5. Inspect HTTPS traffic—while safeguarding privacy:
An increasing proportion of Internet traffic runs over encrypted HTTPS channels. Though the "S" on the end of HTTPS stands for "secure," the encryption of these transactions renders the traffic invisible to traditional firewalls. Full inbound and outbound HTTPS inspection in WatchGuard XTM closes the loophole that other security products leave wide open. URL filtering, AV scanning, and a host of other security functions carried out on HTTPS traffic, identify and stop threats before they can affect your business. Additionally, the data is not exposed to human eyes, so the risk of an intentional or unintentional privacy violation is eliminated.

6. Make Voice over IP Simple and Safe For Your Business:
Voice over IP (VoIP) is an extremely useful tool in business today for decreasing telecommunication costs and increasing productivity. However, it carries inherent risks, because the VoIP protocols are complex and varied in their implementations. WatchGuard XTM provides application-layer VoIP security, allowing businesses to take advantage of VoIP while minimizing exposure and risk to critical systems and data. With the XTM Series, organizations don't have to "wire around the firewall" to take advantage of the huge cost savings and communication capabilities VoIP offers.

7. Making the Most of the Network:
As Internet use has increased, so have temptations, distractions, and security risks online. Organizations require more than a simple "allow/deny" security policy. WatchGuard XTM includes a rich set of tools for maximizing the business value of every dollar spent on Internet connectivity. Traffic Shaping and QoS tools allow organizations to define which types of traffic are most important, and which types are less important or prohibited, ensuring that business traffic always wins out over recreational or discretionary traffic. VPN failover, WAN failover, and High Availability features ensure that mission-critical data keeps flowing, even in the event of failure or degradation of equipment or connectivity.

8. Best-In-Class Security:
Attackers and malware constantly advance, making use of an extensive worldwide underground market for crimeware. To defend against these threats, WatchGuard XTM also works globally, combining advanced capabilities from the world's best suppliers of security technology to complement WatchGuard's award-winning foundation. This "all-star lineup" outpaces firewalls from other vendors who rely only on in-house technology rather than acknowledged best-in-class capabilities for specialized functions. At the same time, the deep integration of these functions and an intuitive user interface streamline the creation and monitoring of the holistic security policy, giving customers best-in-class security while eliminating the complexity and cost of managing disparate point solutions.

9. Connect Your People Securely:
Virtual Private Networking (VPN) is ultimately about securely connecting people to the resources they need. Businesses today have distributed workforces and need to provide privacy over public lines. By deploying VPNs businesses can deliver secure, encrypted connectivity for traveling employees, remote offices and telecommuters that require access to critical corporate network resources. WatchGuard XTM provides a multitude of ways to easily and securely create and manage these connections. The unique "drag and drop VPN" enables an organization to connect offices almost instantly, without error, even when dynamic IP addresses are in use. Mobile VPN enables road warriors, virtual employees, collaborators, and any other authorized person to connect to corporate resources from anywhere, at any time, from a variety of devices including laptops, smartphones, and the popular Apple® iOS devices. You can rest assured that with VPN support your critical corporate network resources are protected.

10. User Friendly:
WatchGuard recognizes that many small businesses do not have a dedicated IT security staff. With this recognition comes a dedication to creating interfaces that take the hard work and guess work out of business security. Task flows are designed for maximum efficiency, and interfaces use plain language that enables even security novices to create, monitor, and audit strong security and acceptable use policies.

U.S. Sales: 1.800.734.9905 • International Sales: 1.206.613.0895 • Web: www.watchguard.com

The WatchGuard® XTM Story

Since 1996, WatchGuard Technologies has provided over one-half million network security appliances to hundreds of thousands of customers worldwide. While the technologies, performance, and individual features of those products have evolved and grown tremendously over that time, the underlying WatchGuard philosophy has remained the same: to deliver strong security that is easy to manage and monitor, at an excellent price. WatchGuard's XTM and XTMv family of all-in-one solutions delivers enterprise-grade network protection for small to midsize businesses, keeping your network secure, employee productivity high, and turning the Internet from a security risk to a business empowerment tool.

1. Complete Security Capabilities Now & into the Future:
WatchGuard XTM enables organizations to define, enforce, and audit a strong security and acceptable use policy, with a range of capabilities unmatched in its class. With WatchGuard XTM, organizations can:

- **Defend Resources** with powerful firewall, anti-malware, and intrusion prevention.
- **Connect Offices Securely** and allow road warriors and virtual employees to access corporate resources from anywhere, anytime, with nearly any device.
- **Extend the XTM's best-in-class security to the WLAN** by adding wireless access points. The AP100 and AP200 let you harness the power of mobile devices without putting network assets at risk.
- **Enforce Acceptable Use** with WebBlocker, spamBlocker, Application Control, and Reputation Enabled Defense – tools that safeguard employee Internet use while providing IT with deep visibility into usage patterns.

