WatchGuard

Unified Security for a **RECONNECTING** world

It's time to reconnect

WatchGuard®

WHEN USERS ARE A NETWORK AWAY, THREATS ARE CLOSER THAN EVER

While social distancing, we have adapted to find new ways to work, collaborate, and play. We've had to rely on digital communications in lieu of watercooler chats and cross-cubical banter. In the process, we have become more digitally distracted.

Providing remote access to corporate resources and data in a way that maintains the "on-site" user experience is critical to the continuity of your business – but doing so securely can be a daunting task. The stakes are high; one wrong click can bring your business grinding to a halt.

More than at any other time, businesses are rethinking how their users maintain connection, productivity, AND security in the remote world.

Business continuity challenges:

- Hybrid offices and work-from-anywhere are now normal
- Personal devices are commonly used for work
- Direct-access Cloud applications circumvent the traditional network protections

Cybersecurity is the #1 challenge to employee mobility.

PULSE

The Challenges of Securing a Distributed Workforce

Digital Distraction

The average office worker receives around 121 emails every workday,[1] and there has been a 55% increase in the number of calls and meetings they attend per week.[2] The ease of working from home also means employees are more likely to be plugged in after hours. According to Pulse, nearly 60% of IT leaders say that unplugging after work is the biggest area where their users struggle with staying engaged while working remotely.

IT Teams Overwhelmed by the New Reality

The majority of tech teams have seen support requests increase 39% as a result of remote work, with VPN, video conferencing, and password reset issues being the leading cause of headaches.

Brands in the Balance

The consequences of security vulnerabilities can wreak devastating havoc on a company's good name, the likes of which some will never recover from. A successful attack can lock you out of systems, freezing the business and preventing you from providing the level of service your customers expect.

Security Budgets Are Tight

Despite being a top business priority for IT leaders, over 70% of businesses invest less than 2% of the revenue on cybersecurity.[3] And even with more people than ever working remotely, more than half of businesses today are spending less than $1,000 on cybersecurity per employee.

Experts in Short Supply

Lack of in-house cybersecurity skills is a major issue, especially for smaller organizations. Over 76% of businesses are understaffed for cybersecurity needs. When the average IT team member only stays for three years or less, you need your team to be able to ramp up quickly to effectively manage security.

Disconnected Point Solutions

The average midsize business uses four or more tools for vulnerability management, and 79% of IT leaders admit that it takes more than 48 hours to close a vulnerability.[4] Multiple point solutions without any integrations do not share context and analytics to identify indicators of compromise. Each security product requires its own management, training, support, and operations process, which are handled by separate teams. Worse still, 41% of IT leaders suggest they rarely or never have time to look at security logs.

74%
of all malware atacks are zero day incidents

Over **280%**
increase of phishing attacks against users

76%
of businesses are understaffed for cybersecurity needs

41%
of IT leaders suggest they rarely or never have time to look at security logs

79%
of IT leaders admit that it takes more than 48 hours to close a vulnerability

