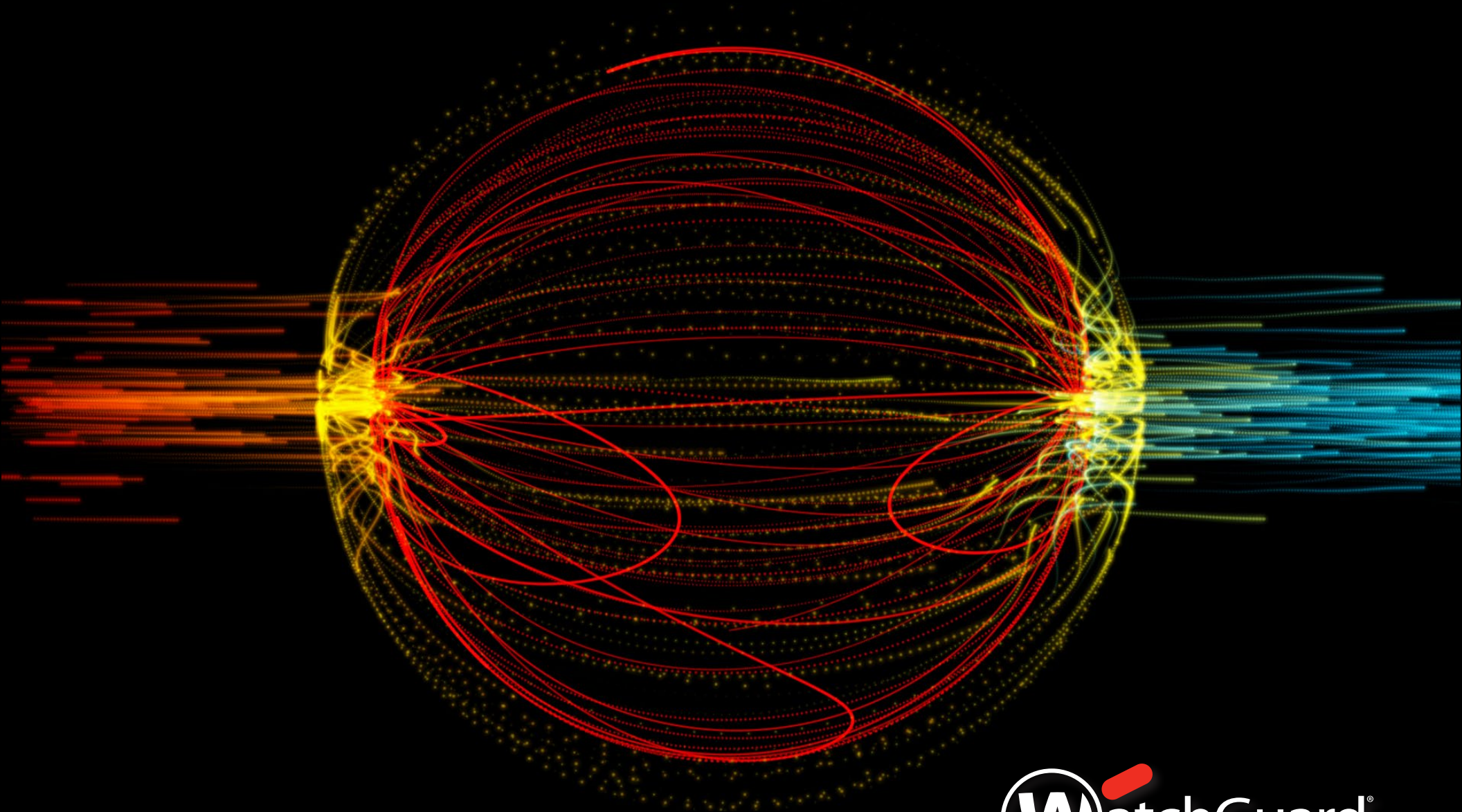


The WatchGuard Automation Core: Building an Intelligent, Autonomous, and Extensible Perimeter



Contents

The New Perimeter	3
The Need for a Unified Security Platform	4
Protecting an Expansive Perimeter Through an Automation Hierarchy	5
Automation Hierarchy	5
01: Management Visibility Automation	6
02: Operational Automation.....	7
03: Responsive Security Automation	8
04: Predictive Security Automation	9
The WatchGuard Automation Core	10

The New Perimeter

Firewalls have been foundational to protecting endpoints and networks since the early days of the web. The importance of their role has not diminished. The modern next-generation firewall sits at the heart of a business performing critical networking and security functions. Firewalls combine many security controls in one place, increasing your overall security efficacy, and making layered security attainable for some organizations that couldn't implement it otherwise. As the gateway to your computing environment, a firewall is a critical security sentry, assessing every bit and byte as it enters and exits your network. Unfortunately, it is a critical component of protection that has become so familiar to us that its role is often taken for granted.

