
WatchGuard
Future-Proof
Endpoint Security in 2025
AI, Automation, and Compliance in Action
Simplifying Cybersecurity

Table of Contents

01 Summary

Endpoint protection in 2025 and beyond requires more than antivirus. It will require AI-driven defenses, automation, and compliance readiness to stay ahead of increasingly advanced threats.

This eBook explores how modern endpoint security strategies are evolving to:

- Stop unknown and evasive threats before they execute using AI and Zero Trust principles
- Correlate signals and automate responses across the attack chain in real time
- Defend against sophisticated techniques such as living-off-the-land (LotL) attacks and fileless malware
- Adapt to compliance standards like NIS 2, DORA, and cyber insurance requirements
- Extend protection beyond the endpoint with XDR-level correlation

By understanding these trends and adopting proactive solutions, organizations can reduce risk, lower exposure time, and build stronger cyber resilience.

02 Introduction

The cybersecurity landscape is evolving rapidly. Threats are more sophisticated, attacks are more targeted, and the margin for error is shrinking. In this new reality, traditional endpoint security is no longer enough. Organizations need to go beyond detection; they need intelligent, automated protection that acts before attackers can do harm.

The most effective endpoint protection strategies today combine artificial intelligence, real-time automation, and integrated compliance tools.

These technologies help organizations defend more effectively while reducing effort, complexity, and operational risk.

03 Why Endpoint Protection Must Evolve in 2025

Organizations are under more pressure than ever. Remote work has expanded the attack surface. Cybercriminals are leveraging AI to bypass traditional defenses.

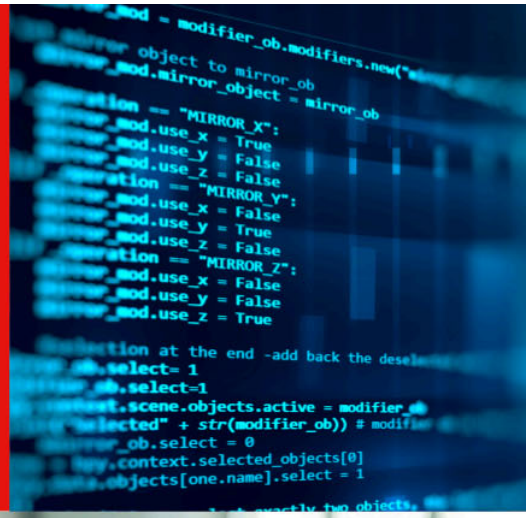
Compliance requirements are becoming stricter and more complex. And internal resources are stretched thinly.

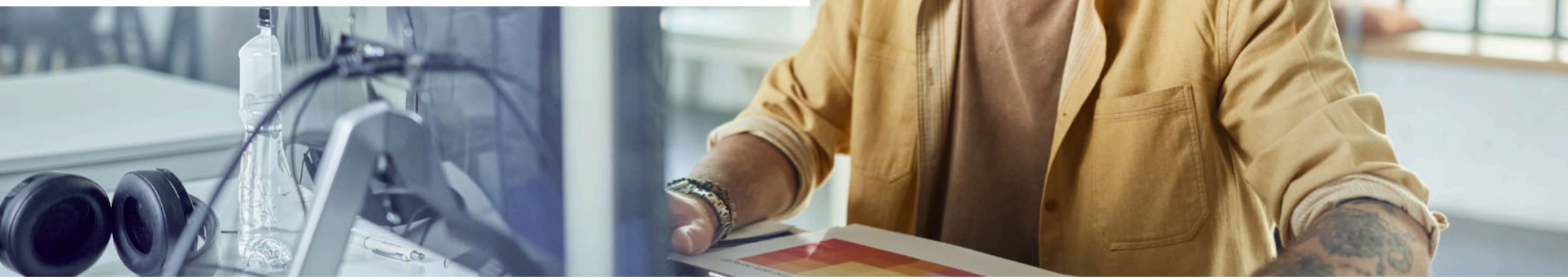
This combination of risk and complexity makes a strong case for modernizing endpoint security. In 2025, a future-ready solution must:

- Prevent unknown threats from executing
- Continuously monitor for abnormal behavior
- Automate incident detection and prioritization
- Adapt to changing compliance frameworks
- Integrate seamlessly with existing environments

A future-ready endpoint security solution should deliver on all these fronts – with lightweight agents, rapid deployment, and compatibility with existing AV environments. However, many solutions fail to integrate AI-driven prevention, real-time behavioral analysis, and automated response as standard features.

