WatchGuard

The Cyber Crime Guide for Small and Midsize Businesses

Find out how hackers wreak havoc on Main Street and learn what you can do to protect yourself.

Main Street Is a Great Place To Be

Your local business or government agency is part of the fabric of your community. People feel secure here. Life is good. But Main Street also has a dark side.

Cyber criminals are targeting Main Street with sophisticated attacks that are tearing down small to midsize businesses (SMBs) and agencies. These crimes don't always make headlines like the hacks that hit nation states or huge entities like Sony, but they're far more pervasive.

The good news? You can protect your Main Street business from cyber attacks. We'll show you how.

Why Main Street?

Today's cyber threats are more sophisticated than ever, making it easy for big-time villains to target small-town businesses. Cyber criminals may be hacktivists with social agendas who want to disrupt your day-to-day business or organized criminal groups going after your customers' financial or personal data.

44% of small businesses have been victims of cyber attacks[1]

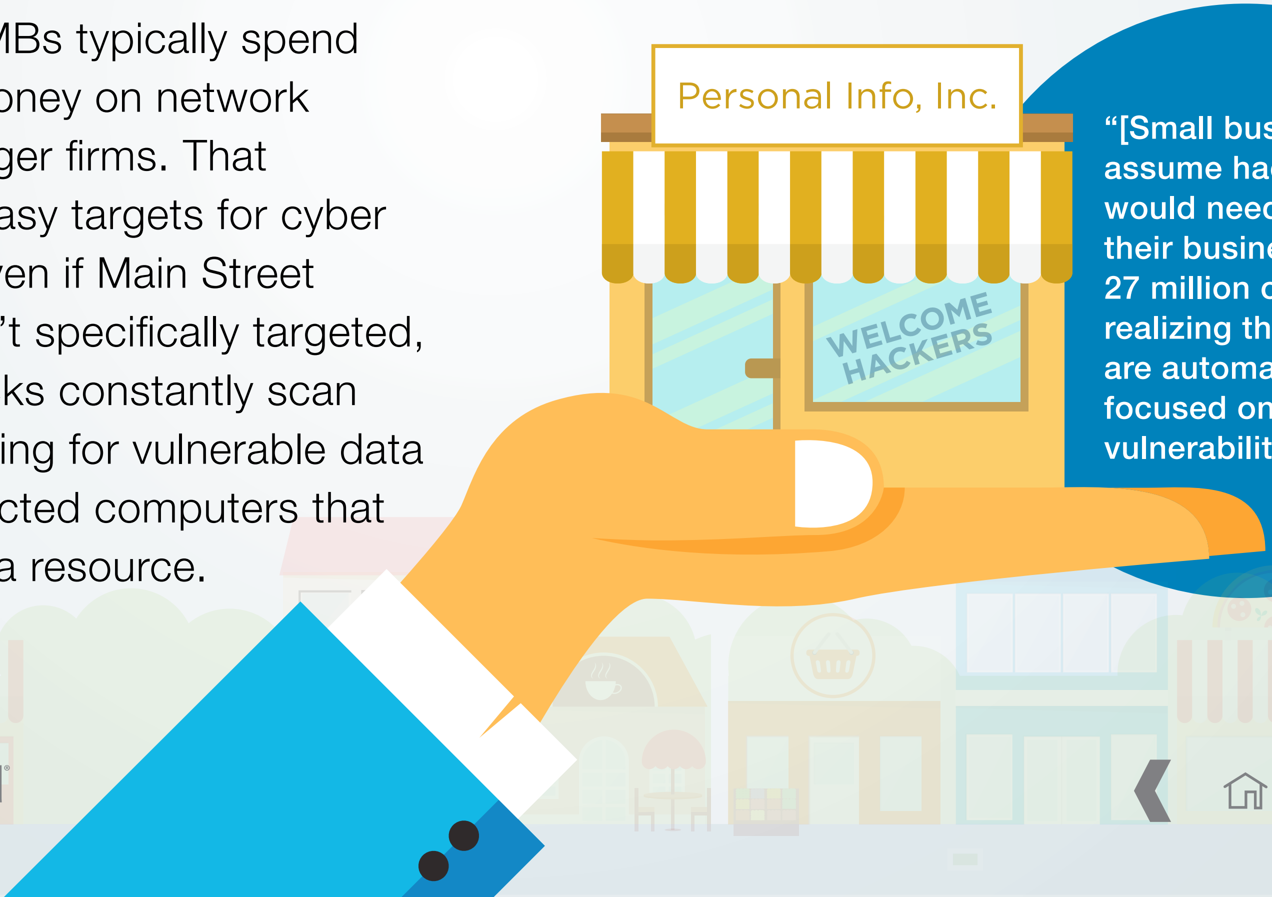
$8,700 Average cost per attack[1]

