

WATCHGUARD THREATSYNC®

# Accessing the XDR Realm

A Guide to Unleashing  
Modern Security



XDR

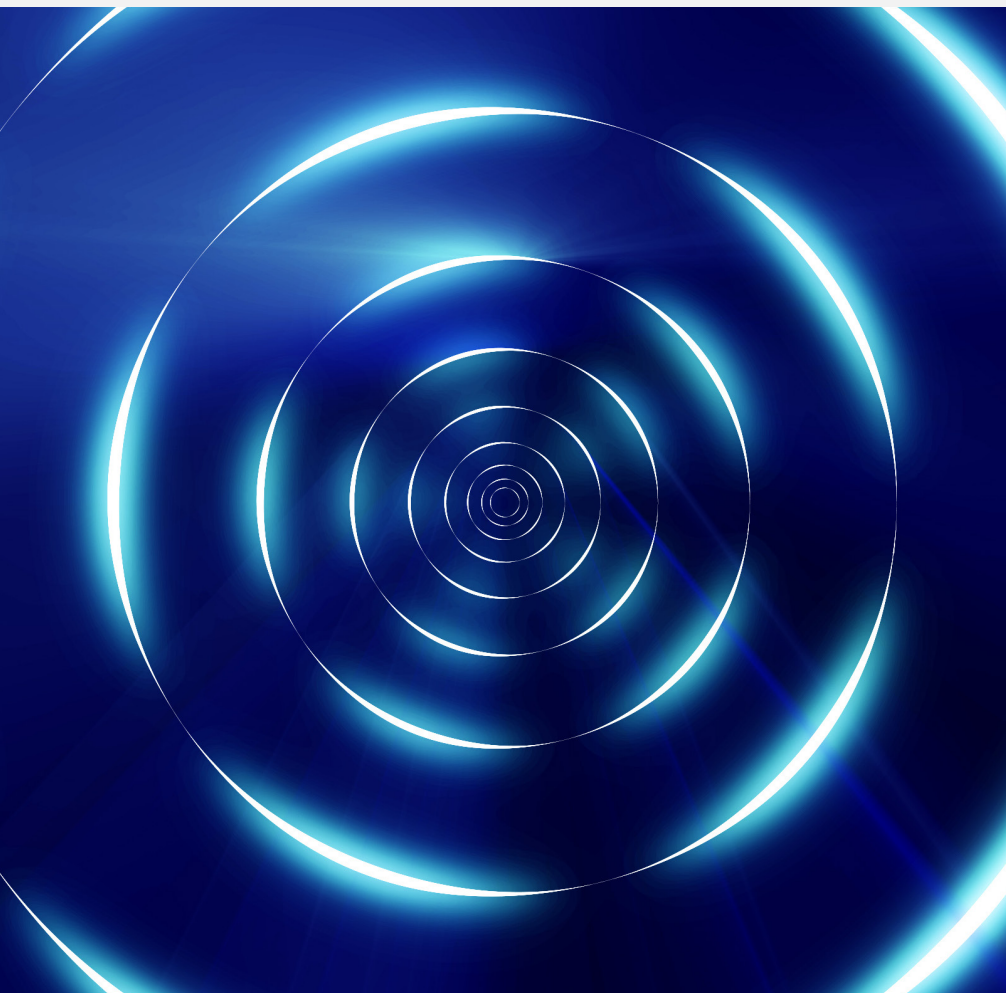


# TABLE OF CONTENTS

**01** Today's Top Cybersecurity Challenges

**02** XDR: Your Gateway to Modern Security

**03** Access the XDR Realm



# 01 Today's Top Cybersecurity Challenges

Organizations of all sizes are struggling to keep up with the increasingly complex and treacherous cybersecurity landscape. Threat actors aren't just hunting large corporations; they're aggressively targeting small and midsize businesses with sophisticated cyberattacks as well.

security status quo. Threat actors and their techniques evolve rapidly, so you must respond in kind to protect your environments, devices, users, and data. This means adopting security solutions that can adapt and grow at pace with your business and its expanding threat surface.

Companies can't afford to bury their heads in the sand and maintain the



“Cybersecurity is not a destination, it's a journey – simply because it's always evolving”

Calvin Engen  
Chief Technology Officer at F12.net

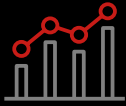
## What Are Today's Top Cybersecurity Challenges?