Compliance requirements are becoming stricter and more complex. And internal resources are stretched thinly.





Five Threats Your Traditional AV Can't Stop (But EDR Solutions with AI Can)

Traditional antivirus solutions were designed for a different era. While they still play a role in basic protection, they simply can't keep up with the advanced threats organizations face today. Below are five types of attacks that a modern EDR solution with AI is built to handle effectively:

1. **RDP brute-force and credential-based attacks:** Traditional AV doesn't monitor connection behavior or account abuse. EDR solutions with AI detect unusual access attempts and block lateral movement early.

2. **Unknown or polymorphic malware:** Legacy AV relies on known signatures. AI-powered EDR classifies unknown threats in real time – even if they've never been seen.

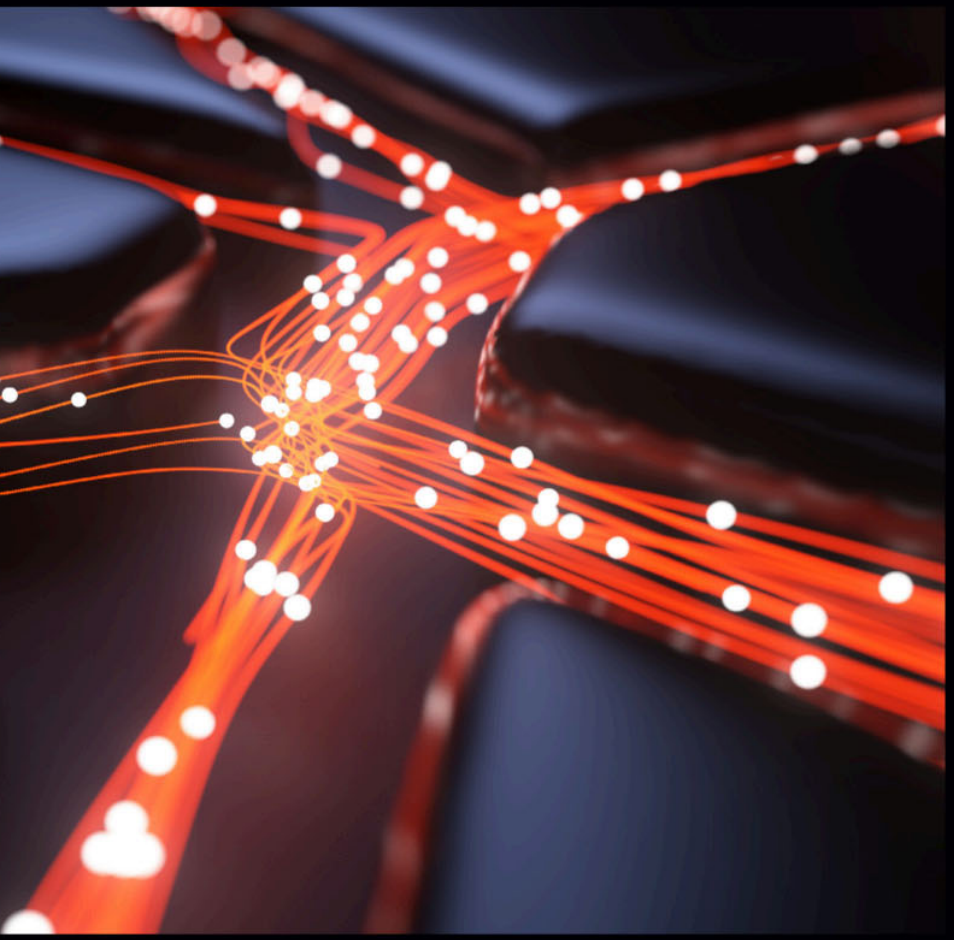
3. **Living-off-the-land binaries (LOLbins)[1] :** These techniques use legitimate, signed system binaries (like PowerShell, WMIC, or Rundll32) that attackers abuse to execute malicious actions without dropping new files. EDR identifies and stops suspicious behavior even when no malware is present.