60% of small businesses hit by a cyber attack go out of business within 6 months of the attack[2]

Main Street Offers Plenty of Easy Targets

In 2014, small firms with annual revenues less than $100 million cut security spending by 20%, while large companies increased security investments by 5%.[3]

Main Street's SMBs typically spend less time and money on network security than larger firms. That means they're easy targets for cyber criminals. But even if Main Street businesses aren't specifically targeted, automated attacks constantly scan the Internet looking for vulnerable data and under-protected computers that can be used as a resource.



"[Small businesses] assume hackers would need to pick their business out of 27 million others, not realizing that the attacks are automated and focused on discovering vulnerabilities."[4]

Could this happen to you?

No Good Deed Goes Unpunished

The receptionist for a small municipal court found a box of branded USB drives left on her desk. In hopes of figuring out who they're for, she plugged one into her computer. The drive was blank, so she gave away the free storage. By then, she had already infected the court's office network—and spread the malware to each of the drive recipients.

U.S. government agencies alone have lost more than 94 million citizens' records since 2009, and each lost record represents a cost of $194.[5]

Main Street Lets Cyber Criminals Stay under the Radar

Security breaches at large companies cost between £450,000 ($697,000) and £850,000 ($1.3 million) on average in 2013. For a small business, a breach could cost anything between £35,000 and £65,000.[6]

Hijacking many smaller businesses rather than individual large entities keeps media and government attention off attackers, while still allowing them to make high returns from multiple targets. In some cases, Main Street businesses may not even be the ultimate target. They're often the weakest link in a chain-of-trust attack in which attackers prey on the security of small, under-protected supply-chain targets to get to their larger business partners.

The 2014 Target breach reportedly occurred when attackers stole network credentials from Target's HVAC provider.[7]

Could this happen to you?

There Is Such a Thing as Bad Press

Hard Hat Construction's (HHC) new building contract for Mega Corporation was well-publicized. On seeing the news, the hackers that had been foiled by Mega's well-crafted network defenses immediately shifted focus. An attachment in a spear-phishing email to an HHC billing manager infected his computer with a key logger. That gave the hackers access to his account in Mega's system, which they used to breach the bigger company—and forever tarnish HCC's reputation.

Nearly 90% of SMBs in the U.S. do not use data protection for company and customer information, and less than half secured company email to prevent phishing scams.[8]

Main Street Is Full of Valuable Data

Retail is one of the top five most-targeted industries in terms of the volume of attacks and attempted intrusions.[9]

Even small and midsize organizations store valuable data that means money for the bad guys. And cyber criminals can target vertical market segments that let them take advantage of common vulnerabilities while still offering the high returns of multiple victims.

Visa Inc. reports that small businesses represent more than **90%** of the payment data breaches reported to their company.[10]

Could this happen to you?

A Hack a Day Keeps the Doctor Away

Westminster Orthopedic's new tablet initiative gave practitioners wireless access to patient data throughout this local health clinic. However, a black hat used a rogue access point to trick a doctor into giving up the private network password. Using the stolen password, the attacker accessed the real network and gained access to patient records, including valuable medical identity numbers.