### Siloed Security

Security teams are charged with managing and protecting an ever-increasing number of threat vectors across corporate networks, endpoints, and identities. With so many different vulnerabilities at play and such a wide range of potential cyberattacks to detect and mitigate, it makes sense to establish a wide breadth of security solutions. However, a broad arsenal of tools can be a double-edged sword if each solution operates independently from the rest. More security products don't mean stronger security.<sup>1</sup>

A broad arsenal of tools can be a double-edged sword if each solution operates independently from the rest.





# 19%

The number of security tools used by companies has increased by 19% over the last two years



# 36%

Only 36% of businesses say they're "very confident" when it comes to ensuring that controls are working as intended



# 64 to 76

The number of security tools used by large enterprises has increased from 64 to 76 applications on average



# 82%

Moreover, 82% say they've been surprised by security incidents that evaded existing tools

## Visibility Gaps

All these siloed tools also make it difficult to build a comprehensive understanding of your security posture. Each tool only provides a limited view into its own area of specialty. Taken together, the result is a collection of puzzle pieces you have to manually classify and attempt to piece together into a complete picture.

Even worse, the process of struggling to fit these puzzle pieces together wastes crucial time in the event of an active cyberattack. If your security administrators have to log in to multiple consoles and switch between a half dozen different tools just to determine what might be happening, threat actors already have a considerable advantage while executing their attack.

**Security administrators must break down these security silos to reclaim this lost time and have a chance to keep up with fast-paced cyberattacks.**

However, unless these tools are implemented by the same vendor, solutions focused on different security areas will rarely provide the interoperability required for effective protection.

## Correlation and contextual data difficulties

All security products, such as network solutions, firewalls, endpoint security, or identity tools, have different ways of presenting logs, telemetry, and alerts; they each have a unique format and frequency.

At the same time, making sense of the vast volume of security data gathered from these products can be overwhelming to manage manually, and complex to combine and analyze. It's easy to miss important threat indicators or get bogged down with false positives if you're drowning in data generated by multiple disparate products. This ultimately leads to overlooked threats that put the whole organization at risk.

Integrating multiple security products from different vendors can be complicated and time-consuming, and require specialized knowledge and expertise. Managing these products can still be challenging even when successfully integrated, mainly when dealing with complex and diverse IT environments.

## Lack of security automation

Your users rely on you to protect their valuable data and safeguard corporate assets. Without automation, detecting and responding to security incidents can be slow and ineffective, increasing the risk of networks, endpoints, and users becoming compromised, as well as the costs and reputational damage that follow data breaches.

### 1 Slow and extended detection times

Without automated detection, security teams must rely on manual processes that significantly impact mean time to detect (MTTD), cause missed threats, trigger false positives, and delay incident response times. This delay in detecting security threats can cause security administrators to miss critical threats and conduct unnecessary investigations into low-level alerts, leading to increased costs and leaving the door open to potential breaches.

### 2 Lack of clarity on appropriate response actions

How do security admins know what response action they should take first? When you experience a security incident, the speed and

accuracy of the response can make all the difference when it comes to the impact and the scope of the attack. However, without automated response capabilities, it can be challenging to know which response action will resolve the threat and reduce the mean time to respond (MTTR).

Time is gold; slow detection times and inaccurate response actions can facilitate the threat actors propagating the attack across the enterprise and often can result in extended downtime and data loss. Security automation enables consistent and effective security services at scale.

**Security automation can help you to provide consistent and effective security services across multiple clients and maintain a standard level of security for all of them.**

## Security complexity and overloaded IT security teams

As technology advances, your IT environments are becoming more complex, with numerous systems, applications, and devices that require constant monitoring and maintenance to ensure security. Additionally, sophisticated threats continue to emerge rapidly, accelerating the pressure to keep up.

Companies looking for new levels of security telemetry aggregation, correlation, and analysis add to the already massive workloads of their security personnel. Administrators must deal with a constant and growing deluge of alerts and protect an increasingly diversified attack surface in which threats have become more complex to detect.

### 1 Shortage of skilled cybersecurity professionals

Recruiting and retaining qualified and knowledgeable staff is becoming increasingly difficult due to the climbing demand for highly scarce skilled professionals in the field. In light of this scenario, you might find yourself struggling to manage a wide range of specialized security

solutions while finding the time required to identify and mitigate threats.

