WatchGuard Total Security

Complete network protection in a single, easy-to-deploy solution.

Total Security.

A stateful packet firewall, while essential, simply isn't enough anymore. The reality is that every network needs a full arsenal of scanning engines to protect against spyware and viruses, malicious apps and data leakage – all the way through ransomware, botnets, advanced persistent threats, and zero day malware. A true network security solution will address all aspects of threat prevention, detection, correlation, and response – today, and as those threats evolve. WatchGuard's award-winning network security platform not only provides the most complete suite of unified security controls on the market today, but has consistently been the first to offer solutions for addressing new and evolving network threats including, but not limited to, advanced malware and ransomware.

Total Simplicity.

It's more than just about security scanning engines, though. At WatchGuard, we believe simplicity is the key to successful adoption of technology. As such, all of our products are not only easy to initially configure and deploy, they are also designed with an emphasis on centralized management, making ongoing policy and network management simple and straightforward. Security is complex, managing it doesn't have to be.

Total Performance.

All businesses, regardless of size, need to pay attention to performance. Slow security scanning times can cripple a network's ability to handle high-volume traffic. Some companies are forced to decrease protection to keep performance strong, but WatchGuard solutions never make you choose between security and speed. Leveraging the power of multi-core processing, WatchGuard's platform is engineered to deliver the fastest throughput when it matters – with all security controls turned on. Our platform can run all scanning engines simultaneously for maximum protection while still maintaining blazing fast throughput.

Total Visibility.

From the board room to the branch office, critical decisions about network security often need to be made quickly and with limited information. How can you ensure that your decisions are timely, effective, and better informed? You need visibility. Visibility is about more than data. Visibility is achieved when that data is converted into easily consumable, actionable information. WatchGuard's award-winning network visibility platform, Dimension, takes the data from all devices across your network and presents that data in the form of visually stunning, immediately actionable information. Using Dimension you can identify behavioral trends, pinpoint potential network threats, block inappropriate use, monitor network health and much more.

Enterprise-Grade Security

Simplicity

Top Performance

Threat Visibility

Future-Proofed

WatchGuard Security Services

WatchGuard offers the most comprehensive portfolio of network security services, from traditional IPS, GAV, application control, spam blocking, and web filtering to more advanced services for protecting against advanced malware, ransomware, and the loss of sensitive data. WatchGuard also offers a full suite of network visibility and management services.

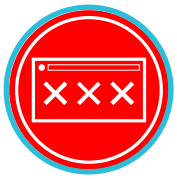
FUNDAMENTAL SECURITY SERVICES

INTRUSION PREVENTION SERVICE (IPS)

IPS uses continually updated signatures to scan traffic on all major protocols to provide real-time protection against network threats, including spyware, SQL injections, cross-site scripting, and buffer overflows.

REPUTATION ENABLED DEFENSE SERVICE (RED)

A powerful, cloud-based reputation lookup service that protects web users from malicious sites and botnets, while dramatically improving web processing overhead.



WEBBLOCKER URL FILTERING

In addition to automatically blocking known malicious sites, WebBlocker's granular content and URL filtering tools enable you to block inappropriate content, conserve network bandwidth, and increase employee productivity.

SPAMBLOCKER

Real-time spam detection for protection from outbreaks. Our spamBlocker is so fast and effective, it can review up to 4 billion messages per day.

GATEWAY ANTIVIRUS (GAV)

Leverage our continuously updated signatures to identify and block known spyware, viruses, trojans, worms, rogueware and blended threats – including new variants of known viruses. At the same time, heuristic analysis tracks down suspicious data constructions and actions to make sure unknown viruses don't slip by.

APPLICATION CONTROL

Selectively allow, block, or restrict access to applications based on a user's department, job function, and time of day and to then see, in real-time, what's being accessed on your network and by whom.

ADVANCED SECURITY SERVICES

APT BLOCKER – ADVANCED MALWARE PROTECTION

APT Blocker uses an award-winning next-gen sandbox to detect and stop the most sophisticated attacks including ransomware, zero day threats and other advanced malware.