In 2013, the cost of medical identity theft to consumers was estimated at $12 billion.[11] In 2014, more than 2 million patients were victim to medical identity theft globally, a half million more than were recorded in 2013.[12]

Where the Threats Come From

Blended threats come from many vectors at once

An attack may start as a phishing email that uses the web to download malware, and then communicates data back to the hackers over another network service.

Advanced malware variants grow exponentially every year

Attackers “morph” existing malware to bypass legacy antivirus protection, which is typically two days to two weeks behind. In 2014 alone, 143 million new malware variants were reported.[13]

Nation-state cyber espionage attacks trickle down

Sophisticated techniques of state-sponsored attackers such as spear phishing and watering hole attacks are increasing in the private sector. Zeus, a common banking botnet, uses Stuxnet’s techniques.

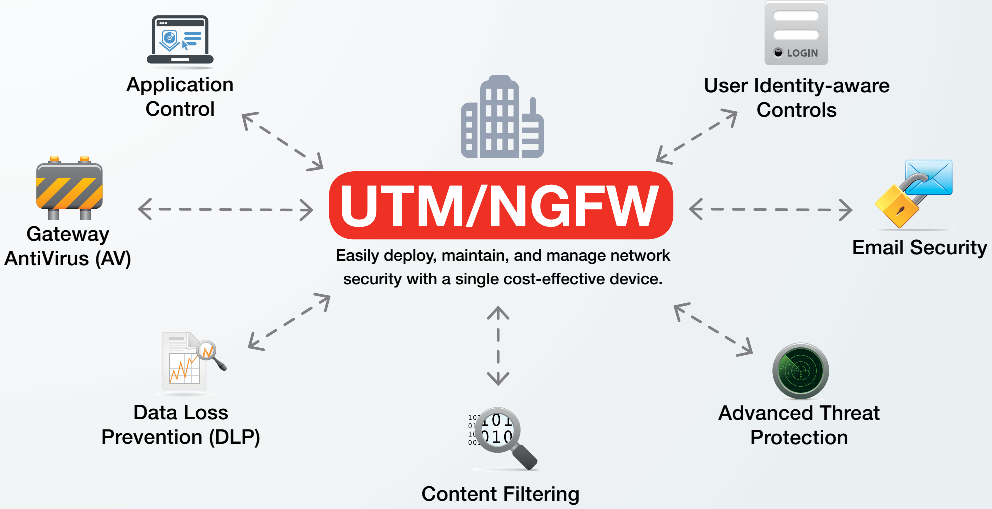
3 Steps to Protecting Main Street

STEP ONE

Upgrade your Protection

Despite the fast-evolving threats to Main Street, many SMBs and local agencies are still focused on legacy defense strategies such as a simple firewall. The first step is to upgrade to the protection of a next-generation firewall (NGFW) or unified threat management (UTM) device that combines all of today's necessary defenses in a single easy-to-manage and cost-effective appliance.

WatchGuard's future-proof platform delivers the industry's best-performing defenses in each category, and performs at line speed so you don't sacrifice network performance even with all security engines turned on. WatchGuard's Firebox® M200 and M300 firewalls are up to 218% faster than the competition in overall performance and up to 385% faster for encrypted traffic inspection.[14]



UTM/NGFW

Easily deploy, maintain, and manage network security with a single cost-effective device.