2. Stay Secure on a Tight Budget:
XTM appliances deliver the best price-performance in the industry, ensuring that you can get rock-solid security as well as the performance your business needs to proceed unimpeded. What's more, with XTM's unique model upgradability, you can choose the appliance that fits your needs today, with the ability to upgrade to a higher model within the series via a simple license key. An assortment of upgrade packages makes it easy to custom-tailor the solution to the organization's exact needs.

3. Know What is Happening On Your Company's Network:
"*Visibility IS security*" – and great visibility is one of the most important ways to ensure compliance with policies. The XTM Series and WatchGuard System Manager (WSM) enable a business to gain deep real-time and historical insights into the network and user events and activities. Interactive real-time monitoring features help pinpoint significant activities as they happen, and let the administrator take immediate corrective or diagnostic actions directly from the monitoring interface. WSM's centralized logging features unique TCP-based, encrypted log channels for maximum reliability and security, while Report Manager includes over 60 predefined reports, with an intuitive user interface that uses plain language, easy-to-read graphics, and drill-down and pivot controls.

4. Centrally Manage Your Organization's Security:
Distributed organizations and Managed Security Services Providers (MSSPs) need the ability to manage large numbers of appliances from a single location, with simplicity and scalability. WatchGuard System Manager, bundled with every XTM appliance, is rich in tools that support policy creation, management, and enforcement across multiple locations. Role-Based Access Control supports the delegation of duties according to function within the organization, and every function can be centrally managed – including firewall, VPN, intrusion prevention, URL filtering, web security, anti-virus and anti-spam services, appliance software updates and more. And, beyond the centralized management capabilities in WSM, WatchGuard XTM solutions may be managed via a Web UI or a Command Line Interface (CLI) for ultimate flexibility.

WatchGuard® XTM Products at a glance

	XTM 2 Series[a]		XTM 3 Series		XTM 5 Series				XTM 800 Series			XTM 1500 Series[b]		XTM 2520
	25/25-W upgradeable to XTM 26	**26/26-W** –	**33/33-W** –	**330** –	**515** upgradable to XTM 525	**525** –	**535** upgradable to XTM 545	**545** –	**850** upgradable to 860/870	**860** upgradable to 870	**870** –	**1520/1520-RP** –	**1525/1525-RP** –	**2520** –
Throughput and Connections														
Firewall throughput	240 Mbps	540 Mbps	850 Mbps	1.4 Gbps	2 Gbps	2.5 Gbps	3 Gbps	3.5 Gbps	8 Gbps	11 Gbps	14 Gbps	14 Gbps	25 Gbps	35 Gbps
VPN throughput	40 Mbps	60 Mbps	100 Mbps	240 Mbps	250 Mbps	350 Mbps	550 Mbps	750 Mbps	8 Gbps	8 Gbps	10 Gbps	10 Gbps	10 Gbps	10 Gbps
AV throughput	75 Mbps	142 Mbps	175 Mbps	340 Mbps	1.5 Gbps	1.7 Gbps	1.8 Gbps	2 Gbps	4 Gbps	5.5 Gbps	7 Gbps	8 Gbps	9 Gbps	9.7 Gbps
IPS throughput	100 Mbps	226 Mbps	328 Mbps	640 Mbps	1.6 Gbps	2 Gbps	2.4 Gbps	2.8 Gbps	5 Gbps	7 Gbps	9 Gbps	11 Gbps	13 Gbps	15 Gbps
UTM throughput	55 Mbps	108 Mbps	146 Mbps	298 Mbps	850 Mbps	1 Gbps	1.4 Gbps	1.7 Gbps	3 Gbps	4 Gbps	5.7 Gbps	6.7 Gbps	6.7 Gbps	up to 10 Gbps
Interfaces 10/100/1000	5	5	5	7	6[c]	6[c]	6[c]	6[c]	14	14	14[d]	14	6 and four 10G SFP+[e]	12 and four 10G SFP+[e]
I/O Interfaces	1 Serial / 1 USB	1 Serial / 1 USB	1 Serial / 1 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	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB	1 Serial / 2 USB
Nodes supported (LAN IPs)	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted
Concurrent connections (bi-directional)	10,000	30,000	40,000	40,000	40,000	50,000	100,000	350,000	1,000,000	1,250,000	1,500,000	2,000,000	2,000,000	2,500,000
VLAN support	20/50*** (incl/max)	20/50*** (incl/max)	75	75	100	200	300	400	750	750	1,000	2,000	3,000	4,000
Authenticated users limit	500	500	500	500	500	500	1,000	2,500	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unrestricted
VPN Tunnels														
Branch Office VPN	10	40	50	50	65	75	200	600	5,000	6,000	7,000	10,000	10,000	Unrestricted
Mobile VPN IPSec (incl/max)	5/10	5/40	5/55	5/55	75/75	100/100	300/300	1,000/1,000	10,000	12,000	14,000	15,000/15,000	20,000/20,000	Unrestricted
Mobile VPN SSL / L2TP	1/11 (incl/max)	1/25 (incl/max)	55	55	65	75	300	600	10,000	12,000	14,000	15,000	20,000	Unrestricted
Networking Features														
General	IP address assignment: static, DynDNS, PPPoE, DHCP (server, client, relay) / Port independence / VLAN support / Transparent/drop-in mode													
Routing	Dynamic routing (BGP, OSPF, RIPv1,2) / Policy-based routing / Virtual IP for server load balancing[f] / 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[f]													
Availability	High availability (active/passive, and active/active for clustering) / VPN failover / Multi-WAN failover / Multi-WAN load balancing / Link aggregation (802.3ad dynamic, static, active/backup) / Wireless WAN failover available with WatchGuard Broadband wireless bridge accessory													
Wireless														
Integrated Wireless	Integrated 802.11a/b/g/n available in model numbers ending in "-W"													
Wireless Access Points	All models†† support AP100 and AP200 wireless access points to extend XTM security capabilities to the WLAN / Includes MAC filtering, client reporting, Captive Portal technology, 802.1X authentication, and PCI compliant scan and reporting													
Wireless WAN	All models support WatchGuard Broadband Extend wireless bridge devices for cellular connectivity / Some direct connect USBs are supported													
Subscriptions														
Security Services	Data Loss Prevention / Application Control / Intrusion Prevention Service / WebBlocker / Gateway AntiVirus / spamBlocker / Reputation Enabled Defense													
LiveSecurity® Service	Multi-year LiveSecurity subscriptions are available for all models / LiveSecurity Plus with 24/7 support and Gold-level service are available as purchase options for XTM models 330 and higher													