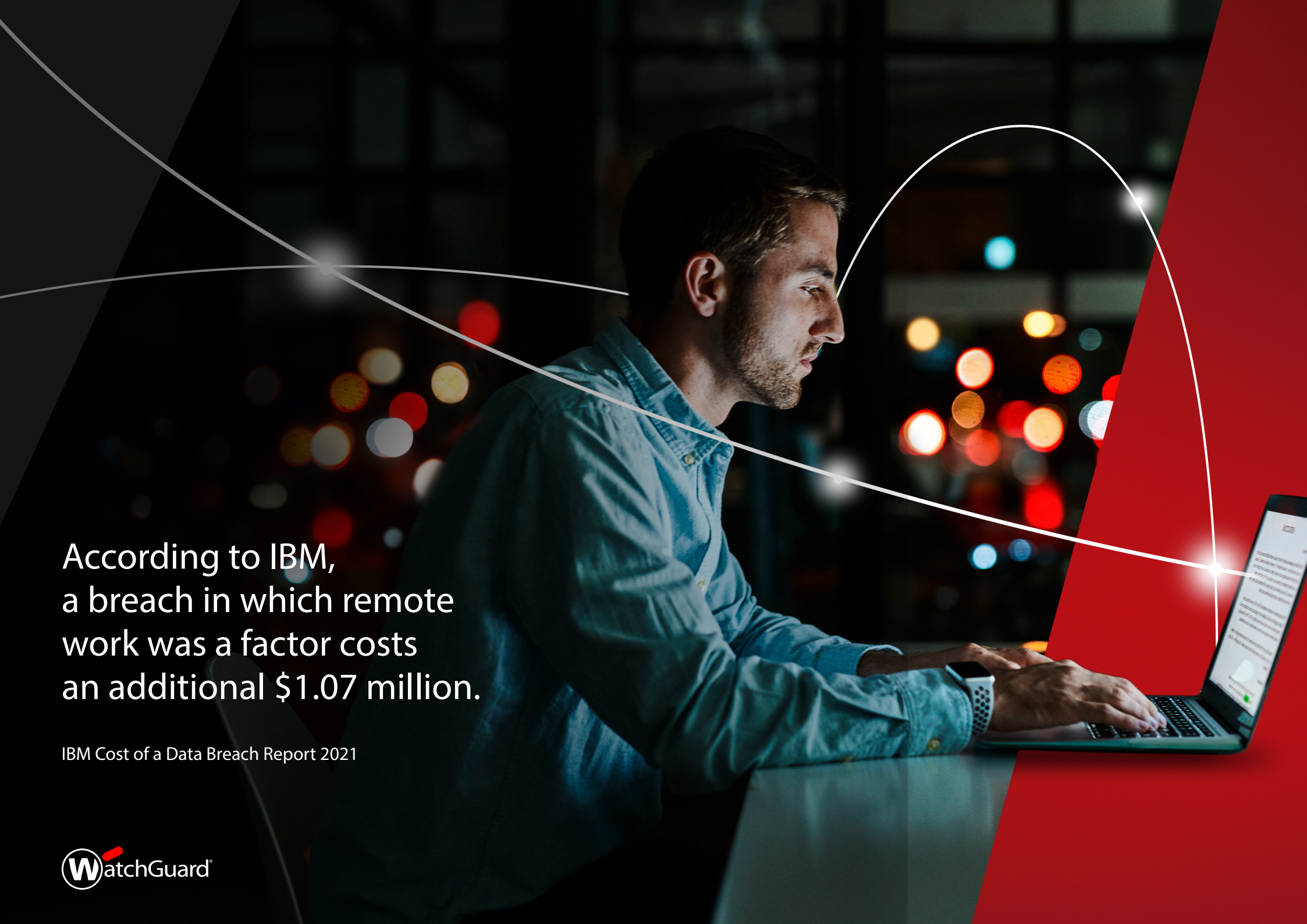
[1]https://www.mckinsey.com/~/media/mckinsey/industries/technology%20media%20and%20telecommunications/high%20tech/our%20insights/the%20social%20economy/mgi_the_social_economy_full_report.pdf
[2] https://www.microsoft.com/en-us/microsoft-365/blog/2020/09/22/pulse-employees-wellbeing-six-months-pandemic/
[3]Pulse
[4]Pulse

Rethink Connection with User-Focused Security

Thanks to the prevalence of remote work, your business has gone from having a few offices with many employees to having nearly as many offices as employees. Simply allowing carte blanche access from home networks to any business application in the Cloud is a security no-no.

Here are some of the most common initial attack vectors your business is likely to encounter:

Initial Threat Vector	Threat Description	Likelihood of Occurrence	Potential impact
Compromised credentials	Credentials can be stolen, bought, guessed, or found on the dark web – especially if your users' password habits are poor.	HIGH	MEDIUM
Phishing & social engineering	Using email, direct messages, or sometimes even phone calls, these attacks target your distracted users to extract their credentials.	HIGH	HIGH
Vulnerability in third-party software	Unpatched software is a frequent entry point to cyberattackers looking to exploit known vulnerabilities.	MEDIUM	HIGH
Business email compromise	Hackers will try to take over all email accounts to escalate their attack and pivot to other targets.	LOW	HIGH
Lost/stolen device	When your users are remote or just on the go, their devices no longer benefit from the physical protection of the office. A lost corporate device can act as a gateway for hackers trying to break into your network.	LOW	MEDIUM


According to IBM,
a breach in which remote
work was a factor costs
an additional $1.07 million.
IBM Cost of a Data Breach Report 2021
WatchGuard

Reconnecting with Zero-Trust Network Access

Virtual Private Networks (VPNs), in isolation, assume that anything that connects through your network gateway can be trusted. While this approach provides a secure connection, and adds a layer of security to less secure protocols and services, it also opens the business up to attacks that exploit your remote users and your devices. All it takes is one compromised password or endpoint device, and suddenly that same VPN connection becomes an entry point for the bad guys.

The "zero-trust" model, a term first coined in 2010, eliminates this risk by taking a "never trust, always verify" approach to extending access to users. Zero-trust network access establishes policies around user access based on the role of the employee and the security status of their endpoint based on three principles:

1

Always know who and what is connecting to the business network.