4. **Fileless scripting and PowerShell abuse:** Script-based attacks don't drop executable files, making them invisible to AV. AI-driven detection identifies malicious intent in scripts based on behavior.

5. **Advanced vulnerability exploits:** EDR detects exploitation patterns across the kill chain, even when a patch is missing, offering real-time containment.

> These threats are increasingly common and designed to evade traditional controls. That's why modern endpoint protection must evolve beyond static detection and why EDR with AI is now essential.

1. LOLBins and LotL are related but not the same. LotL is a broad tactic that uses trusted, native tools (scripts, admin tools, scheduled tasks, etc.) to evade detection. LOLBins are a subset of legitimate system binaries (e.g., PowerShell, WMIC) abused to execute malicious actions without adding new files.



04 The Role of AI in Modern Endpoint Security

AI has become a foundational element of effective cybersecurity. In 2025, its role will be not optional but essential. AI enables faster threat detection, smarter decisions, and near-instant response.

> Security vendors with mature AI models have spent years building adaptive detection capabilities that evolve with the threat landscape, helping protect users and systems in real time.

Modern endpoint solutions powered by AI bring this to life by offering protection against various threats, including stealthy tactics like LotL attacks. These solutions deliver:

- **AI-driven behavioral detection and classification**
- **Context-aware analysis of applications and processes**
- **Autonomous prevention of unknown threats**
- **Real-time attack surface visibility**

Visibility and Risk Awareness

You can't protect what you can't see. That's why leading EDR solutions include built-in telemetry and risk dashboards to provide real-time visibility into endpoint environments. Complementary tools like patch management and encryption help reduce the attack surface and support both regulatory and insurance-related requirements.

Automated Zero Trust Protection

The first line of defense is trust or, better said, the lack of it. A modern Zero Trust model should block all unknown applications by default until they are classified as safe. This proactive approach stops threats before they execute, closing the door on malware that traditional antivirus tools miss.

Unlike reactive systems that wait for signatures or analyst intervention, a real AI-driven security platform can autonomously classify the vast majority of applications in real time. The remaining few are escalated for expert analysis, ensuring a continuous balance of speed and accuracy in preventing unknown threats.

Intelligent Correlation and Automated Response

Proactive protection doesn't stop at the application level. Modern attacks often involve subtle, stealthy behaviors that unfold over time. That's why modern endpoint detection and response (EDR) solutions continuously monitor device activity, detect abnormal behaviors, and correlate multiple signals and indicators of attack into confirmed incidents – automatically and in real time. This enables earlier detection, faster investigation, and precise remediation, reducing exposure and alert fatigue for security teams.

Endpoint Security and Compliance

Meeting regulatory requirements is a growing concern for organizations of all sizes. Whether you're preparing for NIS 2, DORA, HIPAA, or cyber insurance coverage, Modern endpoint platforms support these goals by aligning with evolving regulations and simplifying evidence-gathering for audits.

With automated risk scoring, policy enforcement, and detailed reporting, you can prove due diligence and strengthen your compliance posture without adding administrative burden.