No single security tool has more insight into and control over your security posture – but as more business traffic occurs off of the network, the role of the firewall must evolve to be part of a larger unified security platform.



The Need for a Unified Security Platform

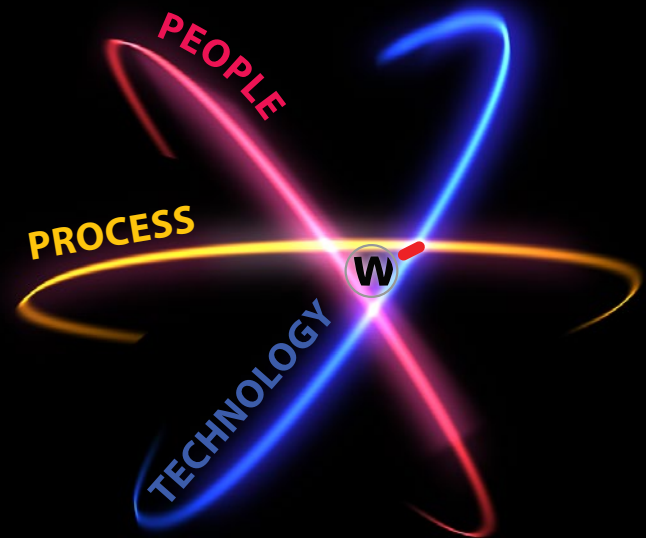
As the perimeter becomes less tangible, businesses need to be able to extend the security capabilities of their network to users and devices, no matter where they may be. Employees, contractors, visitors, and their devices regularly enter and leave your network as they perform their duties on- and off-premises. Yet, in today's aggressive threat landscape, a single infected endpoint or stolen password could open the floodgates for an attacker. Securing your computing environment in the 2020s requires more than a locked door; it requires careful consideration of your points of vulnerability, and the ability to easily address them.

A Unified Security Platform (USP) allows for a greater degree of coordination across your people, processes, and technology, the benefit of which is stronger security and improved efficiency.

PEOPLE. People represent the most significant point of vulnerability in any organization. Educating users to be aware of threats and improve passwords is a no-brainer, but relying on consistent application of best practices alone is a losing proposition. A unified security platform can not only help enforce best-practice compliance, it can support security awareness training initiatives and provide you greater insight into the users who pose the greatest risk.

PROCESSES. While prevention is the ultimate goal, every business needs a game plan for how to quickly respond to a cyber attack. By consolidating threat intelligence and responsive capabilities to a single platform, a unified security platform makes it possible to identify, triage, and mitigate threats wherever they pop up.

TECHNOLOGY. Effective layered security is only made possible when those layers are not deployed in isolation. When each layer is able to "talk" to the other, your threat picture benefits from greater context. A unified security platform brings all of these technologies together seamlessly, allowing your team to quickly identify, prioritize, and mitigate threats.



Protecting an Expansive Perimeter Through an Automation Hierarchy

More than ever, IT leaders need security with a high degree of autonomy and automation to eliminate wasted time, optimize network performance, and deliver the highest resilience to cyber attacks. Automation is key to delivering an effective Unified Security Platform that empowers your team to do more. Greater automation allows technology providers to deploy more sophisticated techniques that match up with today's sometimes complex network architectures and offer greater protection against the latest evasive threats that resource strapped teams miss all too often.

For some businesses, automating manual, repetitive tasks related to the management and maintenance of the perimeter will yield dramatic results compared to how their team operates today. Meanwhile, another business may derive immediate benefit from automated Cloud deployment and tight integration with the web services they are already using.

