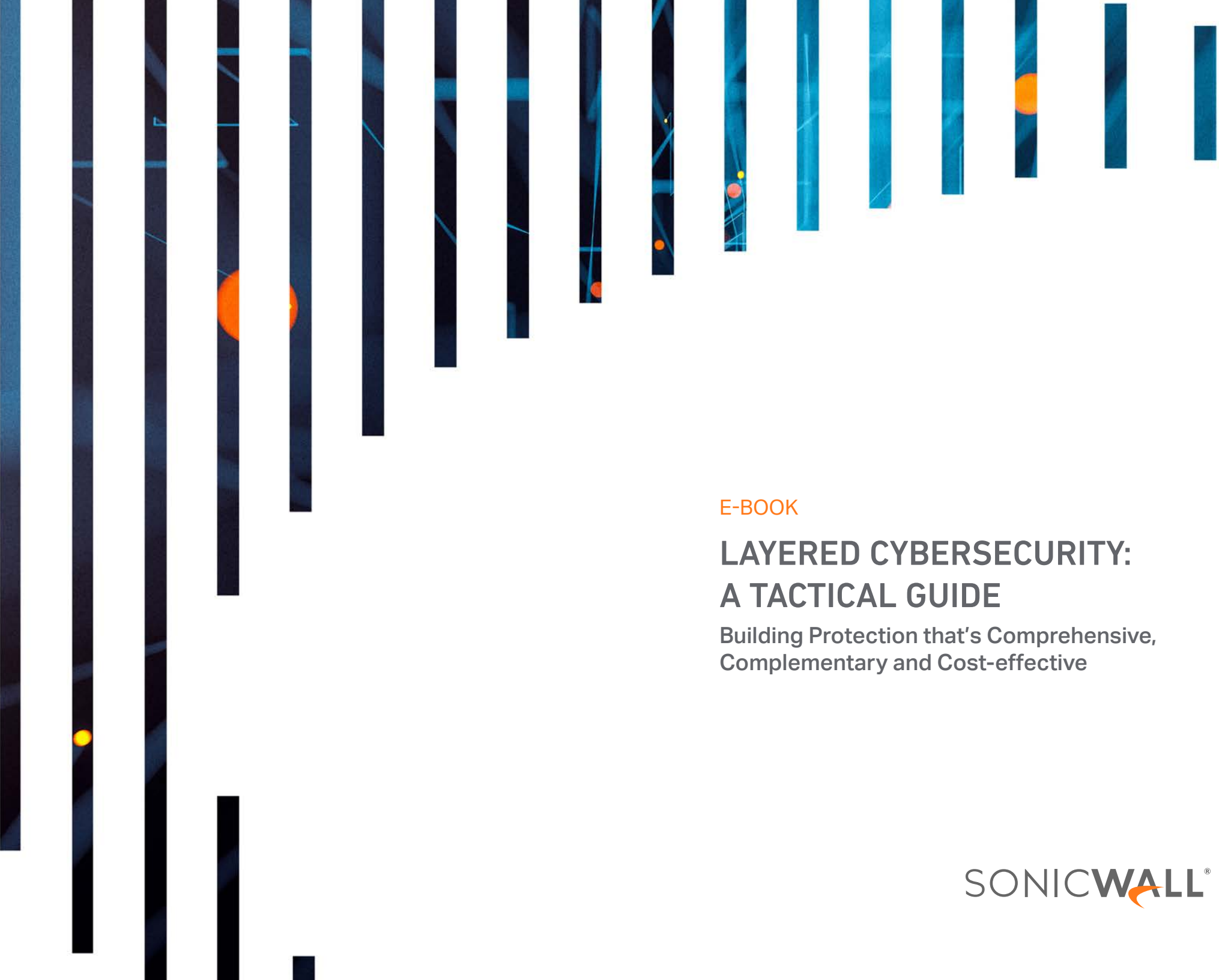


E-BOOK

LAYERED CYBERSECURITY: A TACTICAL GUIDE

Building Protection that's Comprehensive, Complementary and Cost-effective

SONICWALL®

Executive Introduction

The notion of layered security isn't new. But with companies needing to mobilize for the new business normal amid threats that are increasingly sophisticated, more varied and more frequent, layered cybersecurity has never been more relevant.