DATA LOSS PREVENTION (DLP)

This service prevents accidental or malicious data loss by scanning text and common file types to detect sensitive information attempting to leave the network.

NETWORK VISIBILITY & MANAGEMENT SERVICES

NETWORK DISCOVERY

A subscription-based service for Firebox appliances that generates a visual map of all nodes on your network so you can easily see where you may be at risk.

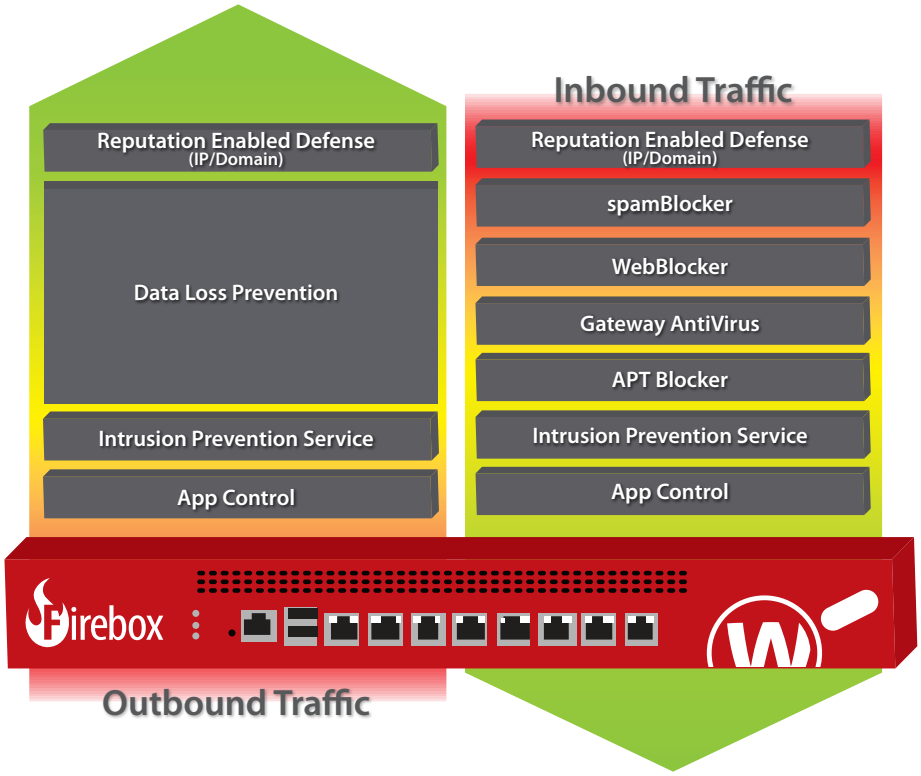
DIMENSION COMMAND

Dimension translates data collected from all appliances across your network into actionable network and threat intelligence. Dimension Command gives you the power to take action to mitigate those threats instantly, from one central console.

A Unified Approach to Network Security

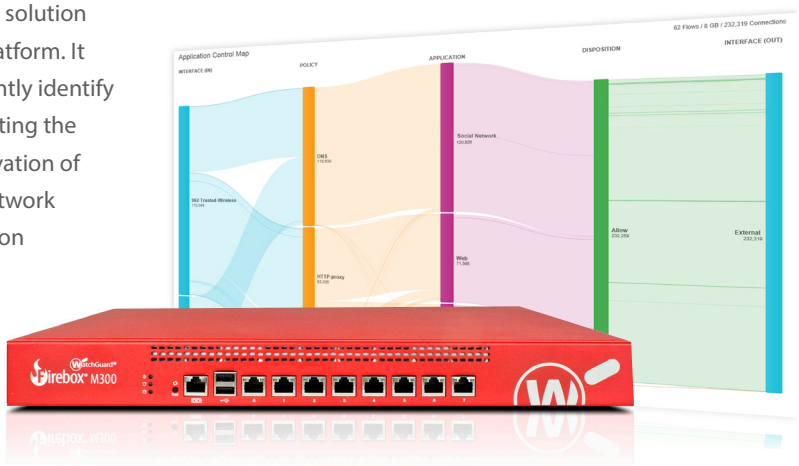
Network security is an arms race and no single security control, or subset of controls, is sufficient. The more stages of an attack you protect against, the more effective your overall defense is, even when new threats bypass one defense.