Application Control

User Identity-aware Controls

Gateway AntiVirus (AV)

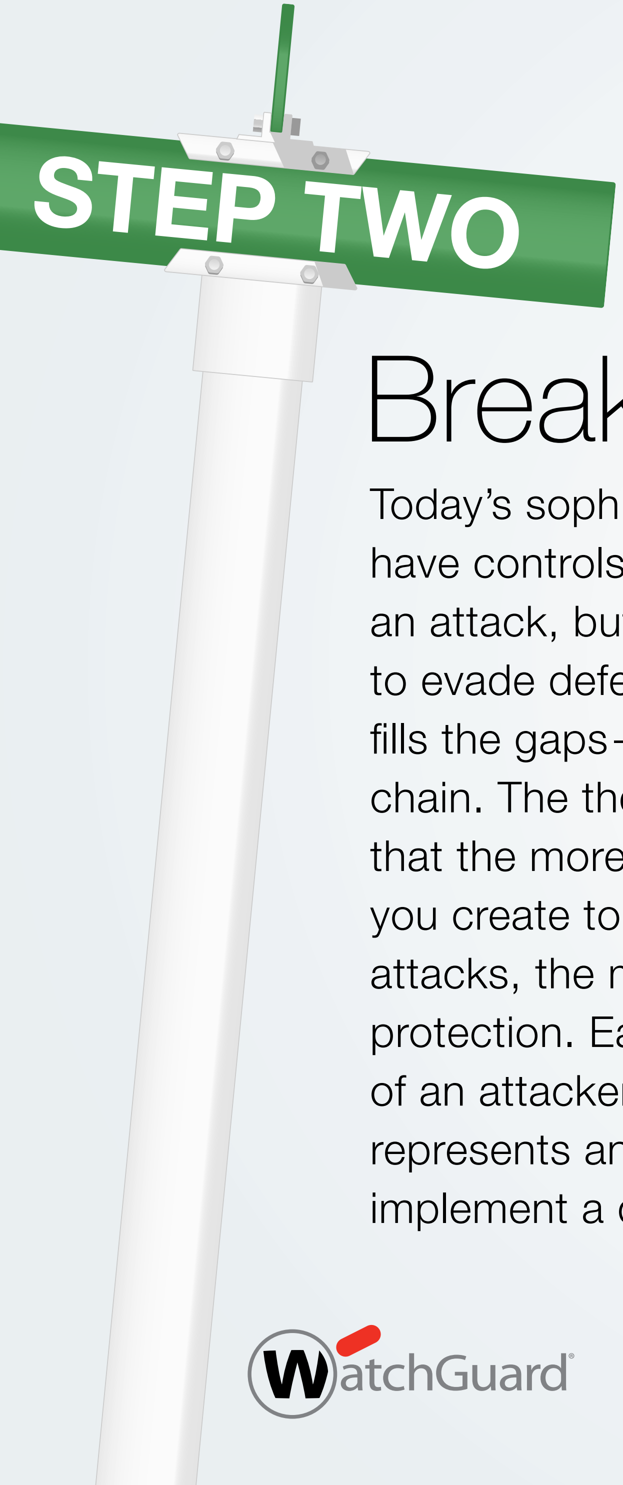
Email Security

Data Loss Prevention (DLP)