The idea behind layered cybersecurity is simple: The more obstacles you place in front of an attacker, the better your chances are to identify and stop the attack before your network, data or business are compromised.

While many organizations understand the basics of layered security, our new hyper-distributed IT reality—where everyone is remote, everyone is mobile, and everyone is less secure—requires us to revisit and refine this best practice.

To help, SonicWall has prepared a layered approach to meet the needs of your boundless workforce while keeping your business objectives a priority.

While there are different schools of thought on which layers are the most important (e.g., logical, most critical, easiest to implement, etc.) this guide offers a top-down look at the vulnerabilities you should mitigate first.

It should also be stated that a modern layered security strategy should be grounded and managed in a unified, harmonized and un-siloed environment.

"This is what layered security is all about: understanding how the bad guys are attacking us. This is a battlefield and they're charting it out."

Bill Conner
President & CEO
SonicWall

LAYER 1

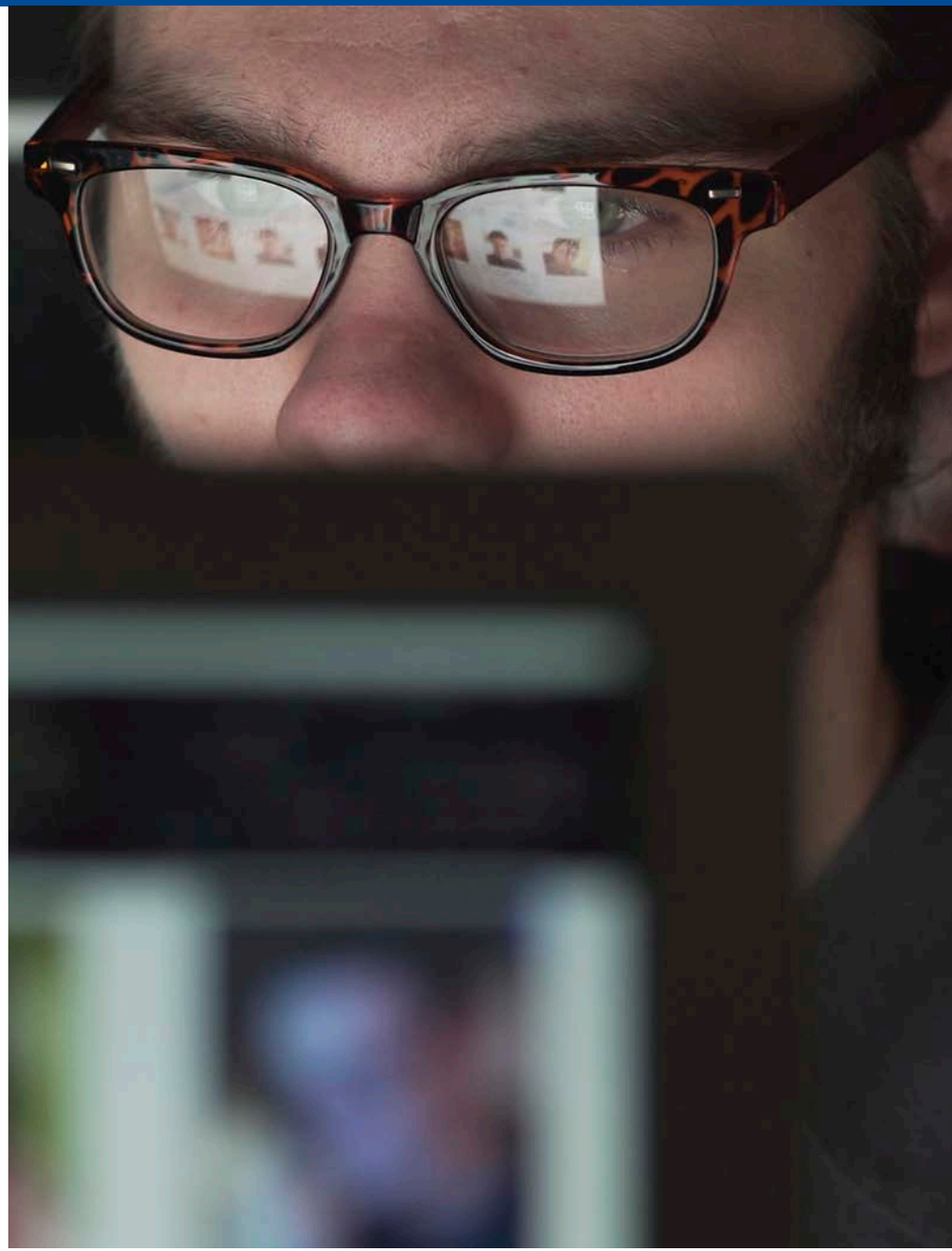
Security Awareness

You've purchased a full complement of the latest and greatest cybersecurity solutions, hired the best cybersecurity team, and patched every vulnerability you could find. On paper, your security posture looks great—until an attacker convinces one of your employees that they're with IT and talks them into giving up their credentials.

Phishing and other social engineering tactics have a long, successful track record—and the current pace of change in the business world is giving them an even bigger advantage. With an unprecedented number of remote employees using more devices than ever, vulnerable to more attacks than ever, it's never been more crucial to educate employees about the dangers of attacks that exploit human behavior and curiosity. It will require a top-down culture shift driven by the C-Suite—but when done correctly, Security Awareness initiatives can successfully mitigate the biggest security risk in any organization.

Security Awareness should include:

- Frequent, consistent and ever-evolving employee cybersecurity education
- Routine but unannounced penetration testing, particularly for phishing, downloads and telephone exploits
- Understanding and complying with established procedures, which could include everything from sites to avoid or which sanctioned apps or services to use.
- Tiered ramification for non-compliance
- Using established best practices and training in the real world (eg., social media)



LAYER 2

Strong Authentication

You have your front door (or wall in this case) in place, but you still need to look through the peep hole to see who you can let in. It's a labored metaphor, but the premise has been around as long as mankind has been building walls, doors and moats.

This is the role of identity and access management (IAM), which is a wide-ranging area of information technology that classifies processes and controls to confirm only appropriate — and vetted — users have secure access to your networks, services and data.

Luckily, most end users are familiar with two-factor authentication (2FA) or multifactor authentication (MFA), so adoption shouldn't be too difficult if deployed properly and with consistent communication.

LAYER 3

Email Security

One of the truths of email-borne threats is that attackers are quick to respond to mega-trends. The work-from-home rush along with the terrible COVID-19 pandemic are just the latest examples that makes email the top attack vector by far for hackers. Sadly, these will not be the last.

Moreover, government regulations now hold your business accountable for protecting privacy data, ensuring it is not leaked and ensuring the secure exchange of email containing sensitive customer data or confidential information.

Thankfully, a range of advanced email protection options are available, including on-premise appliances to cloud-native services.

Regardless of the deployment strategy, organizations must use a layered security solution that goes beyond anti-spam and anti-malware. A sound secure email solution should include dedicated, advanced-threat protection capabilities, and protect against targeted phishing with malicious attachments and URLs, business email compromise (BEC), as well as impostor-based attacks.