Automation Hierarchy

At the highest levels of automation, a unified security platform can operate in near-autonomy, enabling significant advantages to IT teams including:

- Accelerated detection and response
- Significant savings in staff hours and cost
- Increased visibility and actionable insight

Level 1: Management & Visibility	Signature & Software Updates	Ready-to-Use Reports & Dashboards		Secure Firewall Defaults
Level 2: Operational	Cloud Deployment	License Management	Invoice & Support Ticket Processing	API & Web Service Integration
Level 3: Responsive Security	Behavioral & Statistical Modeling	Remediation	Threat Correlation	Endpoint Isolation
Level 4: Predictive Security	AI-powered Prevention, Detection, Triage, and Remediation			

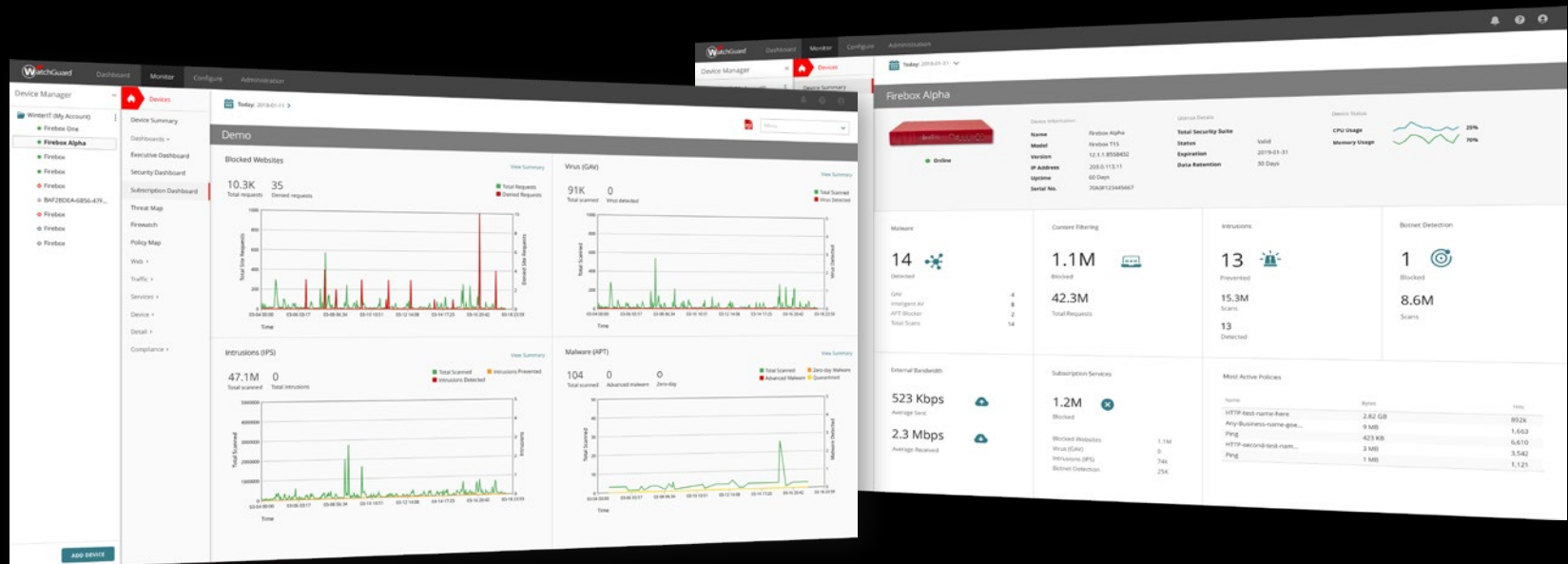
Level 1: Management & Visibility

How can I minimize frequent, repetitive and error-prone manual tasks?

99% of network breaches occur because of a misconfigured firewall.² Automating management and visibility tasks allows for “one set-up, repeated use” that replaces frequent, error-prone manual tasks with automated processes.

Save time with:

- Security as a default. Ensure the device is deployed with optimized security right out of the box.
- Automated updates. Regularly scheduled software and signature updates keep your environment protected against the latest known threats.
- Reports and dashboards. Look to reports stocked with real-time data and actionable, simplified insights from throughout the network, to make discovering issues, proving compliance, and demonstrating value easy, while saving years of staff time compared to manual compilation.



2. <https://www.gartner.com/en/documents/3215918>

Level 2: Operational

How can I more efficiently deploy and support our security offering?

