/Unk	--	↑ Aug 12, 2016 1
Pegatron_D3:29:61	00:71:C2:D3:29:61	9	b/g	802.11	0	802.11	//Locations/Unk	--	↑ Aug 12, 2016 1
C6:27:95:36:1E:0F	C6:27:95:36:1E:0F	1	b/g	802.11	xfinitywifi	Open	//Locations/Unk	--	↑ Aug 12, 2016 1

Financial institutions are experiencing mounting pressure from regulatory bodies to adopt **MFA (multi-factor authentication)** as part of their security programs. This includes New York Department of Financial Services (NYDFS) cyber security regulation, “23 NYCRR 500,” which mandates the use of multi-factor authentication by any medium to large financial services entity in New York.

**WatchGuard AuthPoint** implements MFA using the AuthPoint app to facilitate user authentication. Any external login attempt creates a secure push notification to the user’s smartphone, showing who and from where someone is trying to authenticate. When this message is part of their own login process, they simply accept and quickly gain access to the authorized network resources and Cloud apps. When it’s not, then the authorization attempt is rejected, causing criminals to be blocked from gaining access – even when they are using the correct credentials.



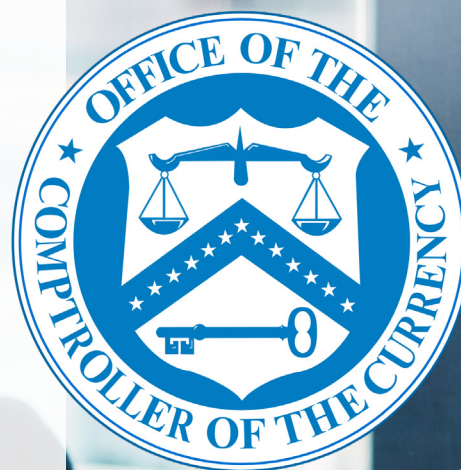
# CHALLENGE

## Increased Risk from 3rd Parties

To reduce costs and comply with regulations, many financial institutions rely on partnerships. Banks and financial services companies continue to increase the number and complexity of these relationships, relying on 3rd parties to a seemingly ever-growing extent. 3rd party relationships include outsourced products and services, use of outside consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements in which a bank has an ongoing 3rd party relationship or may have responsibility for the associated records.

The Office of the Comptroller of the Currency (OCC) has issued guidance that it expects “**comprehensive and objective oversight of 3rd-party relationships that involve significant functions such as payments, clearing, settlements, custody, tax, legal, audit, IT, etc.**”<sup>3</sup> Further, the OCC says the use of 3rd parties does not diminish responsibility of a bank or financial services firm’s board and management to ensure the outsourced functions are performed in a safe manner.

Unfortunately, your business is only as strong as your weakest partner. If your partner is attacked, their vulnerabilities create significant problems for your organization. Can you trust that your partners are keeping your data safe from attackers? If not, you risk an attack on a 3rd party negatively affecting your bottom line and your reputation.

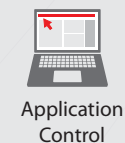


# SOLUTIONS


Take full control over the varying degrees of access you offer to third-parties – and what they can see on your network. Limit access to sensitive network data to only those roles within and outside your organization that require it. **WatchGuard Fireboxes** enable you to easily control and audit which personnel can access sensitive network resources.

One of the best ways to protect your organization from 3rd party risk is to start from within – deploying a multi-layered defense strategy that covers your entire enterprise, all endpoints, all mobile devices, all applications and all data. Every network needs a full arsenal of scanning engines to protect against spyware and viruses, malicious apps and data leakage – all the way through ransomware, botnets, advanced persistent threats, and zero day malware. **WatchGuard's Total Security Suite** provides the most complete package of unified security controls on the market today, all in one cost-effective and easy-to-deploy license.

WatchGuard's Total Security Suite includes these services:







***The financial industry has experienced significant new challenges in the last few years – many stemming from the impacts of evolving into an increasingly digitalized market. With WatchGuard, financial organizations can safely harness the power of these new technologies with robust, secure solutions you can take to the bank.***





## THE WATCHGUARD SECURITY PORTFOLIO



### 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 managing, making WatchGuard the ideal solution for SMB, midsize, and distributed enterprise organizations worldwide.



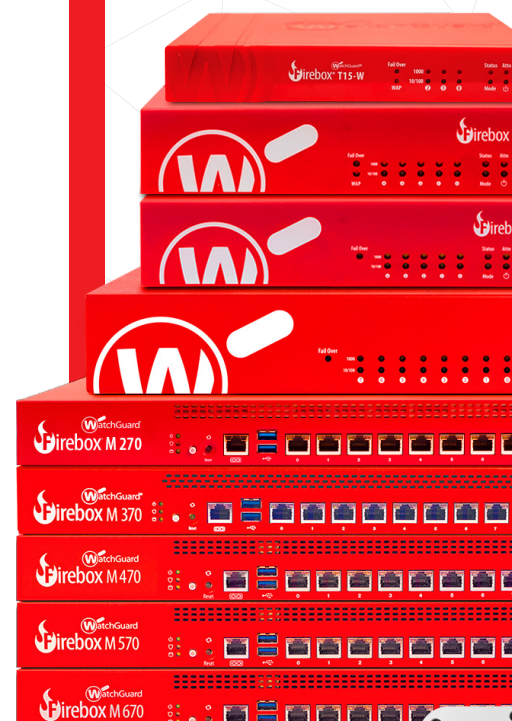
### Secure Wi-Fi

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.



## 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](http://WatchGuard.com).



North America Sales: 1.800.734.9905

International Sales: 1.206.613.0895

Web: [www.watchguard.com/wifi](http://www.watchguard.com/wifi)

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. ©2018 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, Firebox, DNSWatch, IntelligentAV, WatchGuard Dimension, and AuthPoint 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. WGCE671378\_102218