Cybercriminals use a variety of techniques to steal usernames and passwords. Phishing, spear phishing, and social engineering are common. Stolen credentials are for sale on the dark web. Passwords aren't good enough anymore. If it's worth protecting, it requires multi-factor authentication.

2

Limit access to business-critical systems based on well-defined permissions.

Zero-trust allows you to centrally manage access across all common IT systems and limit access to only specific users, devices, or applications. Access decisions happen in real time based on the policies defined by the business and the access request context.

3

Monitor the health and security posture of the network and all managed endpoints.

With employees stuck at home, the chances are good that employees will use company laptops for a hefty amount of personal web surfing and email checking. Staying on top of threats requires persistent, advanced security that goes beyond traditional endpoint antivirus.

Micro-Segmentation and Zero-Trust

Zero-trust policies encompass device, application, and identity verification and enforcement. This allows IT teams to apply micro-segmentation to limit the opportunity for insider threats, network infiltration, and lateral movement. By defining micro-segments and applying policies tailored to your organization's security needs, you create a hierarchy of protection for your environment. This starts by identifying the user that will access those applications and services.

A micro-segment could be built around a Cloud-based application, like a customer relationship management (CRM) solution. Different teams within your business require different levels of access. Sales and technical support teams likely need broad access to a CRM, but engineering? Possibly not.

Using this approach, you can apply granular controls to limit access further. For centrally located tech support teams, it may make sense to restrict their CRM access only during their working hours or prevent them from accessing the system when they connect from a new location.

Evolving the Network with SD-WAN

Before the pandemic, tech teams developed their networks to accommodate more significant use of Cloud applications and environments. SD-WAN solutions helped elevate their workers' productivity and efficiency with fast, direct access to Cloud applications, and prioritized network performance for supporting high-quality VoIP and video utilization. The pandemic forced tech leaders to rethink what was important in connecting their business and users.

While Cloud applications continue to grow, businesses today are grappling with how to architect networks with the predominance of their workforce remote. Many Cloud-first architectures are designed so that everything must pass through the network perimeter and then leave it. Users, regardless of who they are, must still interact with the corporate network, often using inefficient technology, to get back to the outside world. This creates significant challenges in terms of service availability, performance, and user productivity.

When supporting remote work, user experience must be a primary consideration. Users need to be able to access their applications without experiencing undue latency and performance issues. SD-WAN monitors your WAN connections and uses this data to make routing decisions. If a WAN connection becomes congested, it automatically distributes network traffic based on policies you define. SD-WAN also makes it possible to localize security to branch offices, so traffic is inspected in-line, improving efficiency and saving costly bandwidth.

Scoping Your Security

If you only read the headlines, it may seem that defending your business against attack requires costly, bleeding-edge security tools that are only tenable for highly resourced and skilled cybersecurity teams. If you look deeper, you will find that many of the breaches driving the news started with simple exploits of users, devices, and networks that are preventable with standard security tools deployed appropriately.

From the perimeter to the endpoint, a range of different tools addresses potential vulnerabilities and spot breaches. Practical zero-trust approaches combine authentication, endpoint protection, and network security to limit the potential harm of an attack against a user.

In this eBook, we outline four tiers of end-to-end, user-focused security implementation that can help dramatically reduce the threat surface of businesses just like yours.

TIER 1

Block known threats and prevent unauthorized access.

TIER 2

Control web traffic, simplify authentication, and block phishing attempts.

TIER 3

Limit exposure based on risk, respond to advanced threats and inspect encrypted traffic.

TIER 4

Take a 'never-trust, always verify' approach to security.

Many of the breaches start with simple exploits of users, devices, and networks that are preventable with standard security tools.

Tier 1: Good

Block known threats and prevent unauthorized access.

Multi-factor authentication

When a hacker can use a single compromised password to circumvent even the most sophisticated security, businesses need to make every effort to keep user credentials safe. By requiring additional authentication factors, multi-factor authentication mitigates the threat of stolen credentials while reducing network disruptions and data breaches.

Multi-factor authentication enhances user authentication by requiring:

- Something you know (password, PIN)
- Something you have (token, mobile phone)
- Something you are (fingerprint, face)

Business-grade endpoint protection

Chances are your business uses a diverse range of desktops, laptops, mobile devices and servers that need protection from a host of known threats. Malware infection on even one of these endpoints can cause significant disruption and downtime to your business. While consumer-grade antivirus solutions can provide some protection, organizations serious about their security need a business-grade solution.

