WatchGuard

Millgate

Helping clients succeed for 25 years

6 ESSENTIAL FEATURES OF A MODERN FIREWALL

1. HIGH PERFORMANCE SSL/TLS INSPECTION

If you aren't using HTTPS decryption and content inspection, you're likely **missing 2/3 of the malware** entering your organization.

Over 80% of business traffic occurs over encrypted channels and 50% of phishing sites use HTTPS to hide their attacks. HTTPS inspection makes it possible to decrypt HTTPS traffic, examine the content for signs of attack, then encrypt the traffic again with a new certificate for safe delivery.

WITHOUT DECRYPTION:
No visibility into data type, application, policy adherence, file type, or data exfiltration attempts via HTTPS.

TIPS

Look for a firewall with high performance HTTPS inspection when ALL security services are active.

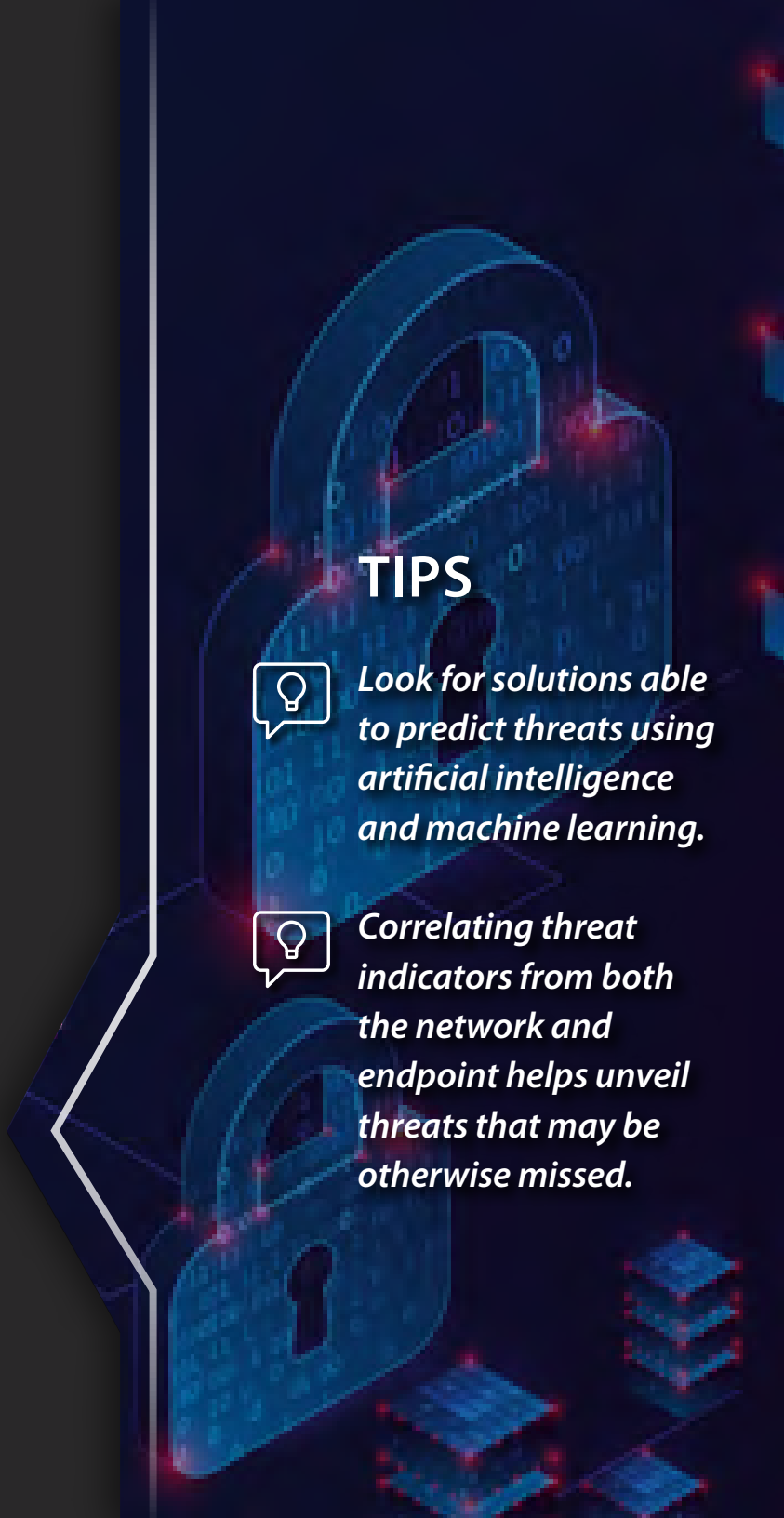
Look for a solution that supports FULL inspection of TLS 1.3.