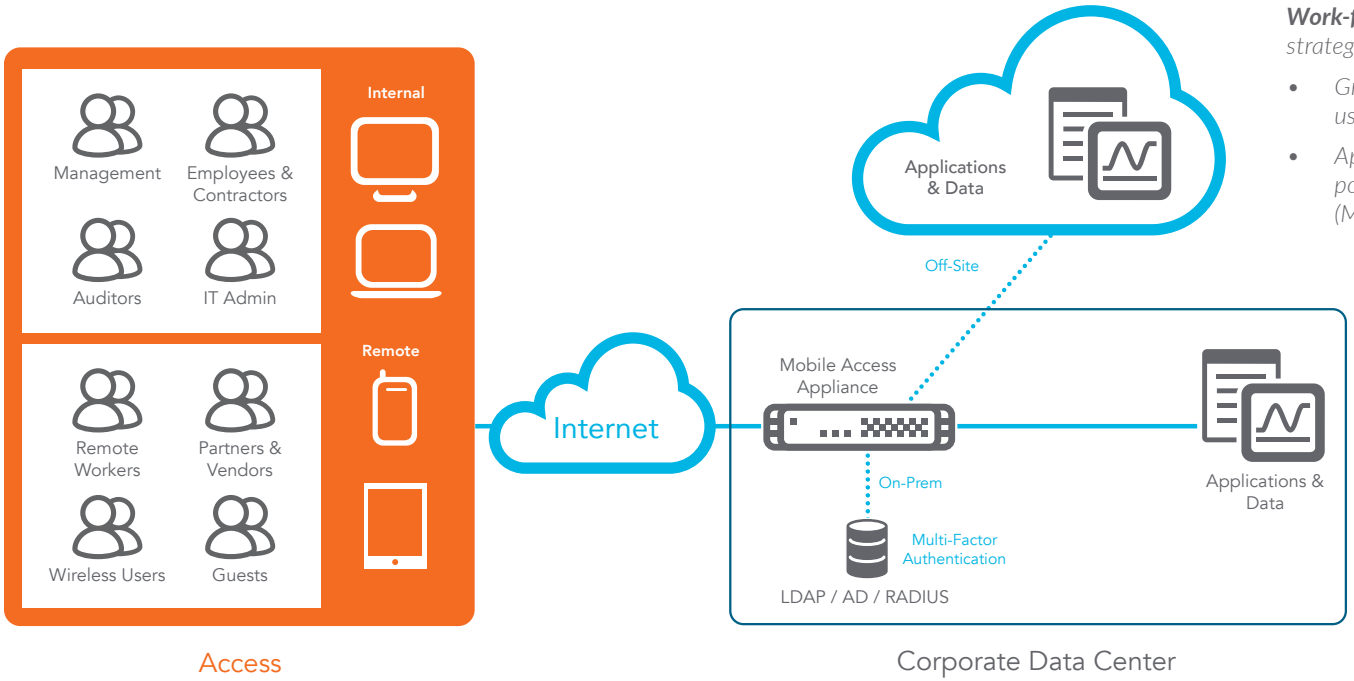
SONICWALL®

LAYER 4

Mobile & Remote Access Security

Security would be much easier if organizations only had to maintain oversite of a controlled, defined environment. But users and devices move in and out of networks — and it's the organization's responsibility to ensure mobile workers have secure access when they leave the network perimeter.

With SonicWall SMA, organizations can provide a field-proven and secure remote access solution that boosts productivity, supports mobility, and enforces compliance through proper user and device authentications.



Work-from-Anywhere Secure Access. *A robust layered security strategy should include capabilities to support:*

- *Grant anywhere, anytime secured access after establishing user and device identities, location and trust*
- *Apply multiple access layer security based on granular policy-based access controls, Multi-Factor Authentication (MFA), Application level VPN, and Geolocation policies*

SONICWALL®

LAYER 5

Wireless Security

Just because employees or users are within the perimeter of your network, doesn't mean any and all threats have been mitigated.

In the modern work environment, users are connected wirelessly to the network via Wi-Fi access points. This can introduce risks depending on what content they access while at work or what sites or applications they use.

Both scenarios can present new risks that should be identified and stopped by advanced secure wireless solutions.

More robust offerings will also include easy-to-use wireless management consoles and Wi-Fi planning tools to add more convenience and help reduce costs.

SONICWALL®

LAYER 6

Endpoint Protection

End-users' curiosity is a risk factor in itself. Forever seeking connectivity, users will often connect to any available network without considering potential ramifications.

They'll also click on unknown links, fall victim to phishing emails, download applications from an untold number of unvetted sources and potentially, worst of all, insert unknown USB drives into their machines. These endpoints then become attack vehicles leveraged to penetrate your defenses.

Safeguard these endpoints (e.g., laptops, computers, servers, etc.) — and protect users from themselves — with next-generation antivirus (NGAV) solutions or an endpoint protection platform (EPP).

