WHITEPAPER

Defeating Ransomware with Unified Security from WatchGuard

Table of Contents

INTRODUCTION

Perhaps the most lucrative method of cyber crime encountered to date, the emergence of ransomware marks a distinct shift in how cyber criminals derive value from their victim's data. With ransomware, attackers no longer need to focus on stealing data they can easily resell, but rather exploit the importance of that data to the victim. Even though the data may not be sensitive in its content, it may be business-critical for the target. By holding the data hostage and demanding a ransom for its return, attackers are able to monetize data for which they may have had no other use.

This paradigm shift places a host of organizations, many of whom have long felt themselves too small to be an appealing target for cyber attacks, firmly in the crosshairs of cyber criminals.

WHAT IS RANSOMWARE?

Ransomware is a type of advanced malware attack that takes hold of a device, either locking the user out entirely or encrypting files so they cannot be used. This type of attack can gain access to your device in a variety of ways, whether downloaded from a malicious or compromised website, delivered as an attachment from a phishing email, or dropped by exploit kits onto vulnerable systems. When a piece of ransomware lands on your computer and is executed, it starts restricting access to important parts of your computer. Early on it would simply encrypt documents on your system, restricting access to the data you need to do your job.

Eventually, newer types of ransomware restricted access to the computer itself, either by blocking access to your desktop or rebooting your computer into a locked state. Lately, some more recent pieces of ransomware will copy your important data from your computer. In all cases the attacker eventually makes themselves known with an "official" ransom demand, as well as thorough instructions and timelines on how to make a payment to either regain access to the device or to receive the decryption key for the captive files.

In 2018 the avg. ransom demand was $41,000.

In 2019, that figure more than doubled.

THE GROWING COST OF RANSOMWARE

It goes without saying that ransomware attacks can be extremely lucrative for our adversaries, but recent attacks have made the profitability of such attacks obscene. In 2018 the average ransom demand was $41,000. In 2019, that figure more than doubled to $84,000, driven in part by the convergence and cooperation of formerly competitive cyber-criminal gangs.[1]

In 2016, the FBI predicted that ransomware would be $1 billion source of income for cyber criminals. Today, estimates suggest the market will reach 20 times that by the end of 2021.[2]

Estimates suggest ransomware source of income will reach 20 times more than 2016.

Unfortunately, the total cost of a ransomware attack often makes the ransom demand seem of little consequence. The true cost of a ransomware attack must consider all of the damages done to IT assets, time and money spent recovering data, and losses to customer/employee confidence. Over one third of ransomware victims report a loss of revenue, while 20% have had to stop operations completely in the aftermath of a successful ransomware attack.[3] Further, research suggests the average cost of downtime for a SMB in 2019 was $141,000, up 200% year over year.[4] Few small businesses could withstand such an attack.

Average cost of downtime for SMB in 2019 was $141,000, up 200% year over year.

RANSOMWARE CHANGES THE DATA VALUE PARADIGM

Security professionals have long talked about the need to protect sensitive data as the threat of identity theft and fraud made prioritizing the security of specific types of data essential. While protecting sensitive data is by no means trivial, organizations are able to rely on a fairly straightforward formula for data protection; identify sensitive data, build protections around where that data is stored and used, and where possible keep the data encrypted.

The protection of sensitive data largely requires that you focus on the data that your attacker will find most valuable, which typically corresponds to the data that an attacker will be able to sell or use for financial gain most easily. Today, this data is highly regulated and for many organizations, its handling requires strict adherence to national and international compliance initiatives.

The emergence of ransomware marks a distinct shift in the data value formula as attackers no longer need to focus on the market value of the data they collect, but rather derive value based on the importance of that data to you or your business. Even though the data may not be sensitive in its content, it may be business-critical for your organization in the short and long term. By holding your data hostage and demanding a ransom for its return, attackers are able to monetize data for which they may have had no other use.

This paradigm shift places a host of new organizations, many of whom have long felt themselves too small to be an appealing target for cyber attacks, firmly in the crosshairs of an increasingly sophisticated onslaught of attackers.