2. LAYERED ZERO DAY MALWARE DEFENSES

Zero day malware accounts for **64% of all malware** threats encountered on the typical business network.

A zero day attack is an attempt to exploit a vulnerability in computer software or equipment, before that vulnerability has been disclosed and a specific preventive measure exists. Zero day protection, therefore, is the ability to block such a threat, even though the exact mechanisms of the attack are unknown.

LAYER FOR MAXIMUM COVERAGE:
AI-powered detection, Cloud sand-boxing, integrated endpoint detection and response.



TIPS

Look for solutions able to predict threats using artificial intelligence and machine learning.

Correlating threat indicators from both the network and endpoint helps unveil threats that may be otherwise missed.

3. PHISHING AND HAPPY-CLICKER PROTECTION

83% of businesses have fallen victim to a phishing attack.

Hackers rely on DNS to phish unsuspecting victims, so careful examination of DNS requests is a great way to find and ultimately intercept attacks. Unwitting attempts to connect to known malicious DNS addresses by your users can be automatically blocked, and the user is seamlessly redirected to a safe landing page.

THE FIRST LINE OF DEFENSE:
Block malicious clickjacking and phishing domains regardless of the connection type, protocol, or port.

TIPS

Look for solutions that block both phishing attempts and command and control channels.

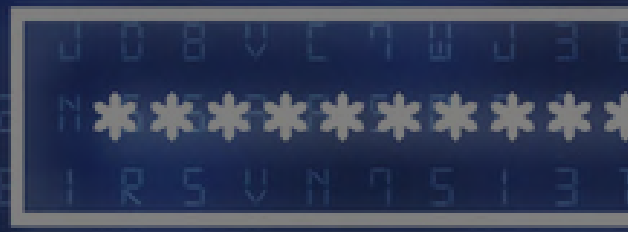
Look for solutions that provide in-the-moment education when a user mistakenly falls for a phish.

4. WEB-BASED PORTAL FOR SECURE ACCESS

The average user spends **36 minutes per month** manually entering their credentials, wasting nearly a full workday per year, per employee.

With single sign-on, employees can log in one time, with a single set of credentials, and access all of the applications, websites and data they need. SSO improves security by minimizing the password burden on users, and lightens the load on IT teams swamped with password reset requests.

BEST PRACTICE:
Combine SSO with MFA to secure RDP (remote desktop), SSH, and web access connections.



TIPS

Make sure the portal supports popular identity providers, like AuthPoint, Shibboleth, OneLogin, ADFS and Okta.

Look for a solution that supports the most common software tokens, including AuthPoint, Okta Mobile, Google Authenticator, OneLogin Protect, Duo Mobile, RSA SecureID.

5. SUPPORT THE LATEST VPN TECH

68% of companies expanded their VPN usage as a direct result of COVID-19.

Virtual Private Networks (VPNs) are used to provide a secure tunnel from remote locations back to a central office. There are several different types of mobile or remote user VPN technology available to use. Some firewall vendors sell additional VPN licenses with the firewall, whereas others include the full capacity of licenses with each model.

REMOTE USER VPN TECHNOLOGIES:
IKEv2 (newest, fastest), IPSec (but don't use pre-shared keys), SSL (most widely used), L2TP (legacy, avoid!)