But one of the most critical best practices is to use device control capabilities to stop unknown USB keys from connecting to the endpoint. With SonicWall Capture Client, for example, administrators can create customized policies for known and unknown USB devices. For instance, they could allow all mice and keyboards, but block unknown USB keys while allowing approved or registered ones.

Once in place, endpoint protection will help you monitor and mitigate cyberattacks that compromise an endpoint, ensuring malware can't laterally spread through your network or organization. The EPP has two roles: first, it serves as your last line of defense within your network and should provide additional sandboxing capabilities and security policies; second, it is your first line of defense on mobile computers and should have the ability to be managed remotely.

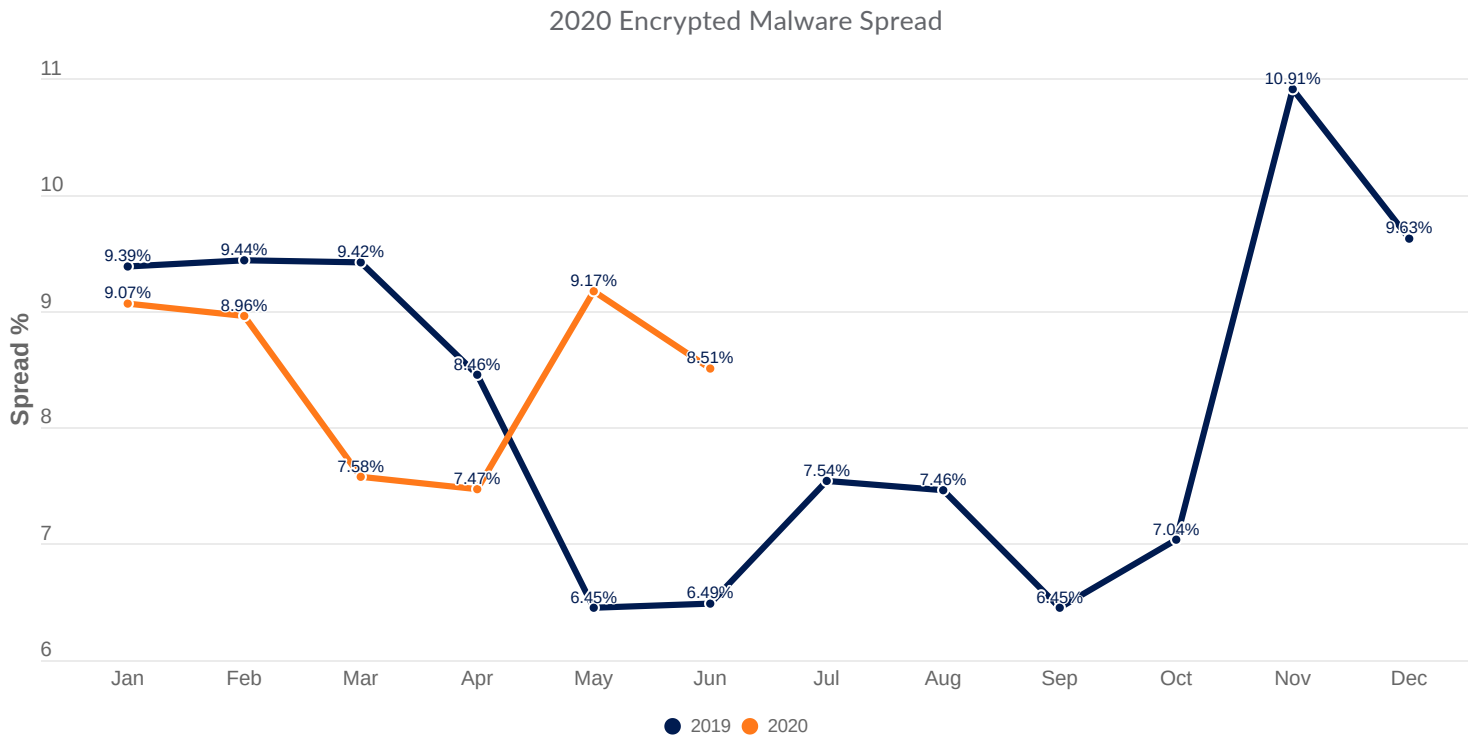
The more advanced endpoint security solutions will also feature automated 'rollback' controls to help administrators return a compromised device or machine to a safe state.