What to look for:

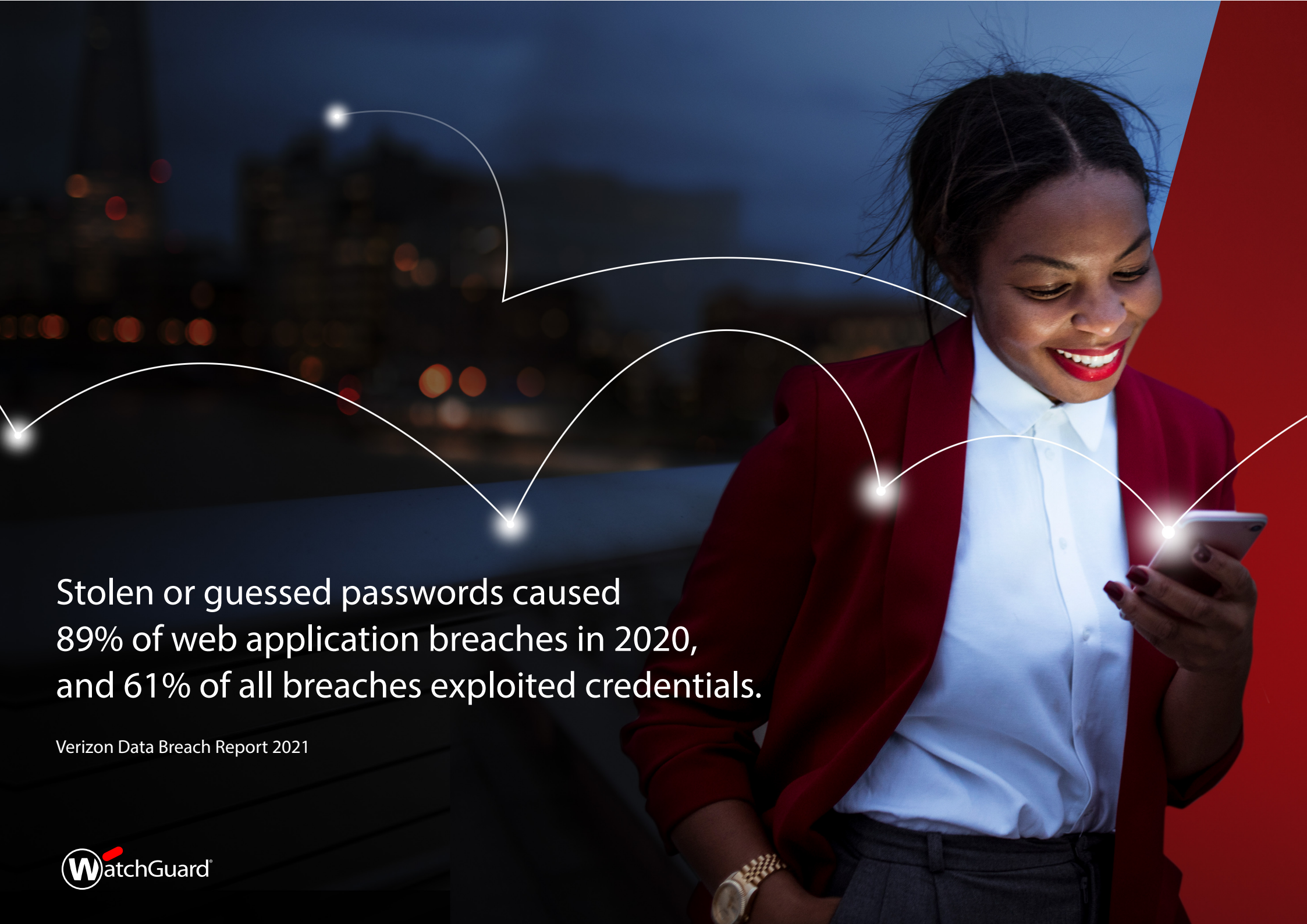
- One solution for all of your Windows, Linux, macOS and Android devices
- Detailed, real-time protection and reporting
- Malware "freezer" to isolate and recover malware if needed

Network firewall, VPN, and secure remote access

Sitting in the heart of your network, a firewall plays a vital role in the overall security of your business. With a firewall you can not only analyze traffic for threats, but also facilitate VPN connections and provide secure access to web applications, internal applications, and Microsoft Exchange services, as well as secure RDP and SSH sessions to local resources.

What to look for:

- VPN
- SD-WAN
- Remote Access


Stolen or guessed passwords caused
89% of web application breaches in 2020,
and 61% of all breaches exploited credentials.
Verizon Data Breach Report 2021
WatchGuard

Tier 2: Better

Control web traffic, simplify authentication, and block phishing attempts.

Push-based authentication

Multi-factor authentication has come a long way since the early days of clunky one-time password tokens. Push-based authentication solutions provide a better balance between security and user experience, eliminating the need for a hardware token while improving security and visibility. With a smartphone in everyone's pocket, why ask your users to carry a hardware token? Users can simply push to approve or reject on their preferred device.