### 2 Alert fatigue

On average, most security professionals are dealing with thousands of weekly malware alerts, of which just 19% are considered trustworthy, and only 4% are ever investigated. What's more, some traditional security solutions, far from solving specific use cases, create greater stress and increase workloads by delegating the responsibility for managing alerts and forcing you to classify threats manually.

Recruiting and retaining qualified and knowledgeable staff is becoming increasingly difficult due to the climbing demand for highly scarce skilled professionals in the field.



### A closer look at the pitfalls of point product security approaches

Endpoint detection and response (EDR) and network security solutions are two crucial components of a modern cybersecurity strategy. These tools help you identify, detect and respond to advanced threats against critical domains.

Although the right network security and EDR solutions are highly effective when it comes to detecting and responding to sophisticated threats, they give visibility into specific areas of IT infrastructure. Network security tools, such as firewalls and intrusion detection systems, operate on a network perimeter-centric model and simply do not provide enough visibility into endpoints. They focus on protecting the entry and exit points of the network and monitoring traffic at the network edge. However, with the rise of a hybrid work model, the network perimeter has become increasingly porous, making it more difficult to maintain effective security.

Similarly, EDR solutions have become essential tools in the battle to detect and respond to endpoint threats. But alone, they cannot provide visibility into threats

taking place across your corporate network environments.

As a result, many businesses are often compelled to use a patchwork of security products to detect threats across multiple security layers. This fragmented approach creates blind spots because your security solutions are operating independently from one another. It limits visibility, contextual results, and the effectiveness of detection and response, making comprehensive, end-to-end protection nearly impossible.

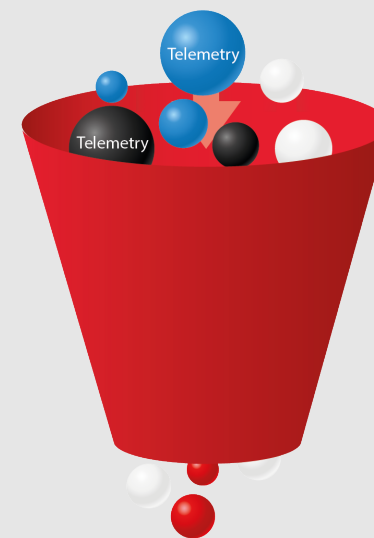
You're probably all too familiar with these challenges. Security administrators have been dealing with them for far too long. The truth is that most of these obstacles are simply the byproduct of outdated approaches to security. Overcoming them requires a commitment to altering your course and embarking on a new security journey.



