
SONICWALL®
Types of Cyberattack Strategies and How to Defeat Them
E-BOOK

Introduction

Modern cybercriminals have elevated their already complex techniques to avoid detection as they sneak quietly into networks for a variety of motives, often driven by financial gain. These threat actors are looking to steal intellectual property, commit espionage, disrupt processes or hold files for ransom among many other crimes. They employ the latest techniques to evade detection, aiming to maintain their access and carry out their malicious activities without being noticed.

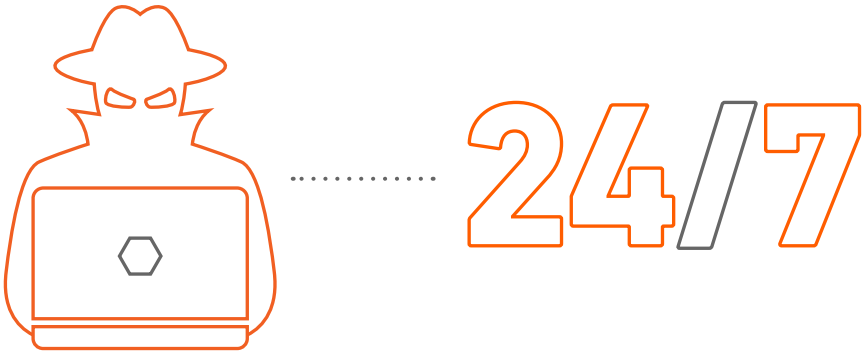
Once they have exploited a target, attackers will attempt to download and install malware onto the compromised system. In many instances, the malware used is a newly evolved variant that traditional anti-virus solutions don't yet know about.

This eBook details the cyberattack strategies and tools that cybercriminals use to infiltrate your network and breaks down how you can counter those strategies to stop cybercriminals in their tracks.

Cyberattack Strategy #1
Bombard Networks with Malware Around the Clock

Malware is on the rise in total volume, with some countries seeing record attempts in the multi-millions . Attacks can come in from all vectors to target and compromise your network. Email, mobile devices, web traffic and more are all targets, and hackers can even compromise you through automated exploits. On top of this, the size of your company doesn't matter. To a hacker you are an IP address, an email address or a prospect for a watering hole attack. Attackers use automated tools to execute exploits or to launch phishing emails throughout the day and night.

The problem that many organizations face is not having the right tools for the job. Many lack automated tools to help scrub traffic, protect endpoints and filter out bad emails. Others run firewalls that can't see into encrypted traffic for hidden threats or rely on limited onboard system memory to store malware signatures.