For example, an attack might begin with a phishing email that triggers a malware download. With WatchGuard's UTM protecting your network, should the initial email slip past spam protection, WatchGuard's award-winning APT Blocker will step in to analyze any suspicious code to block the threat. APT Blocker is freed from spending valuable processing time analyzing all traffic because Gateway AntiVirus, WebBlocker, Intrusion Prevention Service and Reputation Enabled Defense routinely stop most threats at the perimeter of the network. When security defenses work in tandem like this, you have the strongest protection, maximum efficiency, and lightning fast performance.



The Power of Visibility

WatchGuard Dimension is a cloud-ready network security visibility solution that comes standard with every WatchGuard's network security platform. It provides a suite of big data visibility and reporting tools that instantly identify and distill key network security threats, issues and trends, accelerating the ability to set meaningful security policies across the network. Activation of the Dimension Command feature unlocks access to a variety of network control features including, but not limited to, one-click configuration changes, the ability to jump back to previous configurations, direct access to individual appliances through a web UI, and VPN management tools. Knowledge is power and visibility provides knowledge.



> The main benefits for us have been moving from a basic stateful firewall to a full Layer 7 scanning platform. We managed to add IPS/IDS, application filtering, malware detection, Gateway AV, web filtering and all the other security features WatchGuard offers. In this one unit we have managed to combine a lot of security features, which as separate units would not make financial sense.

~ Peter Thomas
IT Manager, Roland UK

One Appliance, One Package, Total Security

Simplicity is our mission at WatchGuard and that mission extends beyond how the product is built to how it is packaged. While all of our services are offered à la carte, we have worked to develop two packages that simplify the decision-making process. The Total and Basic Security Suite packages are only available on our Firebox T and M Series appliances. Similar packages can be custom-created by our Partners for XTM and XTMv customers, however, we are always running promotions to encourage our customers to trade-up to the latest hardware to enjoy the fastest performance and strongest security.

- The **Basic Security Suite** includes all of the traditional network security services typical to a UTM appliance: IPS, GAV, URL filtering, application control, spam blocking and reputation lookup. It also includes our centralized management and network visibility capabilities, as well as, our standard 24x7 support.
- The **Total Security Suite** includes all services offered with the Basic Security Suite plus advanced malware protection, data loss protection, enhanced network visibility capabilities, and the ability to take action against threats right from Dimension, our network visibility platform. It also includes upgraded Gold level 24x7 support.

Services	TOTAL SECURITY	Basic Security
Intrusion Prevention Service (IPS)	✓	✓
Application Control	✓	✓
WebBlocker (URL/Content Filtering)	✓	✓
spamBlocker (Anti-Spam)	✓	✓
Gateway AntiVirus (GAV)	✓	✓
Reputation Enabled Defense (RED)	✓	✓
Network Discovery	✓	✓
APT Blocker	✓	
Data Loss Prevention	✓	
Dimension Command	✓	
Support	**Gold (24x7)**	Standard (24x7)

Getting Started

WatchGuard has the industry's largest network of value-added resellers and service providers. To get started, visit our website to find the best Partner for your business, or opt to contact us directly and we will answer any questions you may have and get you set up with the perfect Partner for your requirements.

- Browse our Partner network: **findpartner.watchguard.com**
- Speak with a WatchGuard security specialist: **www.watchguard.com/wgrd-sales/emailus**
- More information on How to Buy: **www.watchguard.com/totalsecurity**

About WatchGuard

WatchGuard has deployed nearly a million integrated, multi-function threat management appliances worldwide. Our signature red boxes are architected to be the industry's smartest, fastest, and meanest security devices with every scanning engine running at full throttle. Headquartered in Seattle, WA, WatchGuard has offices throughout North America, Europe, Asia Pacific, and Latin America.
Visit **www.watchguard.com** for details, and check out our InfoSec blog, **Secplicity**, for real-time information about the latest threats and how to cope with them – in an easily understood and actionable way. Go to: **www.watchguard.com/secplicity**.