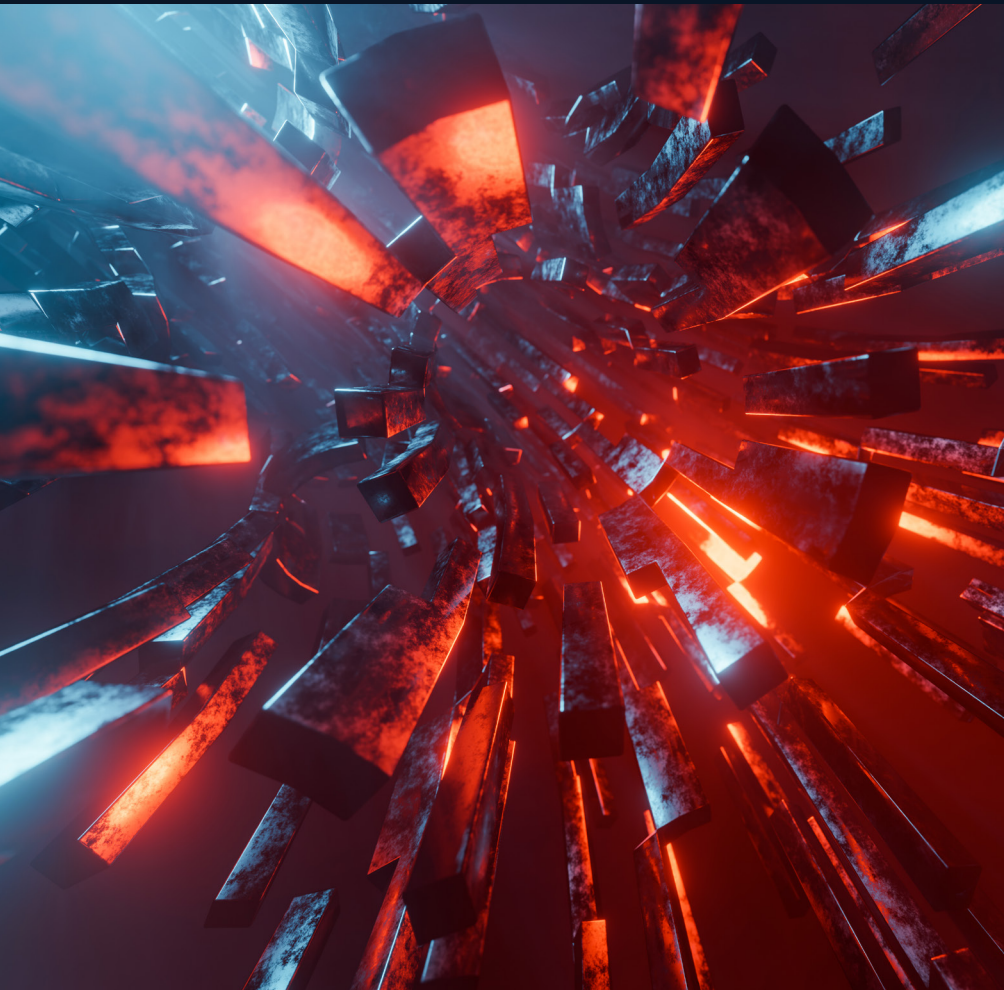
Endpoint Security



Network Security







## 02 XDR: Your Gateway to Modern Security

To overcome these challenges, you need an integrated approach that provides context and telemetry data correlation across multiple security layers and IT domains.

With more tightly integrated security solutions, you get a comprehensive view of your security status.

A modern, integrated approach to cybersecurity should include extended detection and response (XDR) capabilities with automation and AI technologies, which can dramatically improve security efficacy against advanced threats while simplifying security operations.

## How does XDR work?

We live in a reality where cyberattacks are more the rule than the exception, and nothing could cause more havoc than when these threats materialize. With experts grappling with persistent and evolving attacks and multiple systems and tools to take care of, now is the right moment for a comprehensive threat detection and response solution that brings MSPs to a new world of opportunities. XDR is that solution.

XDR offers stark advantages over disconnected security tools. It provides the context and visibility required to identify and remediate cyberattacks with a higher degree of speed and efficacy. XDR enables a comprehensive security approach that leverages automation and AI technologies to detect and respond to threats across firewalls, servers, workstations, and devices.

An integrated XDR solution can streamline security operations, reduce operational friction and costs, and can help you achieve a stronger security posture overall.



# 03 Access the XDR Realm and Unleash Unified Security

We deliver a comprehensive and simple-to-use XDR solution with ThreatSync, a core layer within WatchGuard's Unified Security Platform® architecture. This enables us to unify cross-product detections and enables faster threat remediation from a single interface.