LAYER 7

SSL/TLS Decryption & Inspection

What better way to launch a successful attack than to hide it from discovery? Smart cybercriminals mask their attacks inside traffic encrypted by SSL/TLS standards. This helps them sneak malware by a single-layer network defense.

During the first half of 2020, a full 1 in 12 SonicWall customers with DPI-SSL turned on saw malware on encrypted traffic, according to the mid-year update to the 2020 SonicWall Cyber Threat Report. That's a growing attack vector that requires critical attention.



Source: *2020 SonicWall Cyber Threat Report*

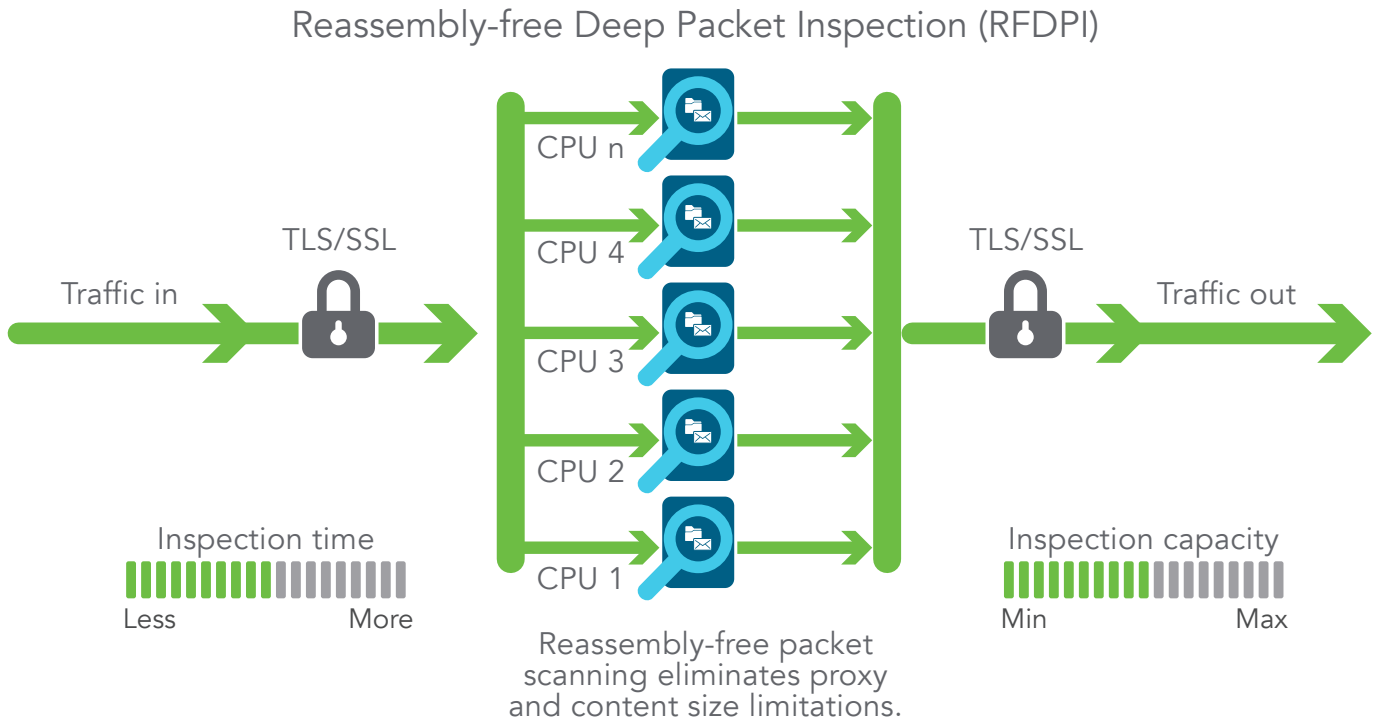
SONICWALL

The respected cybersecurity experts offer solutions to conscientiously decrypt, inspect and re-encrypt SSL and TLS traffic. For some, functionality is integrated on advanced firewalls. Other vendors sell dedicated SSL inspection appliances.