THE RISE OF 2nd WAVE RANSOMWARE

In the first wave of ransomware (2016-2017), the model was to ask for a small ransom, sometimes as low as $100, while infecting as many people as possible. Starting in 2019, ransomware's second wave shifted in operating model. Instead of widespread infection, newer campaigns started targeting specific companies. Attackers worked for weeks or months to get access to a specific company and would deploy the ransomware on many internal computers once they got access.

The ransoms for these attacks grew to thousands of dollars. The increase in ransom becomes viable because the ransomware scare has increased the demand for cyber insurance. If a ransomware event happens to a victim with cyber insurance, the insurance company will assist in recuperating the ransom paid. This means the company is more likely to pay the ransom.

Ransomware for Sale! Black Market for Ransomware Tools Minimizes the Barrier to Entry

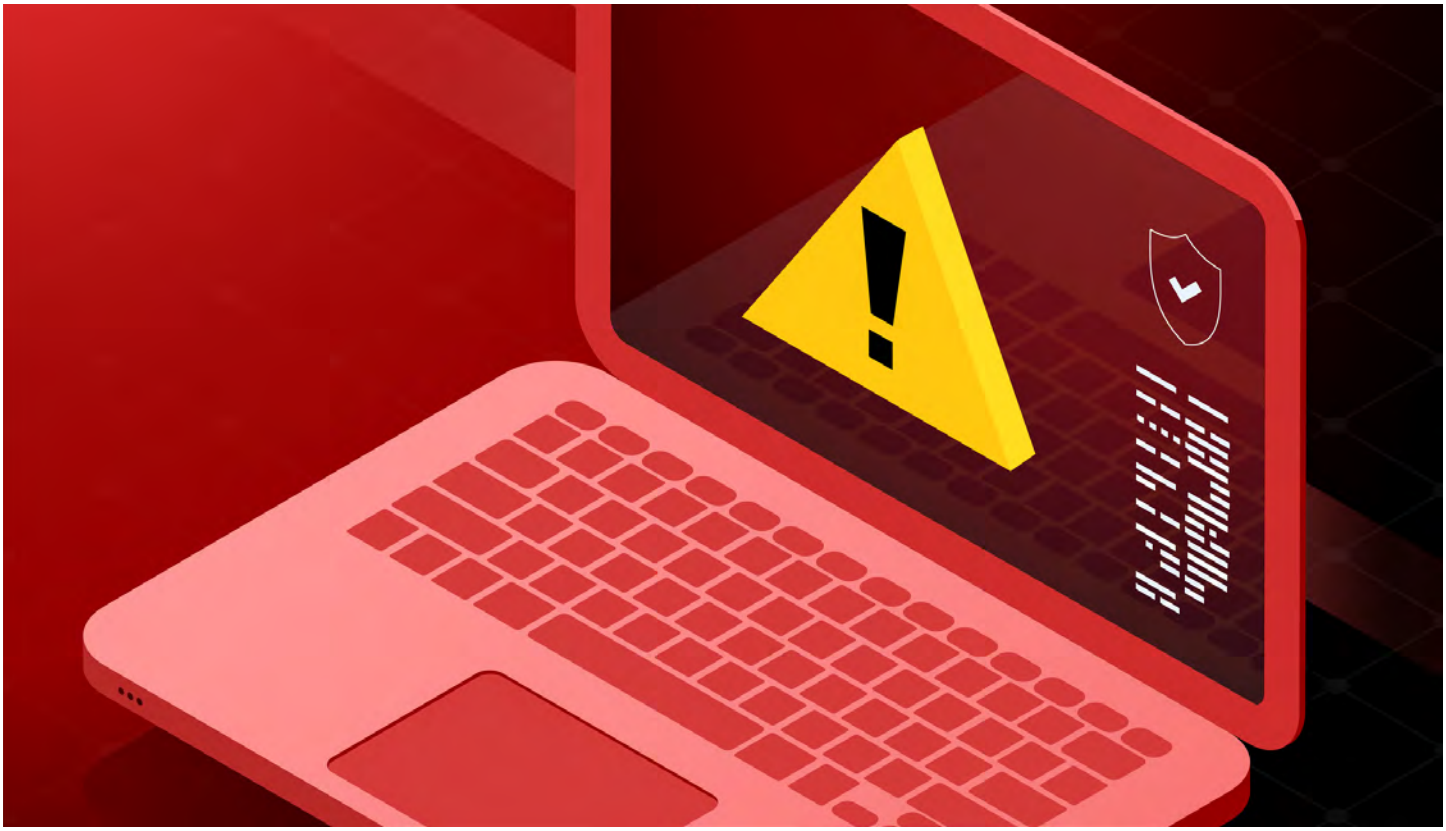
The continued prevalence of the ransomware threat can be attributed in part to the availability of ransomware tools and services offered on the deep web. These tools drive down the level of sophistication required to perpetrate a ransomware attack, enabling would-be attackers with limited computer skills to pull off significant ransomware campaigns.