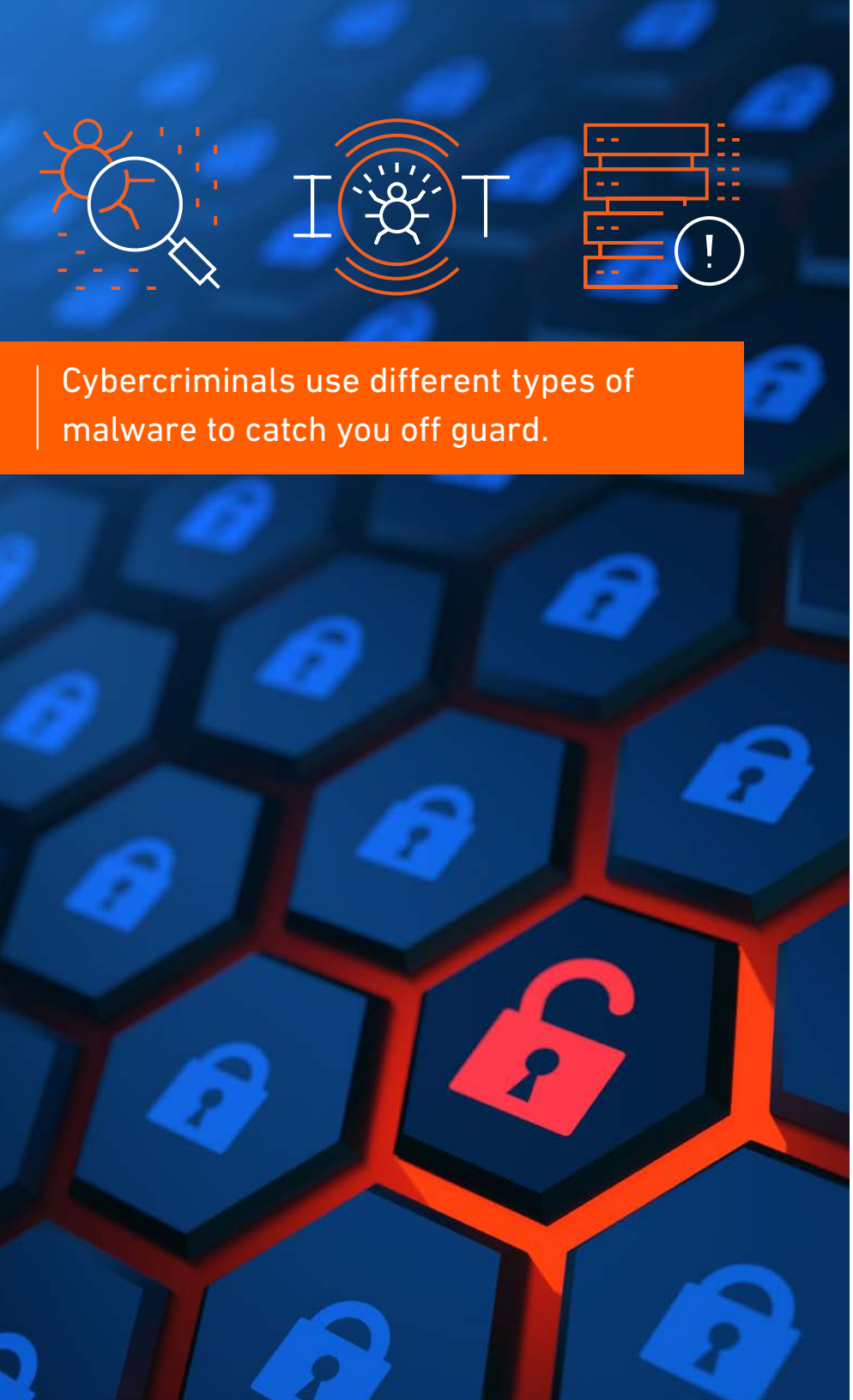


Counter-Attack #1
Protect Your Network Every Minute of Every Day

With hundreds of never-before-seen malware variants developed every hour, organizations need up-to-the-minute, real-time protection against these new threats. An effective security solution needs to have the latest technology to detect danger in real time, protecting your organization 24 hours a day, seven days a week. With the large influx of malware types and variants, the available memory of any firewall is exceeded. A security services solution that includes technology like Real-Time Deep Memory Inspection (RTDMI™) proactively detects and blocks mass-market zero-day threats and unknown malware variants.

Firewalls should use a cloud-based sandbox in order to provide the broadest view of malware and discover and identify brand-new variants. It's also critical to make sure your security solution supports dynamically updated protection not only at the firewall gateway but at mobile and remote endpoints as well, because Internet of Things (IOT) devices can serve as entry points for attackers.

Insist on a security platform that leverages the power of the cloud for automated real-time breach detection and prevention to counter the latest malware threats.



Cybercriminals use different types of malware to catch you off guard.

Cyberattack Strategy #2 Infect Networks with Different Forms of Malware

Cybercriminals use multiple attack vectors and malware variants to compromise networks. The five most typical types are viruses, worms, Trojans, spyware and ransomware.

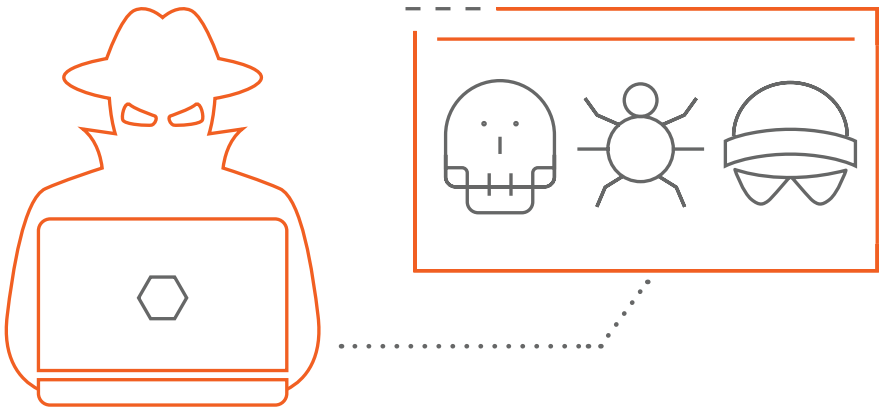
Computer viruses were originally spread through the sharing of infected media. As technology evolved, so too did the distribution method. Today, viruses are commonly spread through legitimate programs, file sharing, web downloads and email attachments. They can commit a range of malicious actions from data corruption to system crashes when opened or executed.

