

APT BLOCKER

Protection from advanced malware including ransomware, advanced persistent threats, and zero day exploits

What makes today's threats so dangerous is that they can easily morph into code that will evade traditional forms of malware pattern recognition and defense. WatchGuard's APT Blocker uses award-winning, next-generation sandbox technology to analyze traffic to detect potential threats before malware can reach your network. By detonating suspicious code in a harmless virtual environment, WatchGuard's APT Blocker can determine the full attack lifecycle of a file and prevent it from entering the network.

"Our latest WatchGuard devices all have APT Blocker. As cyber criminals come up with new ways to poke holes in your security, we need ways to keep them out."

~ David Dongray, IT manager for Network Aviation Group

THREATS HAVE NOWHERE TO HIDE

Advanced threats, including APTs (advanced persistent threats), are designed to recognize traditional forms of malicious code detection and use evasive methods to remain concealed on victim networks. APT Blocker's full system emulation – which simulates physical hardware, including CPU and memory – provides the deepest level of visibility into malware behavior without compromising your network.

LAYERS OF SECURITY

APT Blocker works in tandem with our Gateway AntiVirus (GAV) for the ultimate solution in detecting and preventing advanced malware. First GAV eliminates known threats, saving processing power by pre-filtering known threats so that only suspicious files are sent to APT Blocker. If the suspected file is found to be dangerous, APT Blocker quickly takes action to ensure your network and digital assets stay secure.

EASY TO USE

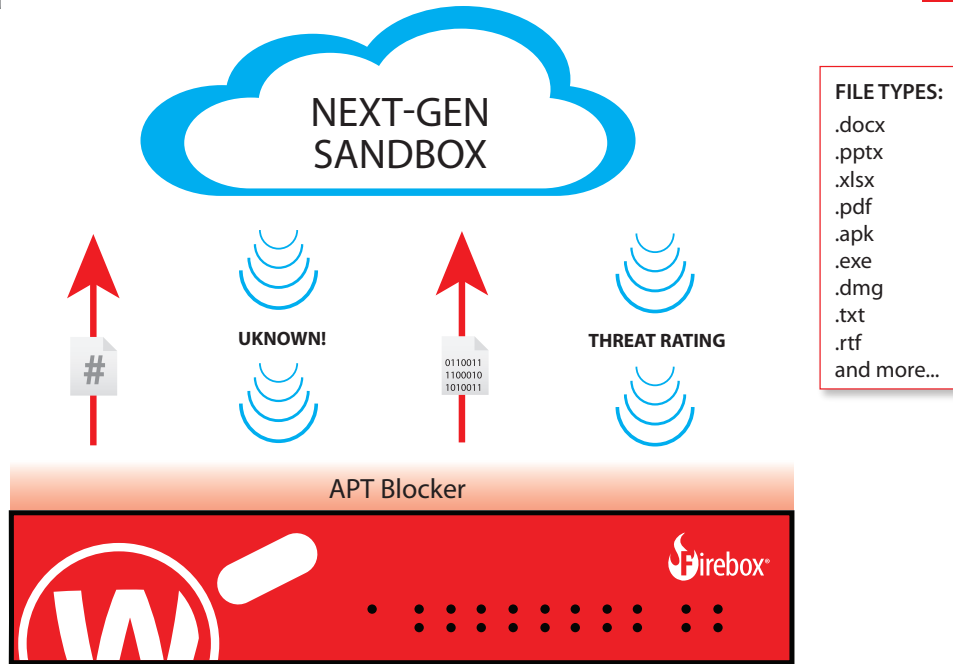
APT Blocker not only provides comprehensive protection against advanced malware, it does so with a simple and intuitive user interface. From the management console, you can access easy-to-use controls that enable you to allow, drop, block, or quarantine by severity level, as well as set customized notifications for APT Blocker detection events.

UNPARALLELED VISIBILITY

Gain complete visibility into the advanced threats attempting to attack your network with WatchGuard Cloud, which comes standard on all WatchGuard UTM solutions. You'll know the protocols used, threat IDs, source information, and the specific types of malicious activities that would have happened if APT Blocker did not take action. Over 100 reports and dashboards enable summary and granular reporting – invaluable in demonstrating compliance with industry and government regulations.

FEATURES & BENEFITS

- Provides advanced protection against ransomware, zero day threats, and evolving malware
- Average analysis time is less than two minutes
- Thoroughly analyzes a wide range of executables and documents, including Office files types
- Delivers Instant threat response with automated alerts
- Seamless integration with WatchGuard Cloud for complete visibility
- Conveniently bundled in WatchGuard's Total Security Suite for a hassle-free, unified solution to today's sophisticated threats



WatchGuard has the industry's largest network of value-added resellers and service providers. Browse our network of certified partners at findpartner.watchguard.com.

TOTAL SECURITY SUITE

STRONG SECURITY AT EVERY LAYER

Uniquely architected to be the industry's smartest, fastest, and most effective network security products, WatchGuard solutions deliver in-depth defenses against advanced malware, ransomware, botnets, trojans, viruses, drive-by downloads, data loss, phishing and much more.

ONE PACKAGE. TOTAL SECURITY.

The flexibility of WatchGuard's integrated platform makes it easy to have exactly the security components your business network requires. Whether you choose to start with the security basics or deploy a comprehensive arsenal of network defenses, we have bundled security services to match your requirements.

	SUPPORT	BASIC SECURITY	TOTAL SECURITY
Stateful Firewall	✓	✓	✓
VPN	✓	✓	✓
SD-WAN	✓	✓	✓
Access Portal*	✓	✓	✓
Intrusion Prevention Service (IPS)		✓	✓
Application Control		✓	✓
WebBlocker		✓	✓
spamBlocker		✓	✓
Gateway AntiVirus		✓	✓
Reputation Enabled Defense		✓	✓
Network Discovery		✓	✓
APT Blocker			✓
DNSWatch			✓
IntelligentAV**			✓
ThreatSync (XDR)			✓
EDR Core			✓
WatchGuard Cloud			
Log Data Retention		90 Days	365 Days
Report Data Retention		1 Day	30 Days
Support	Standard (24 x 7)	Standard (24 x 7)	Gold (24 x 7)

*Not available on Firebox T20/T20-W, T25/T25-W, or T35-R. Total Security Suite required for M270, M370, M470, M570, M670, FireboxV and Firebox Cloud.
 **Not available on Firebox T20/T20-W, T25/T25-W, or T35-R.

THE WATCHGUARD PORTFOLIO



Network Security



Multi-Factor Authentication



Secure Cloud Wi-Fi



Endpoint Security

Contact your authorized WatchGuard reseller or visit www.watchguard.com to learn more.