The emergence of ransomware-as-a-service offerings marks another troubling trend in the war against ransomware. Full-service shops now offer everything from malware samples and the hosting infrastructure, to call centers that help victims pay the ransom, all for a percentage of the ransom received. With all of these tools mere clicks away from our would-be attackers, it should come as no surprise that SMBs are increasingly falling victim to the wave of ransomware attacks.

Ransomware Spotlight - Maze

In January 2020, the Maze ransomware campaign made a major escalation in how ransomware operates. In addition to restricting access to the computer and/or documents, this ransomware transmitted some of that data off the computer to some sort of command and control (c2) system. This bridges ransomware into the other major business model of cyber crime, selling stolen data. Until 2016 the major source of revenue for cyber criminals was to sell the data they stole to anyone willing to pay. Put it all together and attackers can now turn hacked access to a company into two separate revenue streams.

What's even more worrisome about these new ransomware campaigns is that victims now must assume the ransomware can and will transmit their confidential data over the internet. These incidents suddenly fall into the realm of mandatory data loss laws in California and Europe. The burden suddenly doubles on the victim, since they were ultimately responsible with safely storing personal data.



USERS ARE THE KEY BATTLEGROUND

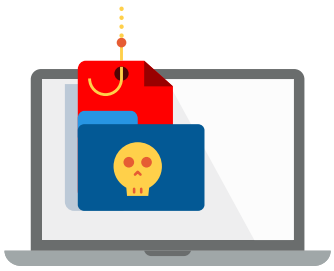
Today, cyber criminals are increasingly exploiting the naivety of users as the initial attack vector, taking advantage of their lack of cybersecurity literacy. Employees represent the front line in preventing a ransomware disaster. All it takes is one wrong click on a link or a file to set the wheels of a ransomware infection in motion. From using scare tactics like impersonating federal agencies or the police, to delivering malware via emails carefully crafted to target a specific person, attackers are well versed in techniques that increase the likelihood of a click. In fact, 90% of cyber attacks today begin with a successful phishing attempt that tricks one of your users to clicking a link or downloading a file that delivers malware or grants the attacker unintended access.

Common Ransomware Attack Vectors

Threat actors use three main vectors to get initial access in ransomware campaigns:

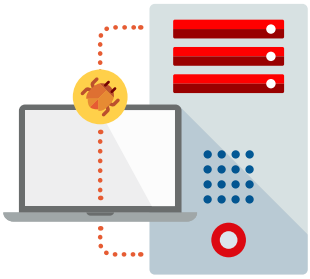
- Phishing a user
- RDP abuse
- Scan & exploit techniques

Phishing



According to Gartner, by 2025, 85% of successful attacks will leverage the human factor, rather than use advanced malware. Compared to technology, the human factor will be by far the slowest one to evolve, and the most stable. 83% of businesses have fallen victim to a phishing attack, and with more employees working remotely than ever before, phishing attacks are on the rise. Email is the preferred delivery method for such attacks, although there are others, like text messages and chat applications. Spear phishing, as well as whaling, targeting CIOs and C-Level employees in organizations, which typically requires impersonating an internal user's email address (business email compromise), are also increasing in frequency. According to the FBI, BEC accounted for more than $26 billion in losses from 2016 through 2019.

RDP Abuse



The COVID-19 pandemic resulted in more than 1.5 million new Remote Desktop Protocol (RDP) servers being exposed to the Internet to get employees connected quickly, with little regard for security. Credential stuffing and brute force attacks against RDP services exposed to the Internet, virtual private network (VPN) services, and user accounts are common. Typically using an attack technique of systematic guessing, lists of passwords, or dumped credentials from previous breaches, the attacker seeks to forcibly authenticate to a device or service.