Computer worms have existed since the late 1980s but were not prevalent until networking infrastructures within organizations became common. Unlike computer viruses, worms are self-replicating and can crawl through networks without any human interaction. They can cause rapid infections and overload networks with traffic.

Trojans are malicious programs posing as legitimate software or files designed specifically to extract sensitive data from the network. Many types of Trojans will take control of the infected system and open up a back door for the attacker to access later. Trojans are also often used in the creation of botnets.

Spyware is not typically malicious in nature, but it is a major nuisance because it often infects web browsers, making them nearly inoperable. Spyware is sometimes disguised as legitimate applications, providing the user with some benefits while secretly recording keystrokes and browsing history, stealing personal data, or tracking user behavior and usage patterns. The stolen data is then sent to the attacker, compromising the users' privacy and security.

Ransomware is an attack that often encrypts the files on an endpoint or an entire server, rendering them inaccessible. Cybercriminals demand ransom from the organization, usually in Bitcoin, to receive the encryption key. When it spreads to business-critical systems, the cost of ransomware can swell to hundreds of thousands of dollars or more.



To stay ahead of threats, consider multiple layers of protection against malware.

Counterattack #2
Ensure That Your Network Is Protected Against All Types of Malware

All firewalls should safeguard organizations from all types of cyber threats. This is best accomplished by integrating these protections into a single pass, low-latency approach that blocks attack vectors not only at the gateway, but also at endpoints beyond the traditional perimeter. Look for features that include:

- Network-based malware protection to block attackers from downloading or transmitting malware to a compromised system
- Continuous and timely updates to safeguard networks around the clock from millions of new malware variants as soon as they are discovered
- Intrusion Prevention Service (IPS) to prevent attackers from exploiting vulnerabilities
- Sandboxing to send suspicious code to a cloud-based isolated environment for detonation and analysis to find never-before-seen malware
- Access security to apply user access control countermeasures at mobile and remote endpoints, both inside and outside of the network perimeter
- Email security to block phishing, spam, Trojans and social engineering attacks transmitted via email

Making sure that every device that has access to your network has up-to-date anti-virus protection software will provide an additional layer of network malware protection. When organizations pair a PC running comprehensive anti-virus with network firewalls, they can stop many of the tools cybercriminals have for compromising the network.

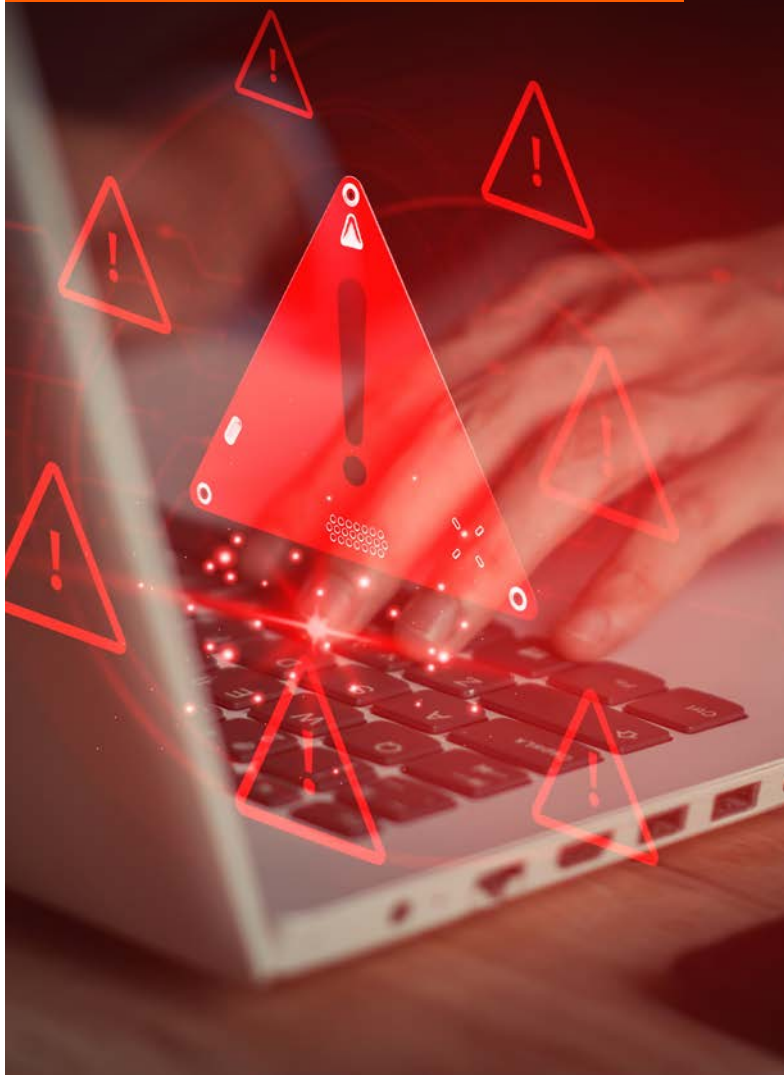
Cyberattack Strategy #3
Find And Compromise the Weakest Networks