Deploying new devices in a remote location can be costly and time consuming. Operational automation uses the power of the Cloud to facilitate deployment, ongoing management, and support.

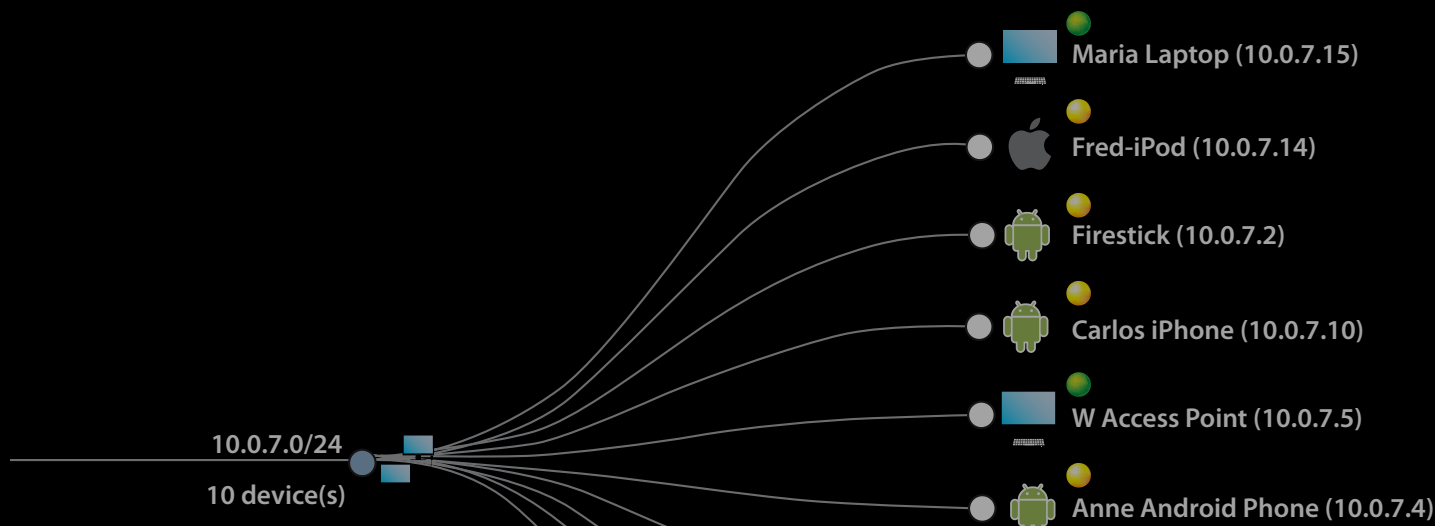
For IT services organizations, this includes software and device license management.

Save time with:

- Zero-touch deployment. Preconfigure and securely deploy devices from the Cloud. No need to send IT staff on-site.
- API and web service integrations. Integrate with the leading web applications.
- Streamlined software license management. Seamlessly integrate processes with Professional Services Automation (PSA) tools.
- Integrated support ticket management. Tightly integrate Remote Monitoring and Management (RMM) tools to allow for more rapid response to support requests.

TIP:

Asking a service provider about their operational automation can shine a light on their ability to be responsive, efficient, and compliant with service-level agreements, and ultimately provide you with the best possible service.



Level 3: Responsive Security

How can I respond faster, and stay up to date with the latest threat intelligence?

Responding to threats in a timely fashion can be the difference between a quick fix and a major security incident. The average business spends hundreds of man hours each week cleaning, fixing and/or patching networks, applications and devices.³ Only 39% of businesses feel they are highly effective at detecting threats.⁴ Automating security response makes it possible to detect and kill threats in minutes instead of months, without needing to scale your team.

Save time with:

- **Advanced detection.** Behavioral and statistical modeling is used to detect ongoing attacks by correlating security event information from on and off the network with threat intelligence feeds. Potential threats can be further triaged in an integrated sandbox environment.
- **Correlated threat scoring.** Correlated threat scoring to take the guesswork out of the process.
- **Automated response.** Automatically move to remediate the threat when a malicious file or process is identified.
- **Endpoint containment.** Immediately isolate infected endpoints from the broader network until they can be returned to good order.