## eXtend, Detect, and Respond with ThreatSync

### 1 eXtend

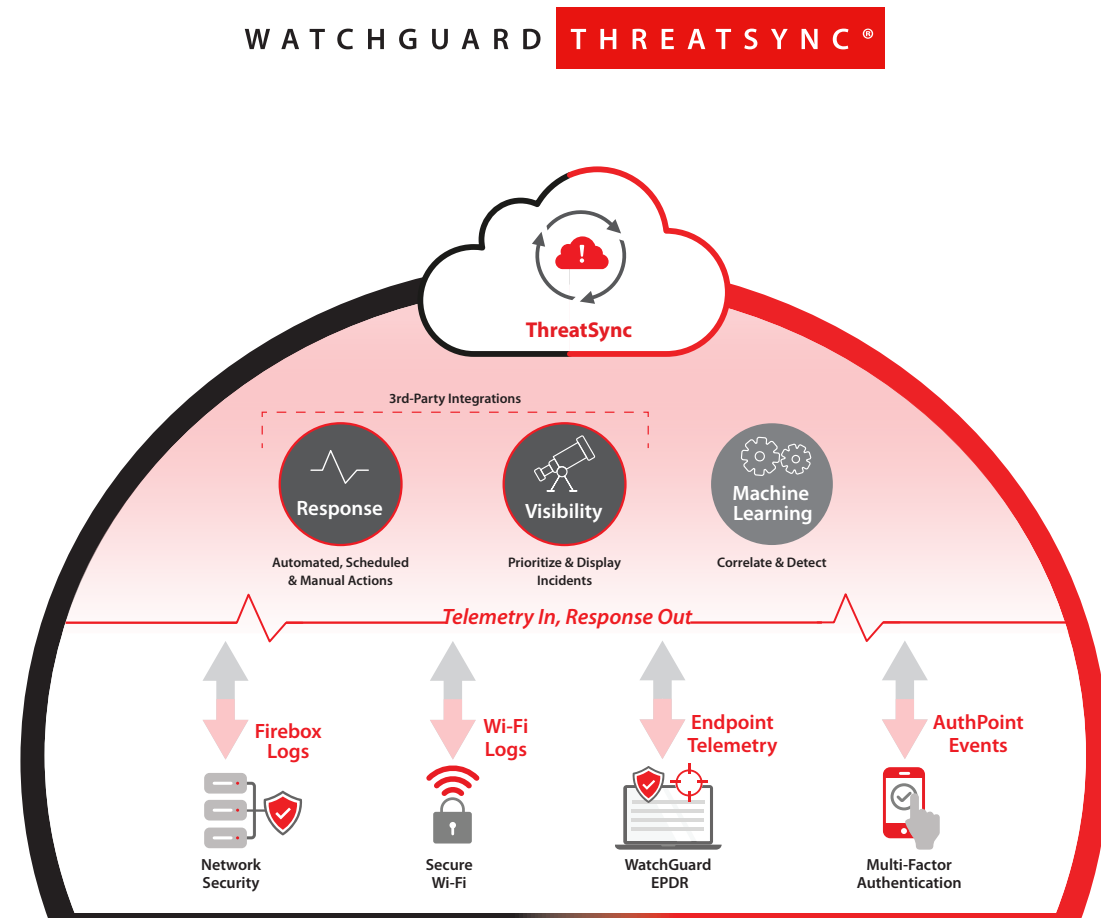
We implement XDR with tight integrations and cross-domain data telemetry from WatchGuard's latest-gen technologies. By broadening the range of data feeds to include network, endpoint, and user threat intelligence, we extend visibility and protection.

### 2 Detect

Say goodbye to siloed security approaches that slow detection times and miss attacks. With ThreatSync AI and machine-learning capabilities, we identify potential threats in real time across different domains for reduced detection timeframes and swift containment.

### 3 Respond

XDR speeds response times and elevates your company's security. We use ThreatSync to orchestrate automated response actions to neutralize threats against your business simply, quickly, and more accurately.



\* Secure Wi-Fi and AuthPoint will be available soon, integrated into ThreatSync.