Cyber Insurance Readiness

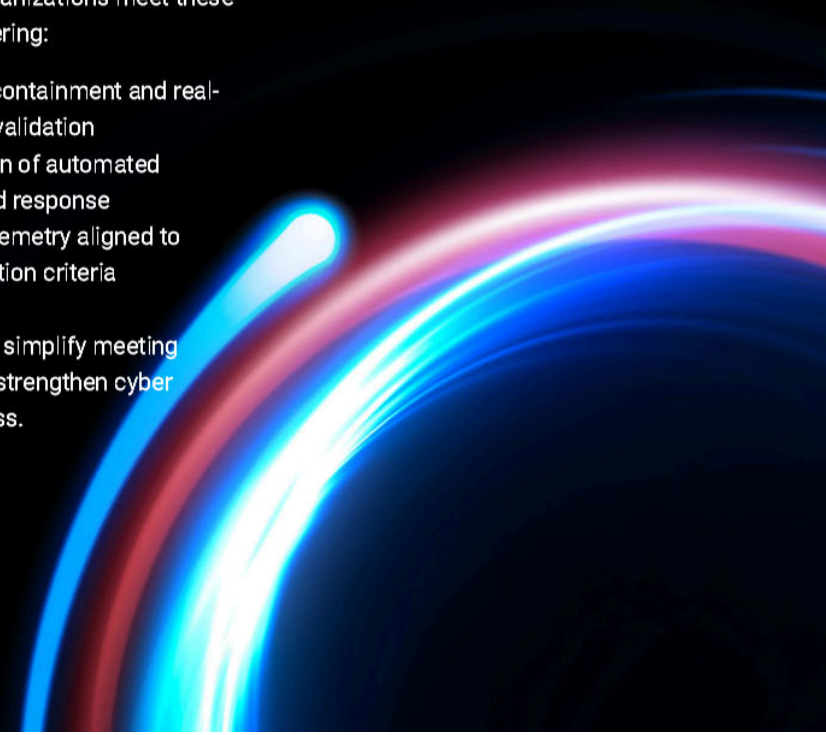
As cyber insurance becomes a requirement for doing business in many sectors, insurers are demanding higher security standards. Advanced endpoint platforms help organizations meet these demands by delivering:

- Active threat containment and real-time incident validation
- Documentation of automated prevention and response
- Risk-based telemetry aligned to insurer evaluation criteria

These capabilities simplify meeting prerequisites and strengthen cyber insurance readiness.

Simple, Efficient, Scalable

The leading endpoint security solutions are built for simplicity and scale. They work across platforms, integrate into existing IT environments, and are managed from centralized consoles designed for usability—resulting in less complexity and better outcomes.



05 Turning Strategy into Action

Throughout this eBook, we've outlined the critical capabilities that define a modern endpoint protection strategy – many of which go beyond what traditional AV or even many EDR platforms provide today.

> From AI-driven detection and Zero Trust execution control to automated correlation of living-off-the-land attacks, vulnerability visibility, and built-in compliance support, these are not just features – they're requirements.

WatchGuard EPDR brings all these capabilities together in a single, lightweight solution. It combines AI-powered behavioral detection with a Zero-Trust Application Service that uses machine learning to classify and block unknown applications before they can execute automatically.

Our AI-driven engines analyze vast volumes of telemetry data in real time. They detect anomalies, classify new threats, and automate responses without human intervention. Combined with human expertise from our Threat Hunting Service and security operations center, this proactive and hybrid model ensures speed and accuracy, reducing risk from emerging threats without disrupting your current infrastructure or replacing existing solutions.

WatchGuard MDR adds expert-driven monitoring and response, while ThreatSync enables XDR-level visibility and automated threat correlation across endpoints, networks, identities, and Cloud environments.

With modular add-ons like Patch Management and Full Disk Encryption, you can reduce your attack surface, align with compliance standards, and strengthen protection against data loss or unauthorized access.

Extending Cybersecurity Across Attack Surfaces

Endpoint protection is just one piece of the cybersecurity puzzle. In today's connected environments, organizations face threats that move laterally – from endpoints to identities to networks to Cloud. Attackers often exploit legitimate tools and system functions in these living-off-the-land techniques, making threats harder to detect and stop. A siloed approach won't cut it.