3. <https://go.juniper.net/assets/pdfs/OSI/2000683-001-EN.pdf>

4. <https://go.juniper.net/assets/pdfs/OSI/2000683-001-EN.pdf>

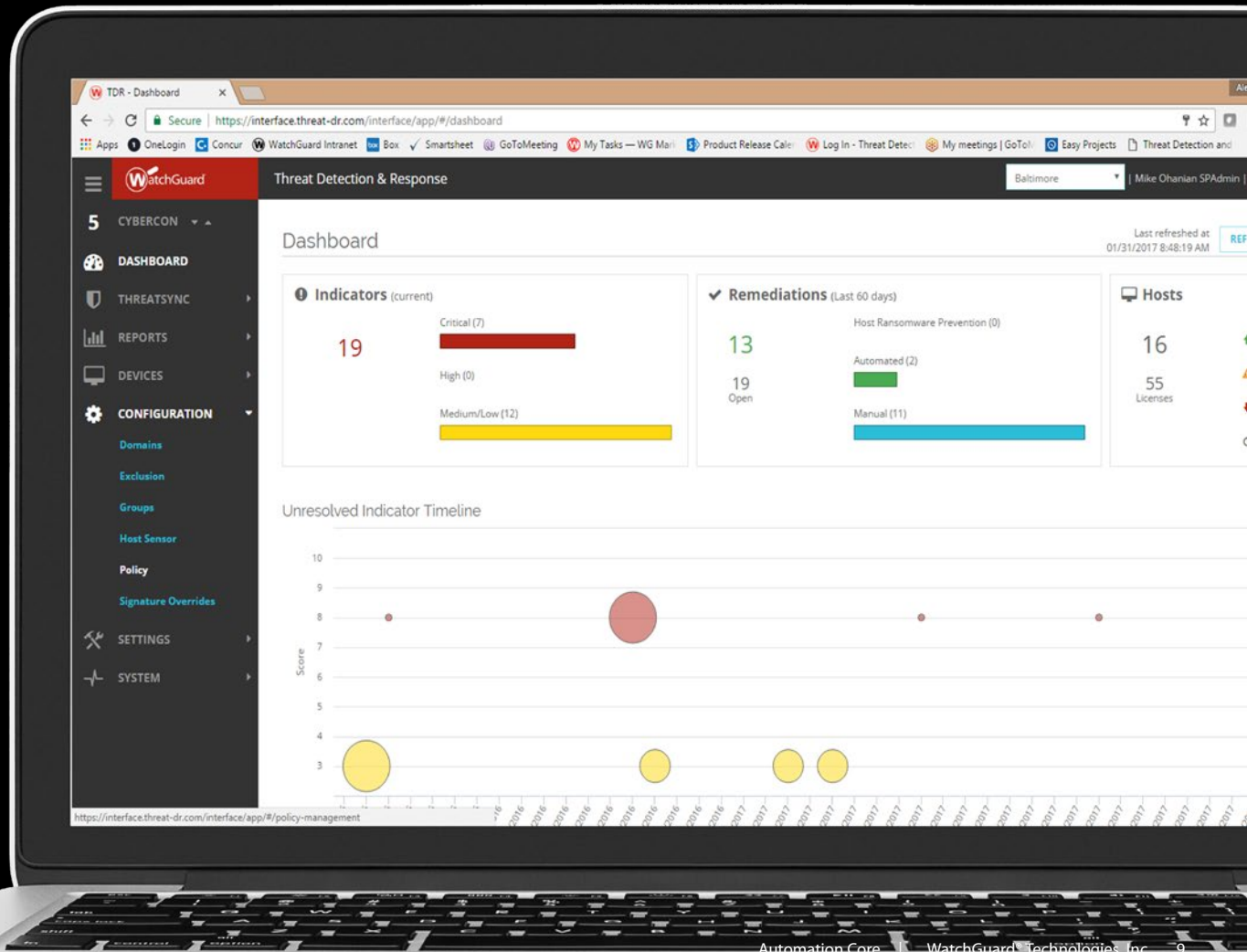
Level 4: Predictive Security

How can I block advanced threats without hiring a team of security experts?

Stopping an attack from entering your environment is the best way to keep your organization safe. Level 4 Security Automation employs artificial intelligence (AI) technology to continually predict and defend against new threats.