Scan-and-Exploit Techniques

These types of tactics take advantage of the fact that many organizations still do not have adequate vulnerability and patch management capabilities yet. This is the low-hanging fruit for the attackers.

In fact, just a small number of vulnerabilities, in some cases years old, are behind a large proportion of ransomware attacks. So, investing in efficient measures to assess and patch those remote systems, even if they are not connected to the VPN, is key. According to a 2020 study from cybersecurity company SenseCy, there are only four vulnerabilities that are being abused in a large proportion of the 180 incidents they studied.

DETECTING RANSOMWARE PAYLOADS

Until recently, antivirus (AV) products were the primary way to prevent malware, like ransomware, from entering your network or infecting your computers. Antivirus solutions depend on human researchers to find new malware variants and uncover distinct patterns in the malicious files that uniquely identify them. Using these patterns – signatures, if you will – these solutions are able to recognize and block previously discovered malware before it enters your network, or infects your computers.

For a long time, these signature-based solutions seemed sufficient, and helped prevent the majority of malware. However, legacy AV solutions have an Achilles' heel in that these pattern-based solutions are always reactive, not proactive. A human or automated system must already have found and analyzed a new malware sample before it can create the signatures to block it. In short, it can't identify brand new malware samples when they're first released.

To exploit this issue, attackers have evolved their malware specifically to evade signature-based AV solutions. They've designed malware that loads in stages using dropper files, malware that tries to disable security programs including AV, and malware files that are encoded in different ways to sneak past the latest signatures.

In response, AV products have also evolved, using more complex signature rules to catch a wider range of samples (called a malware family) and designing basic heuristic solutions to try to identify new malware based on its file attributes. Unfortunately, criminals have increasingly adopted one very effective evasion technique, which has changed the game, and allowed many new malware samples to get past legacy solutions. That technique is *polymorphism*.

Polymorphic malware is a fancy term for malware that constantly changes the way it looks to evade signature-based detection. Using methods the criminals call "packing and crypting," attackers can repeatedly change a malware file on a binary level, making it look different to AV software. Even though the malicious executable still does the exact same thing, it looks like a new file, resulting in AV products missing a piece of malware that they previously knew about. Because of polymorphism, we've seen an exponential increase in the amount of new malware variants released year-over-year (Figure 1).

So how common is "zero day," or new and unique malware? Unfortunately, due to polymorphism this problem has become an epidemic. According to Webroot, 97% of the executable malware found on endpoints was unique,[5] meaning it hadn't been seen before and likely wouldn't have been caught by signature-based AV solutions. Other experts agree, finding that almost half of the AV products miss newly released malware[6] the day it's released (day 0).

In short, while signature-based AV solutions are still partially useful for quickly preventing a certain threshold of basic malware, they're insufficient at detecting the more common evasive and advanced malware samples seen today, including the more sophisticated ransomware that has plagued many organizations recently.