What to look for:

- Shows the context of the authentication – what is being accessed and from where
- Reduces the chance of social engineering
- OTP (one-time password) embedded within push response cannot be copied or stolen

Phishing protection and DNS filtering

Users are a prime target for phishing, especially when connecting remotely. DNS-level detection solutions proactively identify malicious DNS requests associated with phishing attacks, providing an additional layer of security to block connections to the bad guys. DNS filtering can also kill command and control connections, severing the line of communications between an attacker and their malware.

What to look for:

- Automatically protects end users from phishing attacks and C2 connections
- Lightweight, always-on security – no VPN required!
- Content filtering capabilities to limit access to risky areas of the web

Content filtering and gateway antivirus

Firewalls provide broad protections against intrusions and malware for every device connected to your network. They can also enforce web policy using web filtering tools to block inappropriate content, conserve network bandwidth, to preserve employee productivity.

What to look for:

- Identifies and blocks known spyware, viruses, trojans, worms, rogueware and blended threats
- Automatically blocks known malicious sites based on policy
- Multiple real-time feeds to protect from malicious sites and botnets


77% of Cloud account data breaches are due to stolen or hacked login credentials.
Verizon Data Breach Investigation Report 2020
WatchGuard

Tier 3: Best

Limit exposure based on risk, respond to advanced threats and inspect encrypted traffic.

Risk-based authentication

Without risk policies in place, your company would need to enable the most secure authentication method at all times, for all users, potentially causing user friction for some segments. Risk authentication is a way to modernize your strategy by using a precise amount of security with customized risk protection that improves your ability to detect and respond to threats.

What to look for:

- Network location-based rules – better user experience for users on protected networks
- Geolocation-based rules – computer and mobile location can help mitigate privacy and security issues
- Time-based rules – most attacks are done when everyone is sleeping

Endpoint detection and response

Unfortunately, zero day attacks, ransomware, cryptojacking, and advanced threats are targeting smaller businesses more and more. These types of attacks can bypass most traditional antivirus solutions. Without complete visibility into endpoints and servers, you could be missing an active threat. Endpoint detection and response solutions monitor endpoints for malicious activity and can automatically detect and respond to targeted attacks and in-memory exploits.

What to look for:

- Security against unknown advanced threats detects and blocks malware, trojans, phishing, and ransomware
- Security for all attack vectors: browsers, email, file systems, and external devices connected to endpoints
- Protection for Windows, Linux, macOS, and Android devices

Encrypted traffic inspection and advanced anti-malware

Hackers hiding threats in encrypted traffic is now common. Today, malware arriving over TLS-encrypted connections like HTTPS accounts for over 40% of overall detections at the network, and intrusions are rising. The ability to inspect this traffic is now a critical requirement for any firewall. Advanced tools, like Cloud sandboxing and AI-powered anti-malware, can help to expose even the most advanced threats hiding in encrypted traffic.

What to look for:

- High-performance HTTPS inspection with ALL security services active
- Full inspection of TLS 1.3 traffic
- Artificial intelligence and machine-learning capabilities that provide predictive protection against threats

Over 60% of cyberattacks detected on the network today hide in encrypted traffic

WatchGuard Internet Security Report Q1 2021

WatchGuard

Tier 4: Zero-Trust

Take a “never-trust, always verify” approach to security.

Zero-trust authentication

Your company would need to enable the most secure authentication method at all times for all users if risk policies were not in place. For some users, this is unnecessarily cumbersome. Risk authentication is a way to modernize your strategy by using a precise amount of security with customized risk protection that improves your ability to detect and respond to threats.

What to look for:

- Different authentication methods based on different locations and networks
- Geofence applications, reducing exposure

Threat hunting and deny-by-default application control

Threats can linger for hundreds of days. Reducing the time to detection is critical to minimizing the impact of a cyberattack. Continuous monitoring of endpoint behaviors for indicators of attack (IoAs) helps to head off advanced malware, stay on top of shadow ware, and uncover hackers and insider threats. It is also possible to take a deny-by-default approach to endpoint protection, by limiting execution to only those applications known to be safe.