Save time with:

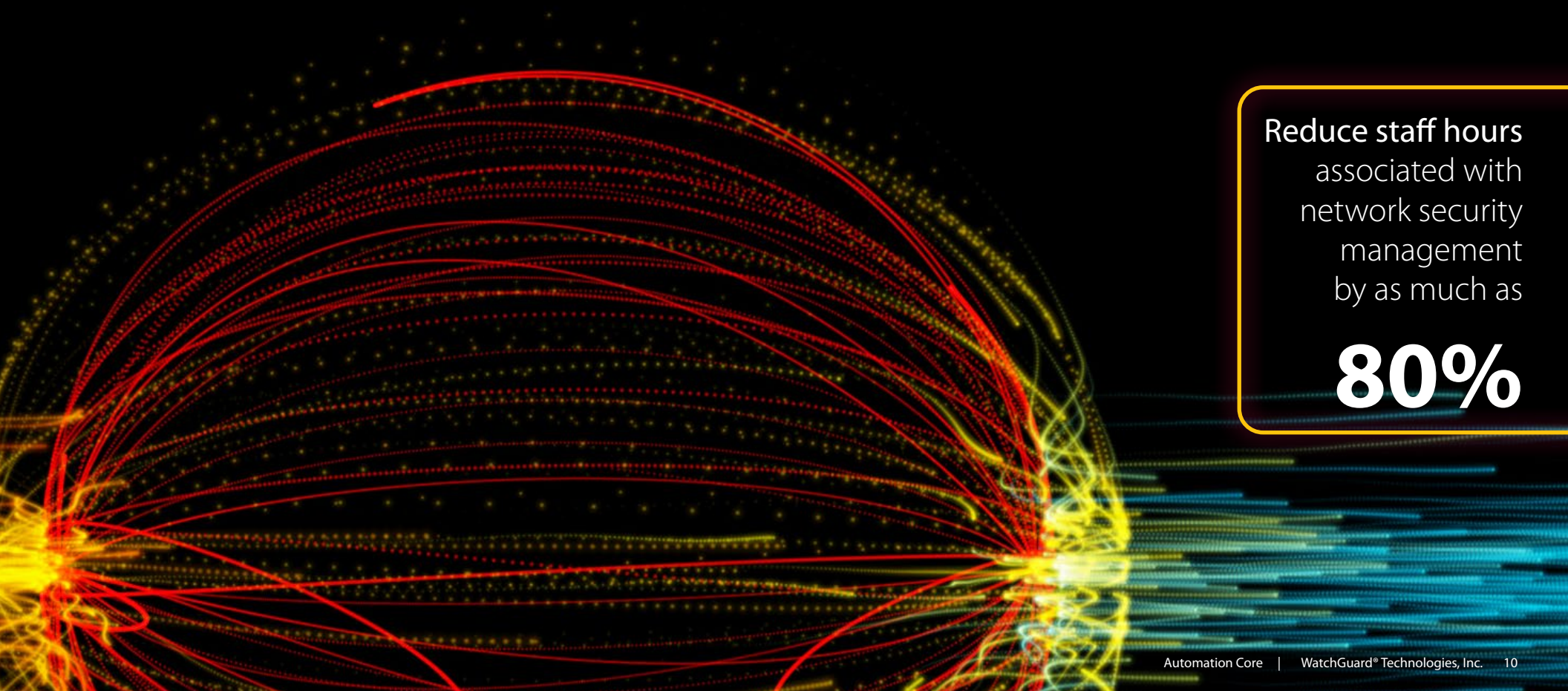
- **Breach avoidance.** Recapture IT staff time spent on post-breach clean-up that could have otherwise been averted.



The WatchGuard Automation Core

Automation is at the heart of WatchGuard's Unified Security Platform, speeding up processes, killing threats, and empowering IT teams to do more with less. Defined as the WatchGuard Automation Core, our use of automation is uniquely comprehensive and addresses all four automation levels. Automating these processes has been shown to **reduce staff hours associated with network security management by as much as 80%** when compared with traditional network security solutions.

WatchGuard's Automation Core creates a zero-touch security feedback loop and accelerates business-driven security management. The Automation Core makes it possible to seamlessly extend security capabilities to every computing environment where your business operates. It defines an intelligent, autonomous perimeter extending from the LAN, to the Cloud, and ultimately the endpoint to deliver persistent, integrated protection for your business. An Automation Core ensures secure user access to essential resources, blocks advanced threats from entering your network, keeps endpoints free of malware, and optimizes network performance, while requiring minimal interaction from your IT team.