Throughput rates are determined using multiple flows through multiple ports and will vary depending on environment and configuration. Contact your WatchGuard reseller or call WatchGuard directly (1.800.734.9905) for help determining the right model for your network.

Every XTM appliance includes these features:

Security Capabilities

- Stateful packet firewall, deep application inspection, application proxies: HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3
- 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

Management Software

WatchGuard XTM appliances can be managed with:

- Command line interface with direct connects and scripting
- Web UI for single device management from anywhere
- WatchGuard System Manager: intuitive, centralized console providing interactive real-time monitoring and logging; includes drag-and-drop VPN creation, rich historical reporting
- Simplified deployment with RemoteDeploy & RemoteConfig

User Authentication

- Transparent Active Directory Authentication (single sign-on)
- XAUTH for RADIUS, LDAP, Secure LDAP, Windows Active Directory
- RSA SecurID® and VASCO
- Local database
- 802.1X for wireless appliances (XTM 25-W, 26-W, 33-W)
- Microsoft® Terminal Services and Citrix XenApp environments supported

LiveSecurity Service Upgrade Options

- Remote Installation Services for comprehensive assistance with the initial setup, configuration, VPN installation
- Premium 4-Hour Hardware Replacement to ensure maximum uptime
- LiveSecurity Platinum for complex environments. Includes assigned Technical Support Manager to help you achieve your strategic goals with WatchGuard products

Logging and Reporting

- Multi-appliance log aggregation
- HTML and PDF reports
- Encrypted, TCP-based log channel
- SNMP v2 & v3
- Logging and reporting with server health status
- Syslog interface also supported
- Logging and reporting with server health status
- Web-based configurable reports portal

[a]XTM 2 Series can be upgraded to Pro version of Fireware OS for maximum SSL tunnels and high availability. [b]XTM 1520-RP and 1525-RP models include redundant hot-swappable power supplies. [c]XTM 5 Series models include one 10/100 interface. [d]XTM 870 appliances come with 6 copper and 8 fiber 10/100/1000 interfaces under model number WatchGuard XTM 870-F. [e]Fiber ports can operate as 10GBase-SR/SW or 1000Base-SX. [f]Server load balancing is not available on XTM 2 Series and 3 Series appliances.