What to look for:

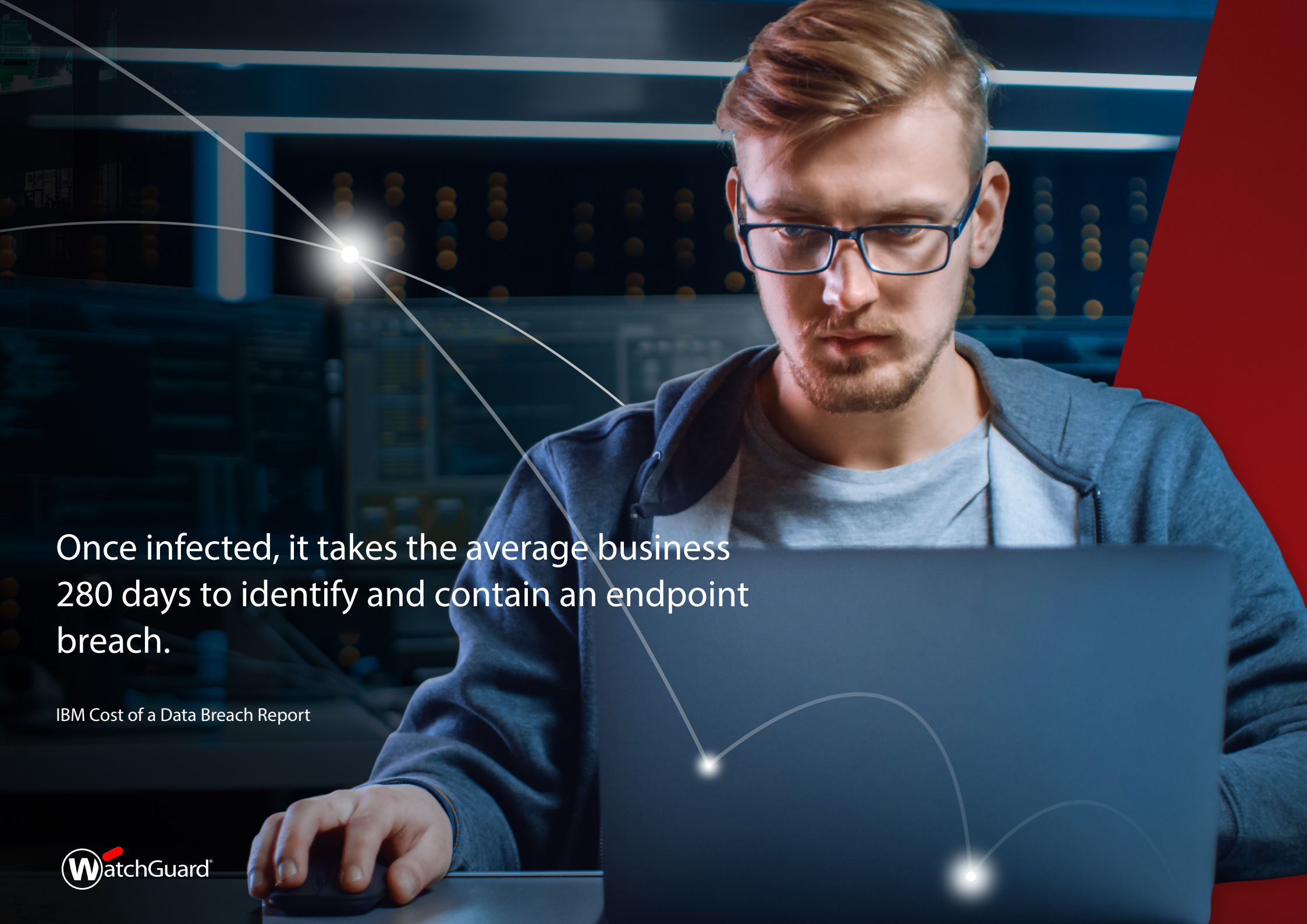
- AI-powered classification of endpoint processes as malware or trusted
- Automatic investigation of indicators of attack to find evasion and compromise techniques
- Rapid delivery of new IoAs to protect endpoints against further attacks

Secure Wi-Fi, threat correlation, and universal scoring

Firewalls are well positioned to provide broad protections against intrusions and malware for every device connected to your network. They can also enforce web policy using web filtering tools to block inappropriate content, conserve network bandwidth, to preserve employee productivity.

What to look for:

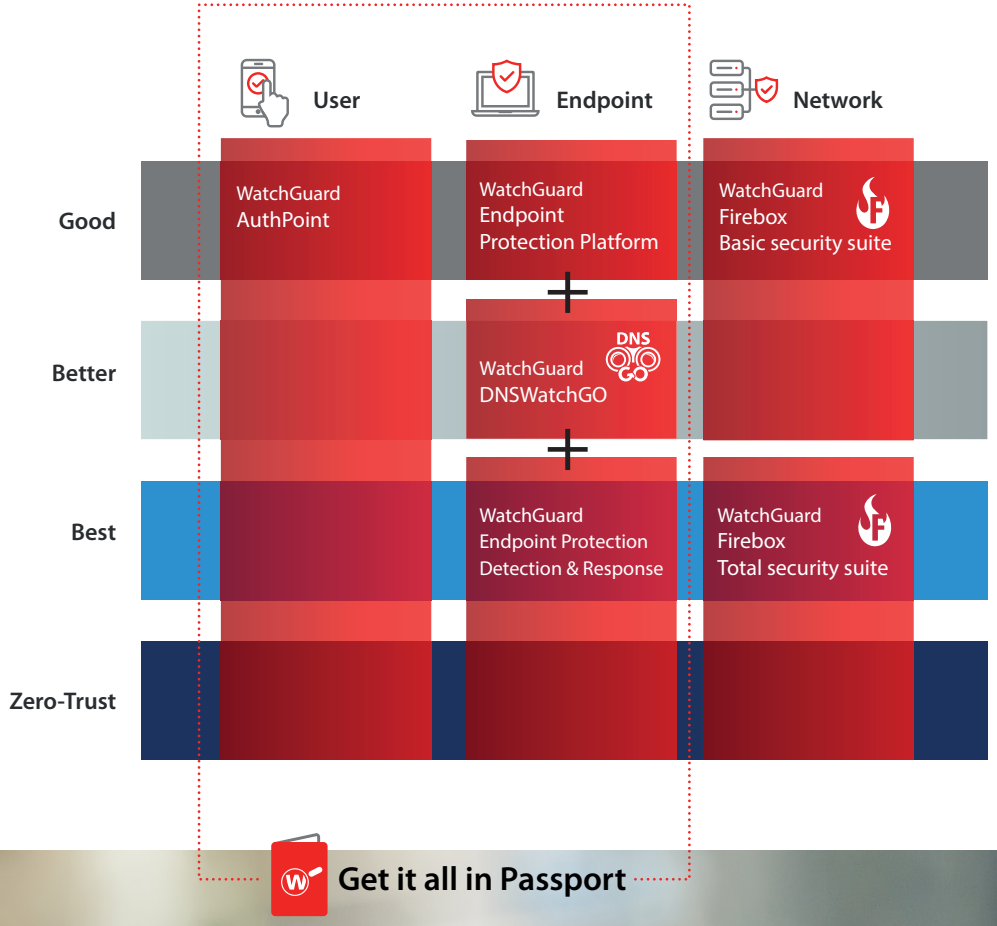
- Identify and block known spyware, viruses, trojans, worms, rogueware and blended threats
- Automatically blocking known malicious sites based on policy
- Multiple real-time feeds to provide protection from malicious sites and botnets


Once infected, it takes the average business 280 days to identify and contain an endpoint breach.
IBM Cost of a Data Breach Report
WatchGuard

WatchGuard Has What You Need

For over two decades, WatchGuard has pioneered cutting-edge cybersecurity technology and delivered it as easy-to-deploy and easy-to-manage solutions. With industry-leading network and endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence products and services, WatchGuard enables more than 250,000 small and midsize enterprises from around the globe to protect their most important assets. Today, WatchGuard is trusted to protect thousands of corporate networks, and over 10 million users rely on WatchGuard technology to keep them safe as they work remotely.

Our unique, user-focused security portfolio addresses critical security vulnerabilities across networks, users, endpoints, and applications.



WatchGuard Has What You Need

Secure your users

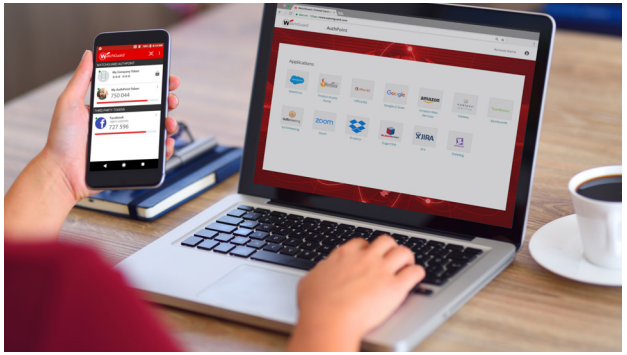
At WatchGuard, we believe the threat landscape requires every business to implement MFA as a best practice, and we make it easy. WatchGuard's AuthPoint is a full-featured MFA solution that goes beyond traditional 2-factor authentication (2FA) by adopting innovative ways to identify users. AuthPoint is delivered entirely from the Cloud for easy set-up and management. Risk-based authentication is built into the platform, giving you the power to create rules that are unique to the security structure in your organization.