WatchGuard® Network Security Products at a glance

	Firebox T10/T10-W/T10-D[x]	Firebox T30/T30-W	Firebox T50/T50-W	Firebox T70	Firebox M200	Firebox M300	Firebox M400	Firebox M440	Firebox M500	Firebox M4600 base + 4 x 10 Gb ports	Firebox M5600 base + 4 x 10 Gb ports
Throughput and Connections											
Firewall throughput	400 Mbps	620 Mbps	1.2 Gbps	4 Gbps	3.2 Gbps	4.0 Gbps	8 Gbps	6.7 Gbps	8 Gbps	40 Gbps	60 Gbps
VPN throughput	100 Mbps	150 Mbps	270 Mbps	740 Mbps	1.2 Gbps	2.0 Gbps	4.4 Gbps	3.2 Gbps	5.3 Gbps	10 Gbps	10 Gbps
AV throughput	120 Mbps	180 Mbps	235 Mbps	1.2 Gbps	620 Mbps	1.2 Gbps	2.5 Gbps	2.2 Gbps	3.2 Gbps	9 Gbps	12 Gbps
IPS throughput	160 Mbps	240 Mbps	410 Mbps	1.5 Gbps	1.4 Gbps	2.5 Gbps	4 Gbps	2.2 Gbps	5.5 Gbps	13 Gbps	18 Gbps
UTM throughput	90 Mbps	135 Mbps	165 Mbps	1.1 Gbps	515 Mbps	800 Mbps	1.4 Gbps	1.6 Gbps	1.7 Gbps	8 Gbps	11 Gbps
Interfaces	3 x 1Gb	5[iii] x 1 Gb	7[iii] x 1 Gb	8 x 1 Gb	8 x 1 Gb	8 x 1 Gb	8 (incl. 2 SFP)[vi]	25 1G copper[iv] 2 10G SFP+	8 (incl. 2 SFP)[vi]	8 x 1 Gb additional ports available*	8 x 1 Gb + 4 x 10 Gb fiber additional ports available
I/O Interfaces	1 Serial / 1 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 SRL/2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB
Concurrent connections	50,000	200,000	300,000	800,000	1,700,000	3,300,000	3,800,000	4,000,000	9,200,000	7,500,000	12,700,000
New connections per second	2,300	3,400	4,600	27,000	20,000	48,000	84,000	62,000	95,000	160,000	240,000
VLAN support	10	50	75	75	100	200	300	400	500	1,000	Unrestricted
Authenticated users limit	200	500	500	500	500	500	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted
VPN Tunnels											
Branch Office VPN	5	40	50	50	50	75	100	300	500	5,000	Unrestricted
Mobile VPN IPSec	5	25	50	60	75	100	150	300	500	10,000	Unrestricted
Mobile VPN SSL / L2TP	5	25	50	60	75	100	150	300	500	10,000	Unrestricted
Wireless											
Wireless Access Points (APs)	WatchGuard offers a family of AP devices that allow all Firebox security capabilities to be extended to the WLAN. APs can be managed in the cloud or through the Firebox's built-in wireless controller.										
Max APs advised per model	4	20	40	50	60	80	100	100	150	200	300
Integrated Wireless	Integrated 802.11a/b/g/n available for Firebox T10-W. Integrated 802.11a/b/g/n/ac is available for Firebox T30-W and T50-W										
Operating System Features											
General	Integrated 802.11a/b/g/n available for Firebox T10-W. Integrated 802.11a/b/g/n/ac is available for Firebox T30-W and T50-W										
Advanced Networking	Dynamic routing (BGP, OSPF, RIPv1,2) / Policy-based routing / NAT: static, dynamic, 1:1, IPSec traversal, policy-based PAT / Traffic shaping & QoS: 8 priority queues, DiffServ, modified strict queuing / Virtual IP for server load balancing										
Availability	High availability – active/passive, and active/active for clustering (not available on wireless models) / VPN failover / Multi-WAN failover / Multi-WAN load balancing / Link aggregation (802.3ad dynamic, static, active/backup) as indoors										
Security Services											
Basic Security Suite	Application Control / Intrusion Prevention Service / WebBlocker / Gateway AntiVirus / Reputation Enabled Defense / Network Discovery / spamBlocker / Standard Support (24 x 7)										
Total Security Suite	Application Control / Intrusion Prevention Service / WebBlocker / Gateway AntiVirus / Reputation Enabled Defense / Network Discovery / spamBlocker / Data Loss Prevention / APT Blocker / Dimension Command / Gold Support (24 x 7, plus escalated response time)										
Management Upgrades	Dimension Command is a suite of management tools for WatchGuard Dimension that allows administrators to manage policies directly from Dimension's visibility dashboards, create VPNs, roll back configurations, and more (Included in Total Security Suite)										