Also, be sure to ask whether the vendor offers full-proxy or artifact-based inspection. The former is expensive and slows performance, while artifact-based technology — like SonicWall's Reassembly-Free Deep Packet Inspection (RFDPI) — can stop more attacks without impacting speeds.

The approach that's sensible for your organization will depend on your particular performance, security deployment and financial objectives.

"Be sure to ask whether the vendor offers full-proxy or artifact-based inspection. The former is expensive and slows performance, while artifact-based technology can stop more attacks without impacting speeds."



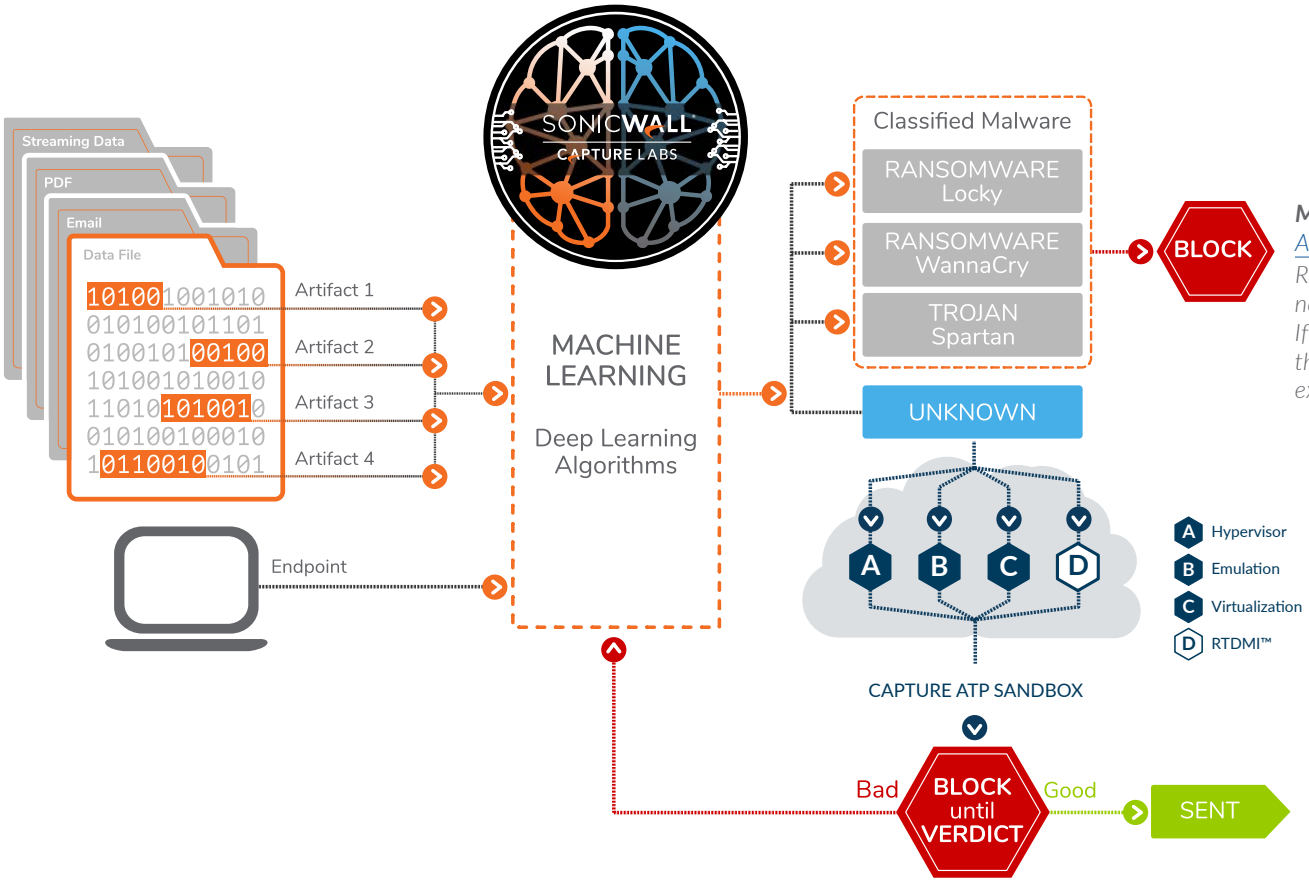
SONICWALL®

LAYER 8

Real-Time Sandboxing

The use of cloud or network sandboxing services complements the power of your firewall. This technology delivers real-time inspection of suspicious files that firewalls don't have a known signature to check against. Sandboxing should also be available across multiple avenues of attack, Next Generation Firewalls (NGFWs), endpoint, email and cloud application security, for example.

Cloud sandboxing is at its best identifying and blocking 'never-before-seen' attacks that are so new they cannot be stopped by static controls. Advanced sandboxes can isolate suspicious files for further analysis until a decision is determined — all in real time. This layer reduces the chance of breach or infection.



Multi-engine threat prevention. *The SonicWall Capture Advanced Threat Protection (ATP) cloud sandbox, with Real-Time Deep Memory Inspection™, stops unknown and never-before-seen attacks from compromising your network. If a threat is unknown, the multi-engine technology analyzes the malware until it can render a good or bad verdict — all executed in seconds.*

SONICWALL®

LAYER 9

Advanced Memory & Side-Channel Inspection

The most disturbing vulnerabilities — and potentially future attack vectors — are occurring at the processor level. Advanced side-channel threats, like MDS, Spoiler, Spectre, Meltdown, Foreshadow and PortSmash, are shifting the cyber war to an entirely new arena, which is extremely difficult to monitor or patch.