MDR

WatchGuard MDR adds expert SOC support, providing continuous monitoring,

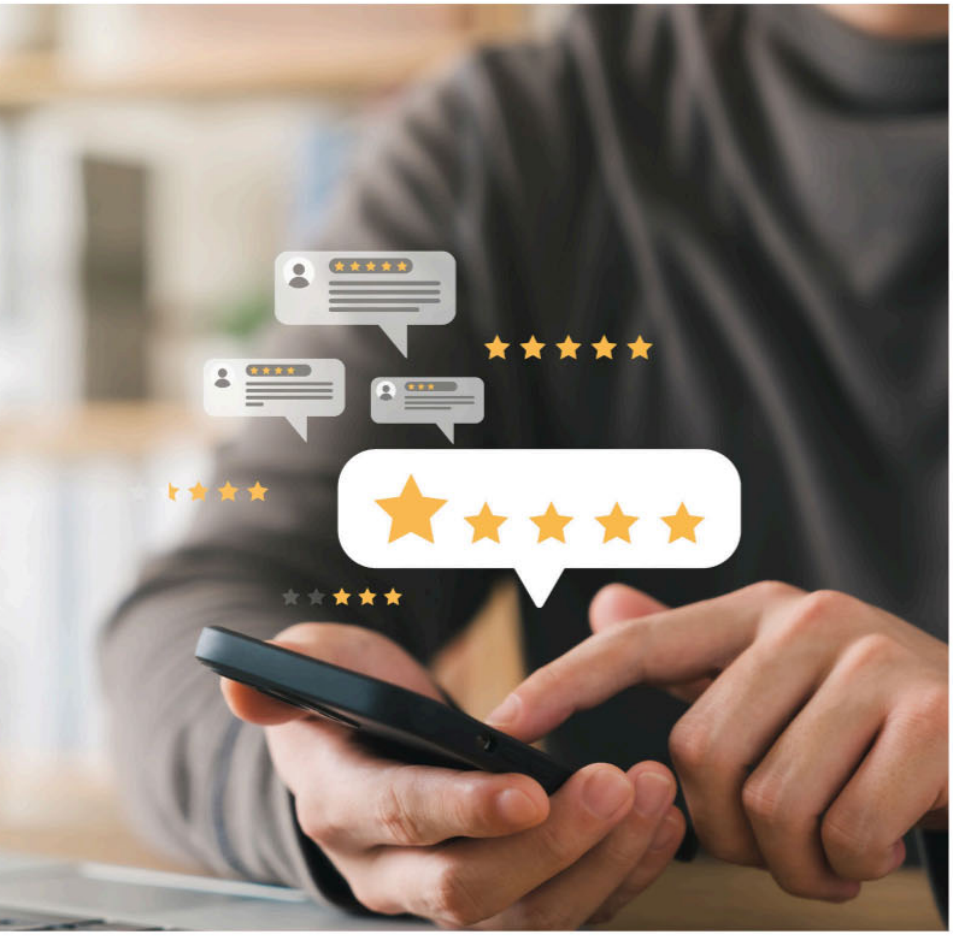
WatchGuard offers a unified approach to threat detection and response across multiple attack surfaces through ThreatSync and WatchGuard MDR.

ThreatSync

ThreatSync enables XDR-level correlation between endpoints, networks, and Cloud services, turning isolated events into coherent incident timelines. threat validation, and actionable guidance – especially critical in environments lacking in-house cybersecurity teams.

Together, these solutions provide a cohesive, scalable defense strategy – proactively identifying, correlating, and responding to threats wherever they emerge.

WatchGuard



Proven Performance and Industry Recognition

Independent validation matters when choosing an endpoint security solution. WatchGuard's approach is innovative, tested, and trusted.

In 2024, WatchGuard Endpoint Security earned top marks in multiple independent assessments:

- PassMark Software recognized WatchGuard with a leading score in performance, protection accuracy, and resource efficiency.
- MITRE ATT&CK evaluations confirmed 100% protection against malware samples, with strong detection across all stages of the attack chain.
- Industry analysts and global awards recognized WatchGuard as a top endpoint security provider for usability, automation, and threat prevention.

This recognition reinforces what our customers experience every day: endpoint protection that is smart, effective, and built for today's cyber landscape.