Although many firewall vendors claim to offer superior threat protection, few are able to demonstrate the effectiveness of their solutions. Organizations that use legacy firewalls may believe their networks are protected, but skilled cybercriminals can sneak past firewalls that lack the right security measures by using complicated algorithms to evade detection and compromise the network.

Some firewalls offer security at the expense of performance which may tempt organizations that use them to turn off or limit their security measures in order to keep up with the demand of high network performance. This is an extremely risky practice that should be avoided.

Another vulnerability in network security arises from the human factor. Criminals depend on the potential for human actions or behaviors to inadvertently compromise the integrity, confidentiality and availability of a network. Actions that can introduce risks and weaken security measures include phishing scams, social engineering, misconfigured systems, unpatched software, ignored security policies and more. Threat actors exploit these tactics to gain login and other authorization information that can enable them to simply sidestep firewall protections by instigating attacks from the inside. On top of this, employees sometimes connect personal devices to the corporate network without proper security measures. This can lead to unauthorized access if a personal device is lost or left unattended, exposing the organization to a breach when they are outside of the network security perimeter.

> Cybercriminals often target their victims based on the network weaknesses they discover.



> All firewalls need an engine that protects networks from both internal and external attacks — without compromising performance.

Counterattack #3

Choose a comprehensive security platform that offers superior threat protection, high performance and centralized management.

Look for security solutions that have been independently tested and certified for network-based malware protection.

Consider a multi-core platform design that can scan files of any size and type to respond to changing traffic flows. All firewalls need an engine that protects networks from both internal and external attacks without compromising performance.

Look for a firewall that offers a cloud-based sandbox to help discover brand-new malware that may be targeting your environment. These choices could be the difference between a normal workday and one where cybercriminals hold your digital assets hostage.