TIPS

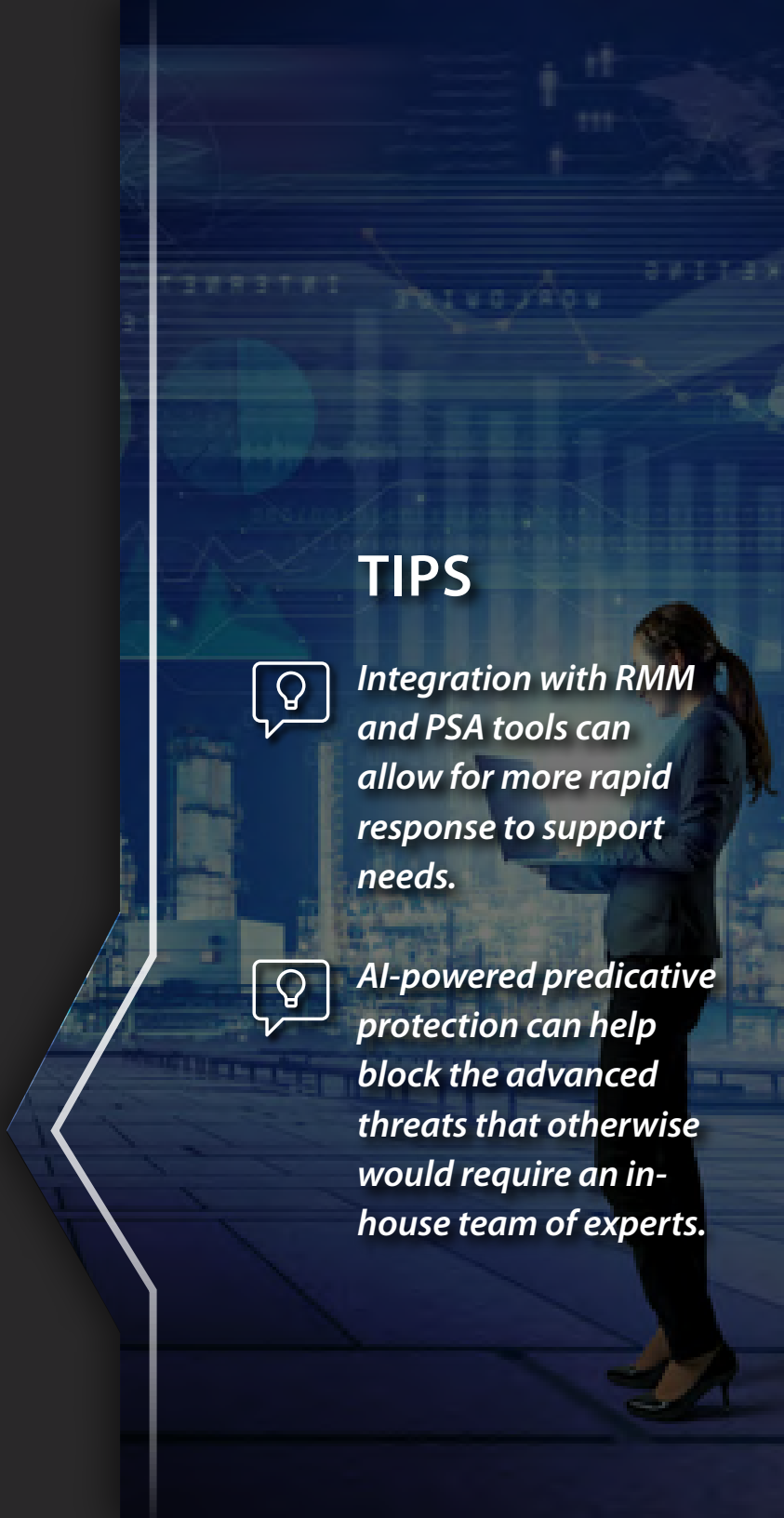
- ***MFA should be applied to logins to Cloud-hosted (SaaS) applications, and also to VPN access to corporate networks.***
- ***Look for platforms that support a default route tunnel with traffic tunneled back to the central firewall for full security inspection.***

6. NATIVE AUTOMATION

Automation has been shown to **reduce the staff-hours** teams spend on security management by as much as 80%.

Keeping pace with threats, reducing time/money waste, and increasing visibility in a modern network environment require a high degree of automation. Unified security platforms are designed with automation from the ground up and can not only keep pace, but extend the security value of your network beyond the traditional perimeter.

4 LEVELS OF AUTOMATION:
Management, operational, responsive, and predictive.



TIPS

Integration with RMM and PSA tools can allow for more rapid response to support needs.

AI-powered predicative protection can help block the advanced threats that otherwise would require an in-house team of experts.

Firebox®

1. Best-in-class SSL/TLS decryption
2. 3 layers of zero day protection
3. Cloud-based DNS filtering
4. Access Portal comes standard
5. 4 Mobile VPN types, including IKEv2
6. Delivers all 4 levels of security automation

250
Network Attacks

1,300
Malicious Files

~ average number of threats blocked per Firebox in 2019

> **WatchGuard earned** high security effectiveness and low total cost of ownership, and is **one of the only two products to block 100% of evasions.**
>
> - NSS Labs

THE WATCHGUARD SECURITY 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 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 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 cyber attacks. Its flagship solution, Panda Adaptive Defense 360, 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.

WatchGuard®

WEB www.millgate.co.uk

Millgate

Helping clients succeed for 25 years