PASSMARK SOFTWARE

MITRE | ATT&CK Evaluations

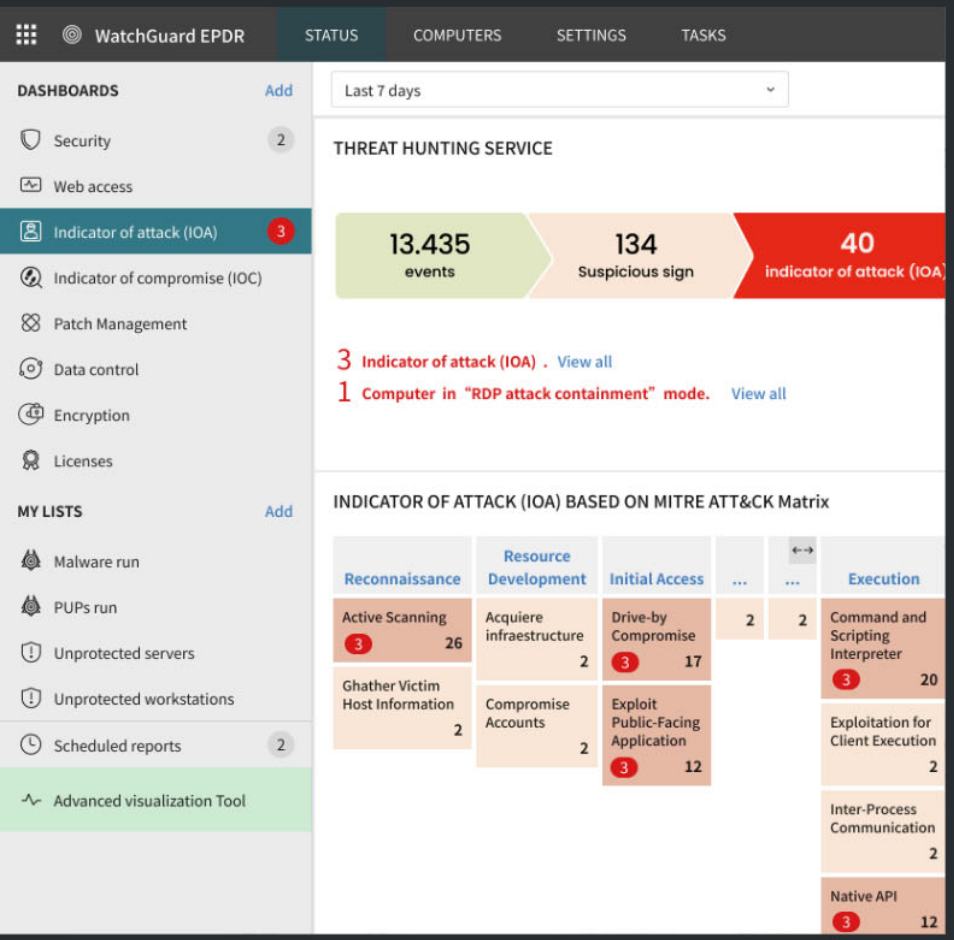
canalys GLOBAL CYBERSECURITY CHAMPION 2025

EXCELLENCE IN CUSTOMER SERVICE AWARD 2024

THE CHANNEL CO. CRN PARTNER PROGRAM GUIDE WINNER 2025

2024

WatchGuard



Get Ready for the Future, Today.

Cybersecurity is no longer just a technical necessity — it's a strategic imperative. In a world where threats are invisible, automated, and relentless, protecting your endpoints isn't enough. You need to get ahead of them.

With WatchGuard EPDR, you don't just block threats — you prevent the unknown, automate the complex, and turn chaos into control.

With MDR and ThreatSync, you extend that intelligence across your entire attack surface.

And with our Unified Security Platform, you simplify operations without compromising protection.

It's time to move beyond patchwork solutions.

It's time to embrace truly proactive defense.

Ready to take the next step?

See WatchGuard EPDR in action.

Request your free trial and start protecting the future of your organization today:

Start Now

WatchGuard

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.

Identity Security

WatchGuard's AuthPoint Identity Security solutions are designed to provide top-rated multi-factor authentication (MFA) and zero trust risk policies for maximum online protection. Additionally, leverage our dark web monitoring services to mitigate the risks of widespread workforce credential attacks. AuthPoint is dedicated to delivering the ultimate user experience and offers online and offline authentication methods, along with a web application portal for easy single sign-on access.

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.

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.

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