*Firebox M4600 and M5600 throughput rates are determined using base configuration + 4 x 10 Gb ports. Both models ship with two empty bays that can accommodate any combination of the following: 4 x 10 Gb fiber, 8 x 1 Gb fiber, 8 x 1 Gb copper, 2 x 40 Gb fiber.

Throughput rates are determined using multiple flows through multiple ports and will vary depending on environment and configuration. Max firewall throughput tested using 1518 byte UDP packets based on RFC 2544 methodology. Contact your WatchGuard reseller or call WatchGuard directly (1.800.734.9905) for help determining the right model for your network. Visit **www.watchguard.com/sizingtool** for online assistance.

Every WatchGuard appliance includes these features:

Security Capabilities

- Stateful packet firewall, deep application inspection, application proxies: HTTP, HTTPS, SMTP, TCP-UDP, FTP, DNS
- Blocks spyware, DoS attacks, fragmented packets, malformed packets, blended threats and more
- Protocol anomaly detection, behavior analysis, pattern matching
- Static and dynamic blocked sources list
- VoIP: H.323 and SIP, call setup and session security

Logging & Reporting with WatchGuard Dimension™

- Real-time multi-appliance log aggregation and reporting
- Public & private cloud-ready
- Visibility at a glance with intuitive and interactive visualizations
- Spot trends, outliers and insights about network traffic and usage
- Over 100 reports including reports for PCI and HIPAA compliance
- Option to deliver reports (PDF, CSV) via email
- Anonymization to comply with privacy directives

Management Software

WatchGuard appliances can be managed with any of the following:

- Dimension Command for interactive real-time management of multiple appliances via web browser
- Web UI for managing single appliance via web browser
- WatchGuard System Manager for intuitive management of appliances via Windows client
- Command line interface (CLI) for direct access via scripting
- Simplified configuration and deployment with RapidDeploy

User Authentication

- Transparent Active Directory Authentication (single sign-on)
- RADIUS, LDAP, Secure LDAP, Windows Active Directory
- RSA SecurID® and VASCO
- Local database
- 802.1X for wireless appliances (Firebox T10-W, T30-W, T50-W)
- Microsoft® Terminal Services and Citrix XenApp environments supported

Support and Maintenance Options

- Standard Support, included in the Basic Security Suite, includes hardware warranty, 24 x 7 technical support, and software updates
- An upgrade to Gold Support, included in the Total Security Suite, delivers all the benefits of Standard Support, plus escalated response times
- For more information on WatchGuard's Support levels and additional service options, visit www.watchguard.com/support

[x]Not available in all geographic locations. Contact your WatchGuard reseller for more information. [iii]Power Over Ethernet (PoE) options: Firebox T30 & T50 have 1 PoE port. Firebox M440 has PoE on 8 of 25 IG ports. [iv]Comes with 6 built-in 10/100/1000 copper ports, two SFP transceiver slots. Optional 1Gb fiber or 1Gb copper transceivers can be used in either slot. [vi] Some advanced networking features, including server load balancing, high availability, and dynamic routing are not available on Firebox T10 appliances. Visit www.watchguard.com/T10 for details.