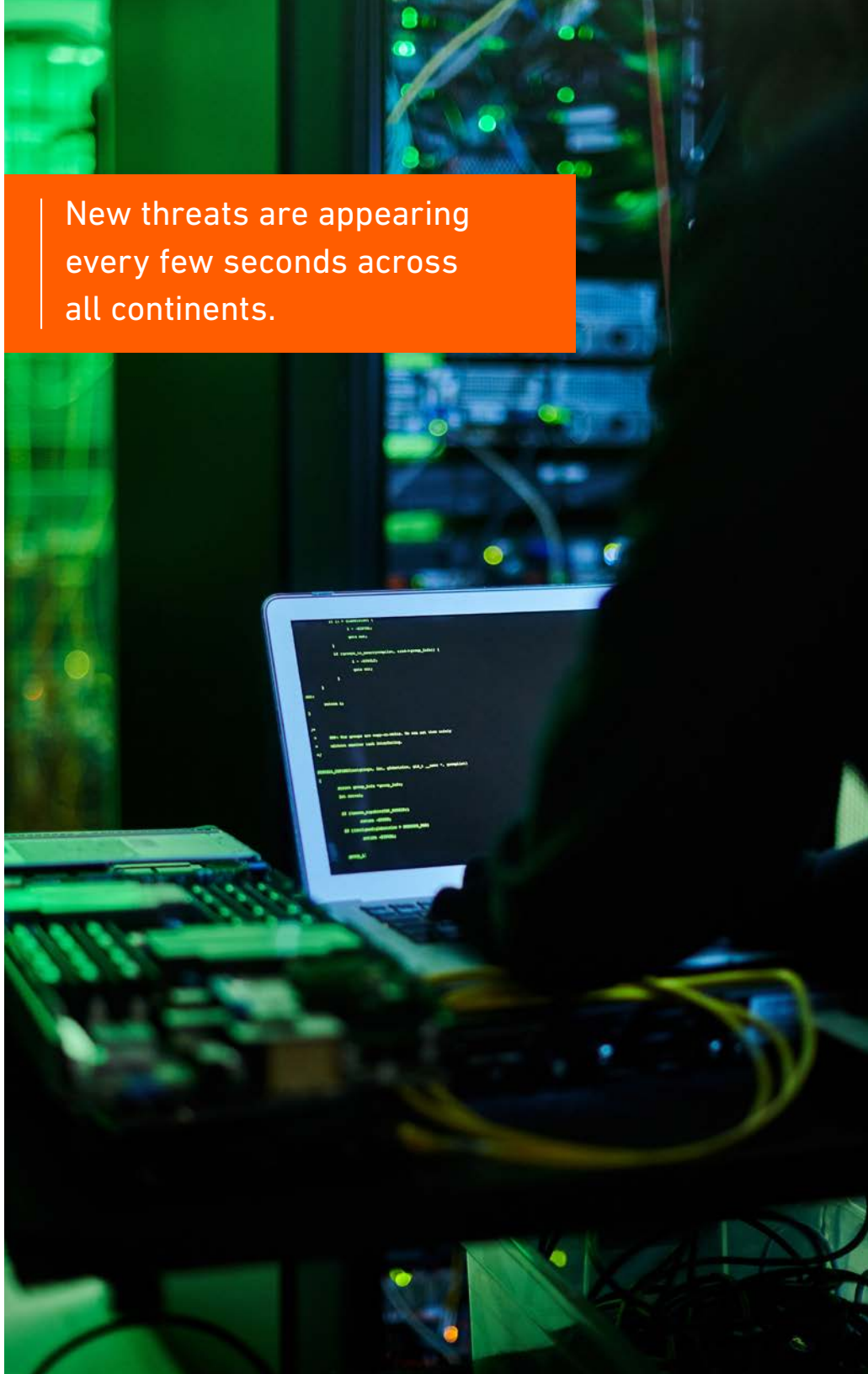
Your security strategy must include the protection of mobile and remote endpoints both inside and outside the perimeter for secure mobile access.

In addition, you need email security to protect against phishing, spam, viruses, social engineering and other threats transmitted via email. Use tools like the free SonicWall Phishing Quiz to educate your organization.

Cyberattack Strategy #4
Morph Frequently and Attack Globally

Many cybercriminals succeed by continually inventing new malware and sharing it with their counterparts around the globe. This means that new threats are appearing every few seconds across all continents. Many cybercriminals use a “smash and grab” approach to attacks: get in, take what they can and get out before anyone can raise the alarm. They can be in and out before you even know what’s hit you. Others go low and slow in an attempt to gain access to more data over a longer period of time. Some attacks come through the web while others go through email or directly into the network on infected devices that were previously roaming outside the network security perimeter.

New threats are appearing every few seconds across all continents.



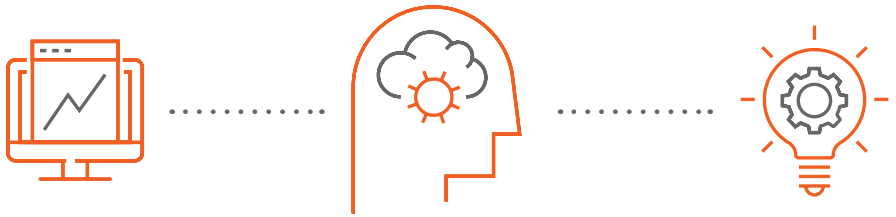
To block the latest global threats, invest in a security solution with global threat intelligence.

Counterattack #4
Choose a Firewall That Protects Against Global Threats

Reacting quickly to threats is critical for maximizing protection. In order to rapidly deploy countermeasures against emerging threats, look for a security solutions provider that has its own threat intelligence, research and counter measures team. In addition, that team should extend its reach by collaborating with the broader security community, similar to the SonicWall Cyber Threat Report.

A broad-spectrum solution utilizes a globally comprehensive cloud-based malware catalogue to augment local firewall analysis.