Secure your devices

With plenty of vulnerabilities to be exploited and outdated software versions, endpoint devices are frequently on the Internet without protection from corporate perimeter security, making them a favorite target for cybercriminals. WatchGuard's endpoint security platform delivers maximum protection, and minimal complexity with advanced endpoint protection platform (EPP) and endpoint detection and response (EDR) approaches. Our unique Zero-Trust Application Service and Threat Hunting Service offering (included in EDR) make it possible to detect hackers and insider threats and prevents malicious applications from running on a managed endpoint.

Secure your environments

WatchGuard offers an award-winning portfolio of network security services, from intrusion prevention service, gateway antivirus, application control, spam blocking, and web filtering to more advanced services for protecting against advanced malware, ransomware, and data theft. WatchGuard Firebox is a comprehensive advanced network security platform that puts IT security professionals back in charge of their networks. Every year the average WatchGuard Firebox blocks over 1,300 malware attacks and 250 network intrusions for WatchGuard customers.



Simplify with Unified Security

Disparate solutions are not just difficult to manage; they make identifying threats and vulnerabilities nearly impossible. WatchGuard's Unified Security Platform™ helps businesses elevate and expand their security while reducing overhead and simplifying risk mitigation through user-focused security approaches.

Not Just *Consolidated* – *Unified* Security

The Unified Security Platform is a true force multiplier for IT teams. This platform makes operational ease possible by integrating normally disconnected, advanced technologies to enable comprehensive, multi-layered security across the network, users, hosts, and applications.

> Lack of a unified cybersecurity strategy is the #1 reason organizations fall victim to a ransomware attack.
>
> PULSE

Clarity and Control

WatchGuard Cloud is the centralized management reporting and visibility interface for the entire Unified Security Platform, giving tech teams a single-pane-of-glass for end-to-end security management of their entire WatchGuard security stack.

Comprehensive Security

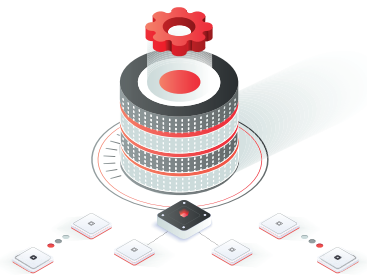
WatchGuard's comprehensive portfolio breaks the Cyber Kill Chain® at each level. Stop the attempted discovery and exploitation of vulnerable systems, phishing, ransomware, intrusions, advanced malware across all of your users, environments, and devices.

Shared Knowledge

No matter how advanced the tech, deploying security layers in isolation risks that an attacker will slip through the cracks. With correlation and a strong identity framework delivered from a single platform, you can close gaps in visibility and bring light to security shadows.

Operational Alignment

Security that works for your business with three key purchasing options for partners, including fixed-term pre-pay, fixed-term pay-as-you-go, and zero commitment pay-as-you-go. Easily integrate WatchGuard into your ecosystem with RESTful APIs across the platform.



Automation

Automation is at the heart of WatchGuard's Unified Security Platform, speeding up processes, killing threats, and empowering IT teams to do more in less time. WatchGuard's Automation Core creates a zero-touch security feedback loop and accelerates business-driven security management.

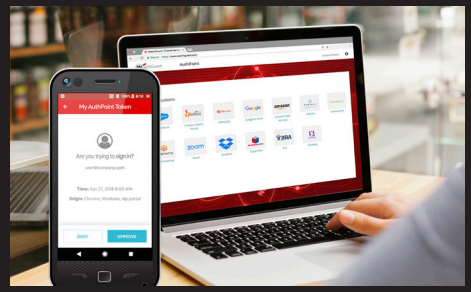
WatchGuard Portfolio

Network Security

WatchGuard Network Security solutions are designed from the ground up to be easy to deploy, use, and manage – in addition to providing the strongest security possible. Our unique approach to network security focuses on bringing best-in-class, enterprise-grade security to any organization, regardless of size or technical expertise.

Secure Wi-Fi

WatchGuard's Secure Wi-Fi solutions, true game-changers in today's market, are 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 address the password-driven security gap with multi-factor authentication on an easy-to-use Cloud platform. WatchGuard's unique approach adds the "mobile phone DNA" as an identifying factor to ensure that only the correct individual is granted access to sensitive networks and Cloud applications.

Endpoint Security

WatchGuard Endpoint Security is a Cloud-native, advanced endpoint security portfolio that protects businesses of any kind from present and future cyberattacks. Its flagship solution, WatchGuard EPDR, powered by artificial intelligence, immediately improves the security posture of organizations. It combines endpoint protection (EPP) and detection and response (EDR) capabilities with zero-trust application and threat hunting services.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by more than18,000 security resellers and service providers to protect more than 250,000 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 midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.

NORTH AMERICA SALES 1.800.734.9905 INTERNATIONAL SALES 1.206.613.0895 WEB www.watchguard.com

Part No. WGCE67514_110421