Content Filtering

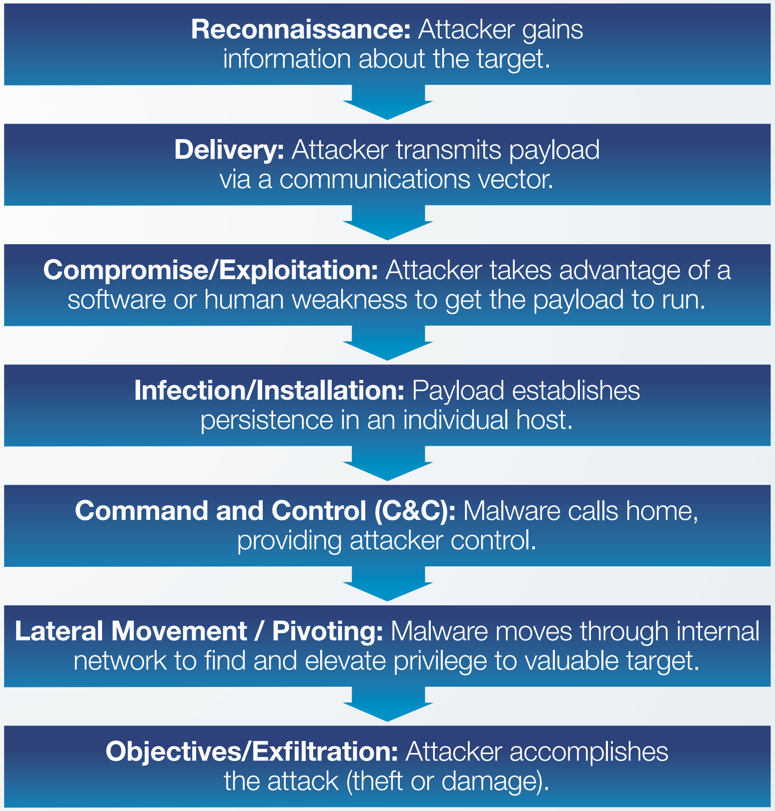
Advanced Threat Protection

3 Steps to Protecting Main Street



Break the Kill Chain

Today's sophisticated security devices have controls to catch different parts of an attack, but attackers can still find ways to evade defenses. Defense-in-depth fills the gaps—breaking the attacker's kill chain. The theory behind the kill chain is that the more layers (or links) of defense you create to prevent different types of attacks, the more you maximize your protection. Each link represents part of an attacker's methodology, but also represents an opportunity for you to implement a defense.



Reconnaissance: Attacker gains information about the target.

Delivery: Attacker transmits payload via a communications vector.

Compromise/Exploitation: Attacker takes advantage of a software or human weakness to get the payload to run.

Infection/Installation: Payload establishes persistence in an individual host.

Command and Control (C&C): Malware calls home, providing attacker control.

Lateral Movement / Pivoting: Malware moves through internal network to find and elevate privilege to valuable target.

Objectives/Exfiltration: Attacker accomplishes the attack (theft or damage).

3 Steps to Protecting Main Street

See the Threat to Defend Against It

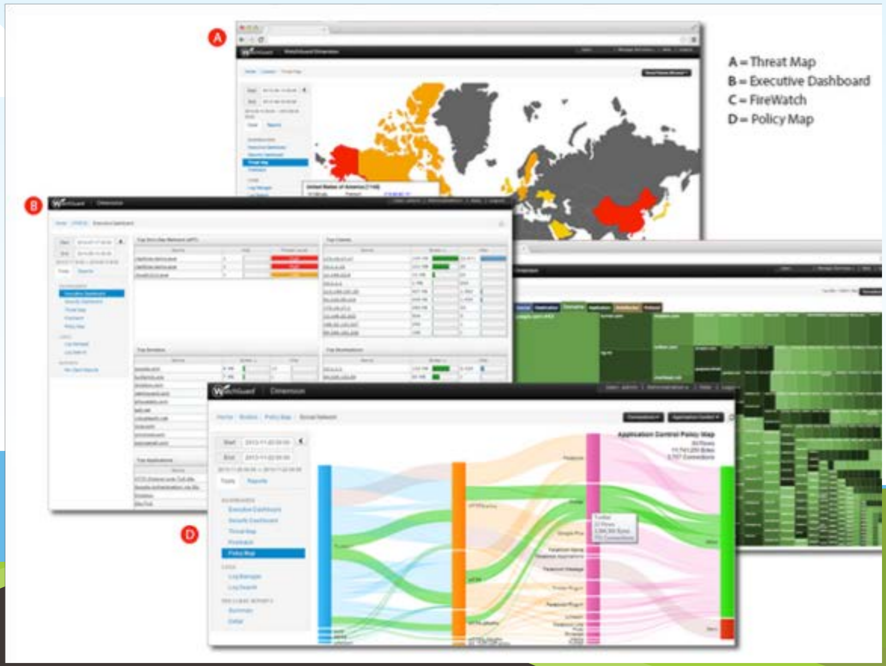
Small businesses are breached every day, but a third of them admit to being uncertain about whether or not they were attacked.[15] For both small and large organizations, it takes an average of 80 days for businesses to notice they've been breached.[16] By that time, the damage is already done. These breaches are being missed because we're drowning in an ocean of data.