## Powerful XDR Made Simple

### Cross-Platform Threat Detection

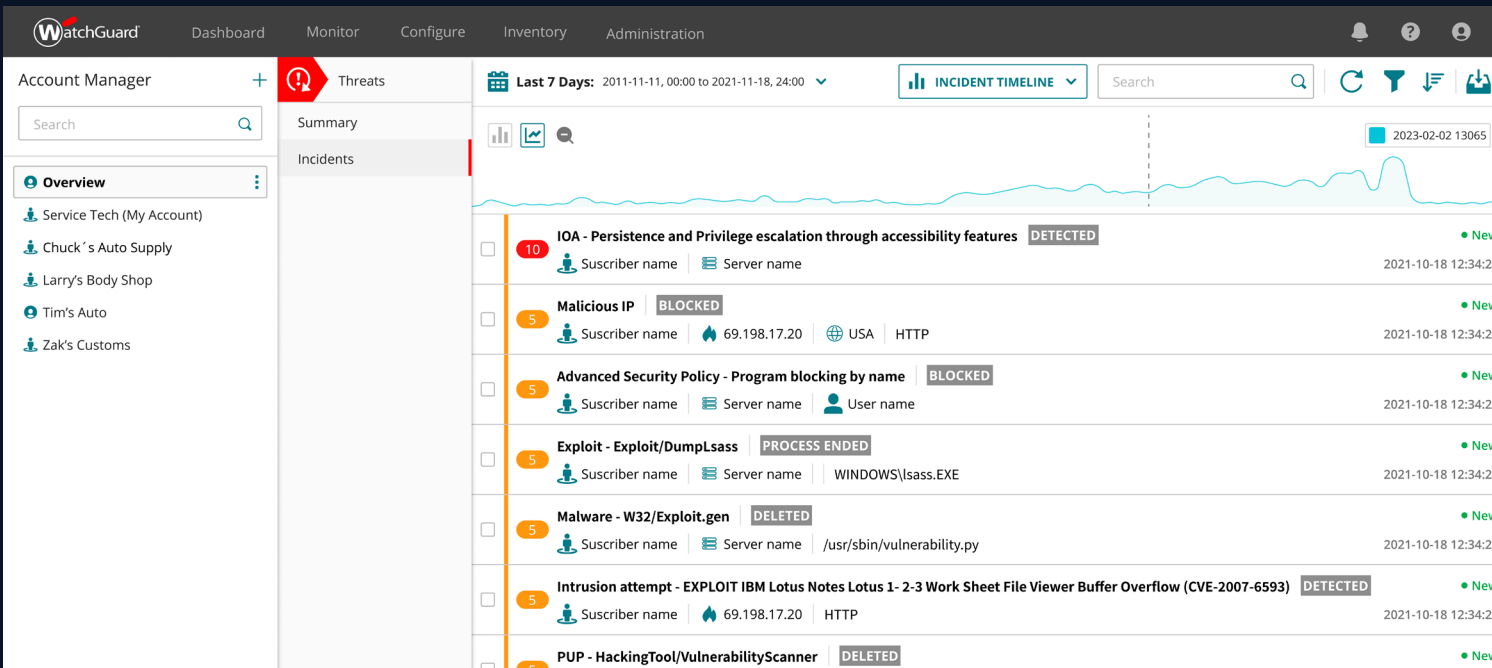
ThreatSync provides extended detection capabilities by consuming and correlating indicators of compromise (IoCs) from all WatchGuard security products. This cross-domain correlation and context enables the solution to detect and score potentially malicious activities related to specific environments, users, and devices to reduce MTTD, improve accuracy, and ultimately enable faster remediation.

### Unified Security Orchestration and Threat Response

XDR delivers a holistic view of your threat surface, making it easy to identify issues, triage, and respond with speed and confidence. ThreatSync enables higher efficiency and efficacy with intelligent alert scoring, automated remediation policies, and options for manual intervention as needed. This level of threat response orchestration elevates both scale and accuracy.

### Simple to Deploy and Manage

ThreatSync makes adopting an XDR approach easy with its intuitive Cloud-based management and automation capabilities. As the robust XDR layer within WatchGuard's Unified Security Platform architecture, ThreatSync integrates cross-product intelligence to reduce the costs and management burdens of deploying multiple point solutions for threat detection and response.



**Greater Visibility** into network and endpoint activity, helping to identify threats that might otherwise, go undetected



**Comprehensive Security** by unifying data and alerts into a single platform where solutions can work together to prioritize and respond to threats



**Reduce Security Team** burdens by automating the threat detection and response process and freeing up time and resources for another high-value task



**Streamline Response Process** providing coordinated and automated responses to detected threats

Cyber threats become more complex and sophisticated every day and impact businesses of all sizes and industries. Many CIOs, CISOs, and IT leaders see security vendor consolidation and outsourcing security to a trusted managed service provider as cost-effective routes to strengthening their security posture.

With ThreatSync and WatchGuard's Unified Security Platform architecture, we can deliver the comprehensive, intelligent protection you need to safeguard your environments, employees, and devices. Our unified approach to security delivers the comprehensive security, clarity and control, shared knowledge, operational alignment, and automation you need to enjoy effective security at scale.



Access the XDR Realm with WatchGuard ThreatSync to Unleash the Power of Unified Security Today!



# WatchGuard Portfolio



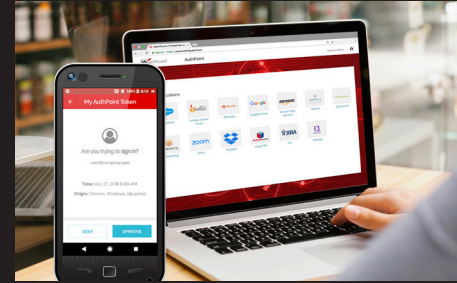
## Network Security

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 unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia 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](http://www.watchguard.com)**



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. ©2022 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, Firebox, ThreatSync, Unified Security Platform, WatchGuard Automation Core and AuthPoint are 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. WGCE67661\_031723