Reduce staff hours
associated with
network security
management
by as much as

80%

Building Blocks of the WatchGuard Automation Core

Level 1	WatchGuard Firebox. The Firebox platform features firewall defaults and ready-to-use logs and reports, helping your team get up and running quickly, while ensuring the devices are configured securely.
	WatchGuard Cloud. WatchGuard Cloud provides real-time data and actionable, simplified insights from throughout your deployment. Managing Firebox system tasks and running reports is easy with our ready-to-use report templates. Further, WatchGuard Cloud is the only Cloud-based management platform on the market to enable full multi-tier, multi-tenant capabilities.
Level 2	RapidDeploy. Pre-configure your Firebox from the Cloud for zero-touch deployment that doesn't require your IT staff to go on-site.
	WatchGuard Firebox. Tight integration and the availability of APIs for the leading PSA and RMM tools allow for easier license management and faster response to support requests.
	AuthPoint MFA. WatchGuard's AuthPoint service includes automated token management as well as AD and LDAP sync features that make it easy to deploy.
Level 3	ThreatSync, APT Blocker and DNSWatch. WatchGuard spots suspicious DNS behavior and blocks users from connecting to risky sites up front. Next, we correlate signals from network and endpoint devices to assess threat conditions, using sandboxing when needed for a deeper look. And without you lifting a finger, our solution automates remediation tasks to contain a threat in seconds. Best yet, this automated protection protects your users and data, no matter whether they are on-site or away from the office.
Level 4	IntelligentAV. Our AI-powered antivirus is the only firewall solution to block major threats 33 months before they appeared in the wild, making WatchGuard the only firewall platform with an Automation Core featuring Level 4 predictive protection!

The WatchGuard Automation Core Delivers:

Security Efficacy

- The average Firebox blocked over 2,100 malware variants in 2019, nearly 40% of which were classified as zero day, that is, completely undetectable by signatures. Each device blocked a further 240 network attacks on average.
- In the NSS Labs testing, WatchGuard was one of just 2 firewall platforms that had ZERO missed evasions. WatchGuard has achieved the Recommended rating three years running.

Extensibility

- Protect your users from phishing and ransomware, on- and off-network.
- Isolate endpoints, and remediate threats anywhere in the world.
- Control access to assets, accounts and information with integrated multi-factor authentication and SSO for centralized access to Cloud-hosted applications, and internal resources via RDP and SSH.
- Seamlessly apply granular policies to users and devices as they transition in and out of the network.

Higher IT Staff Utilization

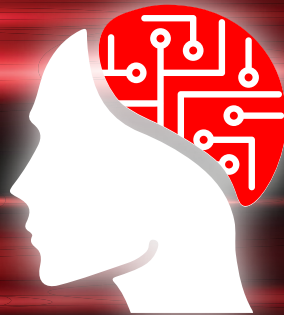
- Over 12,000 deployments have used our Cloud deployment service, spending 1/100th the time and cost of a standard device set-up and configuration.
- WatchGuard's powerful visibility tools provide more than 100 dashboards and reports built-in, saving hundreds of hours compared with searching through logs for time-sensitive answers on usage and anomalies.

Less Time and Money Spent

- Using AI, the Firebox platform predicts threats up to 33 months before they appeared in the wild.
- Should attacks find their way to the network, the Automation Core makes it possible to spot suspicious behaviors early and automatically contain and remediate threats in minutes instead of the months it could exist on your network otherwise.

WatchGuard Delivers Across the Full Spectrum

When you need to do more with less, our WatchGuard Cloud, DNSWatch, ThreatSync and IntelligentAV products are changing the game so that IT teams can stay on top of security and still deliver value across the full spectrum of IT responsibilities. The Automation Core makes it possible to extend the value of the WatchGuard unified security platform beyond your core network to every environment your business operates in, while freeing up IT staff time and delivering superior protection against the latest threats.



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 management, 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.

Find out more

For additional details, talk to your authorized WatchGuard reseller or visit <https://www.watchguard.com>.

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 midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Pacific, and Latin America. To learn more, visit [WatchGuard.com](https://www.watchguard.com).



North America Sales: 1.800.734.9905

• International Sales: 1.206.613.0895

• Web: www.watchguard.com