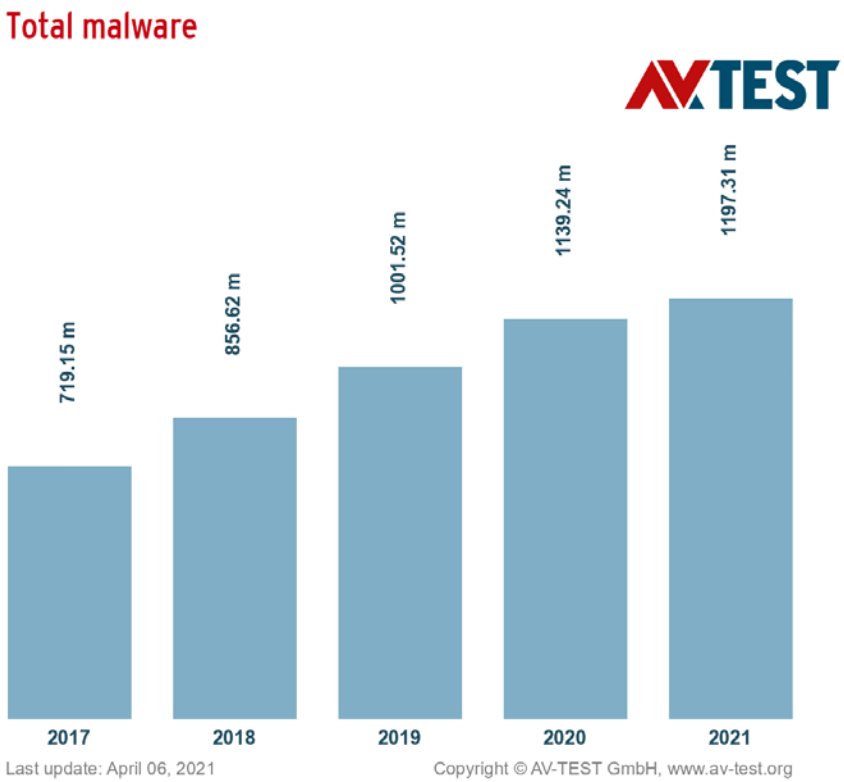
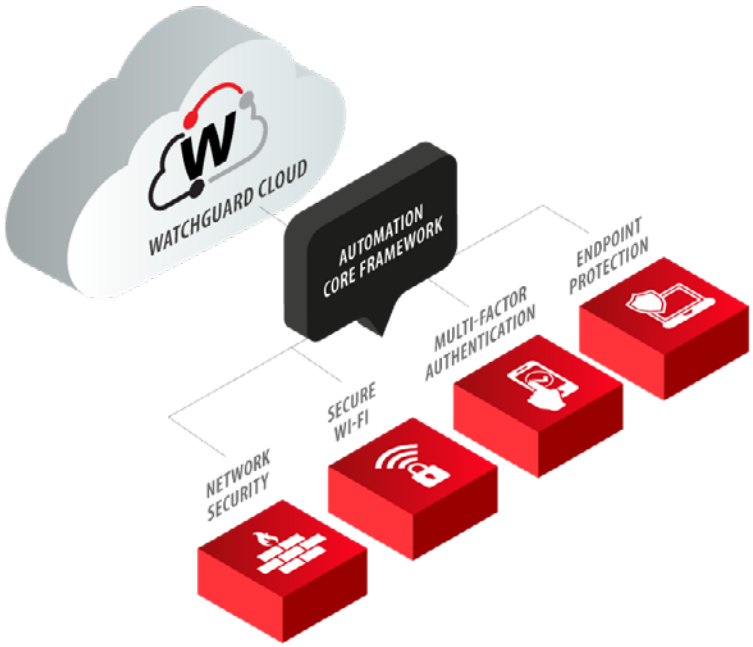


Figure 1: Growth of malware over time according to AV-Test.org [7]

DEFEATING RANSOMWARE WITH UNIFIED SECURITY FROM WATCHGUARD

Originally published by Lockheed Martin as part of the Intelligence Driven Defense model for the identification and prevention of cyber intrusion activity, the Cyber Kill Chain identifies what the adversaries must complete to achieve their objective, by targeting the network, exfiltrating data and maintaining persistence in the organization.

Deploying a unified security platform makes it possible to intercede at several points in the kill chain, preventing the attack from proceeding closer to their objective. Key to this approach is the ability to correlate network and endpoint security events with threat intelligence to detect, prioritize and take immediate action to stop malware attacks. WatchGuard's multi-layer platform makes it possible for organizations of all sizes to defend against advanced malware threats, including ransomware attacks, without unnecessary complexity.



Stopping ransomware attacks before they start requires blocking the three common vectors: phishing, RDP abuse, and scan & exploit techniques. WatchGuard offers a host of solutions that protect your users from being the "patient-zero" for ransomware attacks, including DNS-filtering, spam protection, patch management, and multi-factor authentication. A unified security platform lightens the load for your IT team by integrating advanced technologies to enable comprehensive, multi-layered security across networks, users, endpoints, data, and applications (in the Cloud or on premises). Unifying security into a single platform unlocks efficiencies simply not possible with disparate systems, allowing for automation of frequent manual tasks that take up your IT team's time.

Here are 10 ways WatchGuard can help your IT team defeat ransomware:

1. **Automatically Block Phishing Attempts.** Phishing via email is the most common method for starting a ransomware attack. Blocking malicious emails with spamBlocker on the Firebox and antispam on the endpoint can keep your user's mailbox free of compromise. Miss an email, and a user clicks a link they shouldn't? DNSWatch makes it possible to kill command and control channels and block connections to the bad guys. Need to protect users remotely? DNSWatchGO delivers the same protection on a per-user basis, without requiring a VPN.