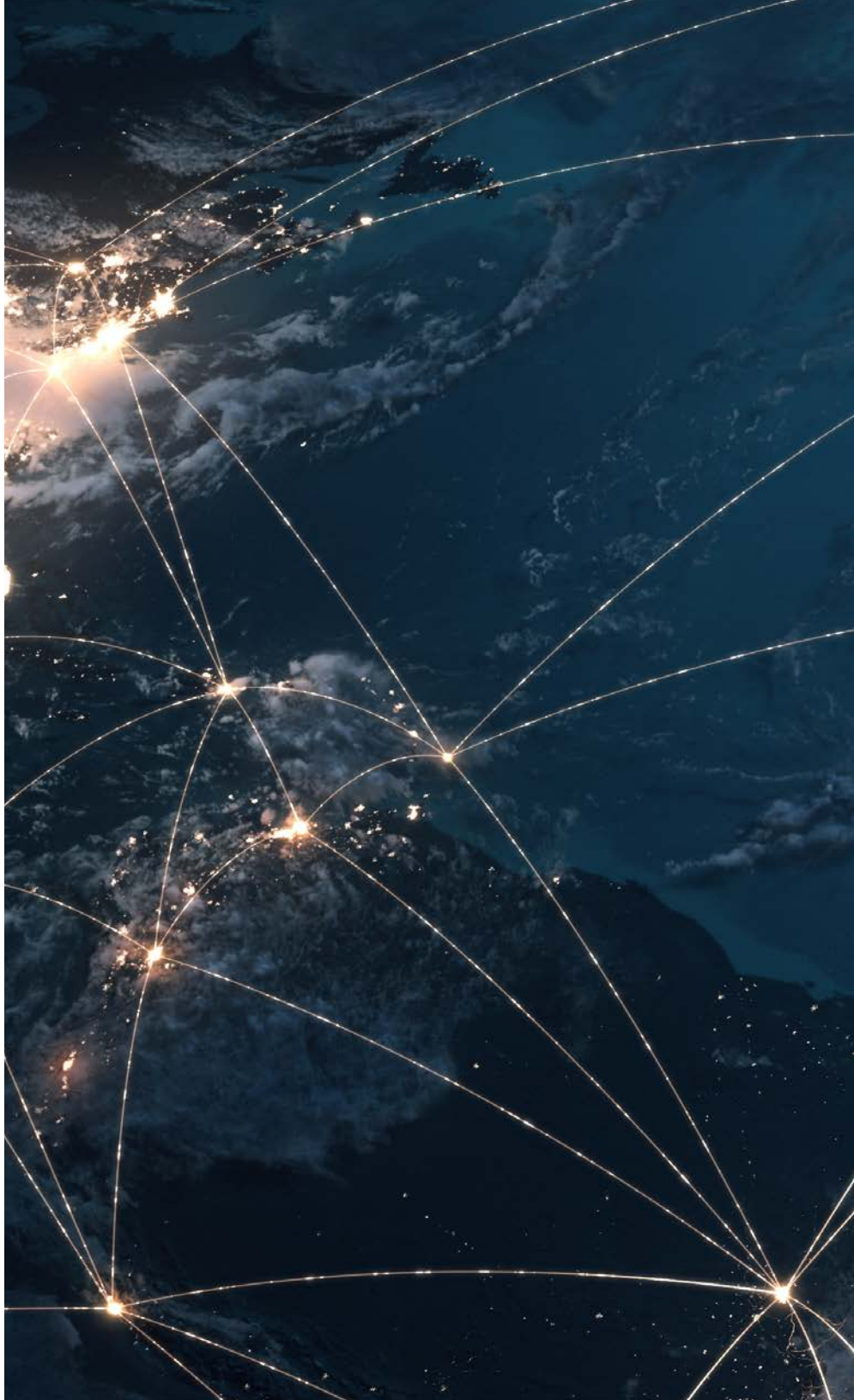
Finally, while a simple firewall can identify and block by geography, a more sophisticated next-generation firewall will add botnet filtering capabilities to reduce exposure to known global threats by blocking traffic from dangerous domains or blocking connections to and from malicious locations.



Conclusion

When developing effective defense strategies against network-based cyberattacks, you should implement a holistic approach incorporating strong security practices and the use of effective security tools that detect and respond to abnormal network behavior without compromising performance. Protect yourself and your organization from the unknown by staying proactive in adapting to evolving threats.

When you're ready to evaluate counterattack solutions that fit the unique needs of your organization, contact your SonicWall representative or visit us online to learn more about SonicWall's Next-generation Firewall (NGFW).



How can I learn more?

Contact us to get in touch with a SonicWall security expert.

Check out our available Live Demos of our SonicWall product line.

Visit our web page, Next-generation Firewalls

See where up-to-date attacks are happening in our Capture Labs Security Center.

SONICWALL

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®

Ebook-TypesofCyberattacks-JK-8854