Since you can never have perfect defense, the third critical step in your security strategy is to implement discovery-and-response tools to help you see and handle the incidents that get past your gates. You need a tool that brings the data from all your security controls together and correlates different security triggers into a single incident so you don't miss signs of a sophisticated, multi-vector attack.

Keep Main Street Safe

SMBs and local government agencies are increasingly targets of sophisticated, enterprise-class network attacks. WatchGuard offers enterprise-class defense that's designed specifically to meet the unique needs of SMBs. We'd love to help you keep Main Street safe. Contact us today!

Visibility and analytics tools such as WatchGuard Dimension™ translate millions of lines of logs into the thimble-full of intelligence you need to recognize and address problems in your network.



A = Threat Map
B = Executive Dashboard
C = FireWatch
D = Policy Map

505 Fifth Avenue South
Suite 500
Seattle, WA 98104
www.watchguard.com
North America Sales
+1.800.734.9905
International Sales
+1.206.613.0895

About Watchguard

WatchGuard® Technologies, Inc. is a global leader of integrated, multi-function business security solutions that intelligently combine industry standard hardware, best-of-breed security features, and policy-based management tools. WatchGuard provides easy-to-use, but enterprise-powerful protection to hundreds of thousands of businesses worldwide. WatchGuard is headquartered in Seattle, Wash. with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis.

[1] 2013 survey by the National Small Business Association, http://www.nsba.biz/wp-content/uploads/2013/09/Technology-Survey-2013.pdf

[2] National Cyber Security Alliance, Stay Safe Online, Small Business Online Security Infographic, 2014, https://www.staysafeonline.org/stay-safe-online/resources/small-business-online-security-infographic

[3] PWC's Global State of Information Security Survey 2015, http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

[4] "Hackers put a bull's-eye on small business." http://www.pcworld.com/article/2046300/hackers-put-a-bulls-eye-on-small-business.html

[5] "2012 Deloitte-NASCIO Cybersecurity Study: State governments at risk: a call for collaboration and compliance." http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy2012.pdf

[6] "The threat from cybercrime? 'You ain't seen nothing yet.'" PricewaterhouseCoopers (PwC) research, reported by CNBC http://www.cnbc.com/id/100959481

[7] "Target Hackers Broke in Via HVAC Company." http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[8] "Cybercrime and hacking are even bigger worries for small business owners." http://www.theguardian.com/business/2015/jan/21/cybersecurity-small-business-thwarting-hackers-obama-cameron

[9] "How Small Businesses Are Vulnerable to Cyber Attack." http://www.mydigitalshield.com/small-businesses-vulnerable-cyber-attack/

[10] "The challenge of digital security: What will it take for retailers to protect themselves?" http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SNDE_RE_RE_USEN&htmlfid=REW03017USEN&attachment=REW03017USEN.PDF#loaded

[11] "2013 Survey on Medical Identity Theft." http://medidfraud.org/2013-survey-on-medical-identity-theft/

[12] "2014 Fifth Annual Study on Medical Identity Theft." http://medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft/

[13] AV-Test report http://www.av-test.org/en/statistics/malware/

[14] Miercom Performance Report http://www.watchguard.com/docs/analysis/miercom_report_062015.pdf

[15] "The Risk of an Uncertain Security Strategy: Study of Global IT Practitioners in SMB Organizations." https://sophos.files.wordpress.com/2013/11/2013-ponemon-institute-midmarket-trends-sophos.pdf

[16] "The Post Breach Boom." Ponemon Institute study 2013. http://www.ponemon.org/local/upload/file/Post%20Breach%20Boom%20V7.pdf