2. **Enforce Strong User Identities.** AuthPoint provides effective multi-factor authentication for your workforce, protecting business assets, accounts, and data against credential theft, fraud and phishing attacks. What's more, the AuthPoint mobile app makes each login attempt visible and its unique Mobile DNA ensures only the original device can perform authentication when sophisticated threats try to clone mobile devices.

3. **Easily Close Security Gaps.** According to Ponemon Institute, 57% of victims of cyber attacks said that applying a patch would have prevented them from being attacked and 34% said that they even knew about the vulnerability before the attack. WatchGuard's user-friendly Patch Management solution for managing vulnerabilities in operating systems and third-party applications on Windows workstations and servers can help reduce the attack surface against ransomware attacks.

4. Prevent Unknown Application Execution. Our exclusive Zero-Trust Application Service enables continuous endpoint monitoring, detection and classification of all activity to reveal and block anomalous behaviors of users, machines and processes. Adaptive Defense 360 automatically mitigates the attack, by blocking any unknown application execution until it is validated as trustable by our machine-learning system and/or cybersecurity team.

5 **Eliminate Initial Malware Payloads at the Gateway.** Firewalls like the WatchGuard Firebox are in good position to block first-stage malware files, like droppers, which often are followed by more malicious assets. The Firebox offers three levels of malware protection: Gateway AV (signatures and heuristics), IntelligentAV (signature-less AI-powered prevention), and APT Blocker (advanced Cloud sandbox).

6 **Monitor Active Attacks with Real-Time Visibility.** By nature, ransomware infects endpoint devices. Having visibility into the event activity on these devices makes it possible to detect and remediate the threats before the damage is done. Adaptive Defense 360 provides clear and timely visibility into malicious activity throughout an organization. This visibility allows security teams to quickly assess the scope of an attack and take appropriate responses.

7 **Correlate Telemetry for Greater Context.** Cyber criminals are ninjas at sneaking by traditional security systems. They use stealthy, targeted attacks to soften their footsteps and hide in the shadows, making attacks easy to miss. Part of the WatchGuard Firebox, our ThreatSync solution uses a light-weight host sensor and the power of the Cloud to automatically correlate telemetry data from multiple points in your security stack to rapidly spotlight and kill threats that would have otherwise gone undetected.

8 **Halt File Encryption Without Lifting a Finger.** Host Ransomware Prevention (HRP) leverages a behavioral analytics engine and a decoy directory honeypot to monitor a wide array of characteristics determining if a given action is associated with a ransomware attack or not. If it's determined that the threat is malicious, HRP can automatically prevent a ransomware attack before file encryption on the endpoint takes place.

9 **Restore Endpoints with Ease.** During execution, malware often creates, modifies, or deletes system file and registry settings and changes configuration settings. These changes, or remnants that are left behind, can cause system malfunction instability or even an open door to new attacks. Adaptive Defense 360, in those residual cases in which malware is allowed to run, restores endpoints to their pre-malware trusted state.

10 **Minimize Time to Detection.** WatchGuard's Threat Hunting and Investigation Service helps detect emergent hacking and living-off-the-land techniques. Using our security experts, we analyze suspicious cases to find new and unique evasion techniques (TTPs) in the event stream. From there, we create rules representing new IoAs (indicators of attack) that can be delivered to your endpoints to rapidly protect them against new attacks.

1. https://www.darkreading.com/risk/average-ransomware-payments-more-than-doubled-in-q4-2019/d/d-id/1336893
2. https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion
3. https://www.scribd.com/document/320027570/Malwarebytes
4. https://www.businesswire.com/news/home/20191016005043/en/Cost-Ransomware-Related-Downtime-Increased-200-Percent
5. http://webroot-cms-cdn.s3.amazonaws.com/7814/5617/2382/Webroot-2016-Threat-Brief.pdf
6. http://labs.lastline.com/lastline-labs-av-isnt-dead-it-just-cant-keep-up
7. https://www.av-test.org/en/statistics/malware/

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 over 18,000 security resellers and service providers to protect 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. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuard, on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com