Soon, advanced organizations (e.g., nation-state attackers) could exploit processor vulnerabilities to access credentials and cryptography keys, potentially providing cyberattackers administrative access to full systems, networks or devices.

Innovative security vendors offer advanced deep memory inspection technology that identifies and stops both malicious PDFs and Office files, but also defends against advanced processor-based attacks.

For example, SonicWall Real-Time Deep Memory Inspection™ (RTDMI) provides CPU-level instruction detection granularity (unlike typical behavior-based systems, which have only API/system call-level granularity) to detect malware variants that contain exploit code targeting processor vulnerabilities, including MDS, Spoiler, PortSmash, Foreshadow and more.

RTDMI protects organizations from processor and side-channels attacks and is included as a part of the SonicWall Capture Advanced Threat Protection (ATP) sandbox service. The table on the next page outlines the speed in which RTDMI detected these advanced threats.

SONICWALL®

Identifying Zero-Day Attacks in Real Time

(Before VirusTotal)

The SonicWall RTDMI engine looks inside multiple layers of packaging and obfuscation to find well-entrenched malware that conventional anti-malware solutions don't uncover. It identifies zero-day attacks in real time, often before they are listed in industry malware search portals.

- Based on data from VirusTotal, a market-leading malware repository, SonicWall is identifying never-before-seen malware variants a full 1.9 days before VirusTotal receives the samples. In some cases (see table below), SonicWall is discovering new threats months before samples are submitted.
- In early 2019, RTDMI detected a surge in archive files containing an obfuscated JavaScript file that used PowerShell.exe to execute a downloader that downloaded a variant of the popular ransomware family GandCrab. This complex threat had not been posted on any of the popular threat intelligence portals.

Vulnerability	Publically Announced	RTDMI Detection Confirmed
Meltdown	1/3/2018	1/30/2018
Spectre	1/3/2018	6/13/2018
Foreshadow	8/14/2018	8/15/2018
PortSmash	11/2/2018	11/15/2018
Spoiler	3/5/2019	3/5/2019
MDS (ZombieLoad, RIDL, Fallout)	5/14/2019	5/15/2019
TPM-FAIL (CVE-2019)-11090)	11/12/2019	1/7/2020

LAYER 10

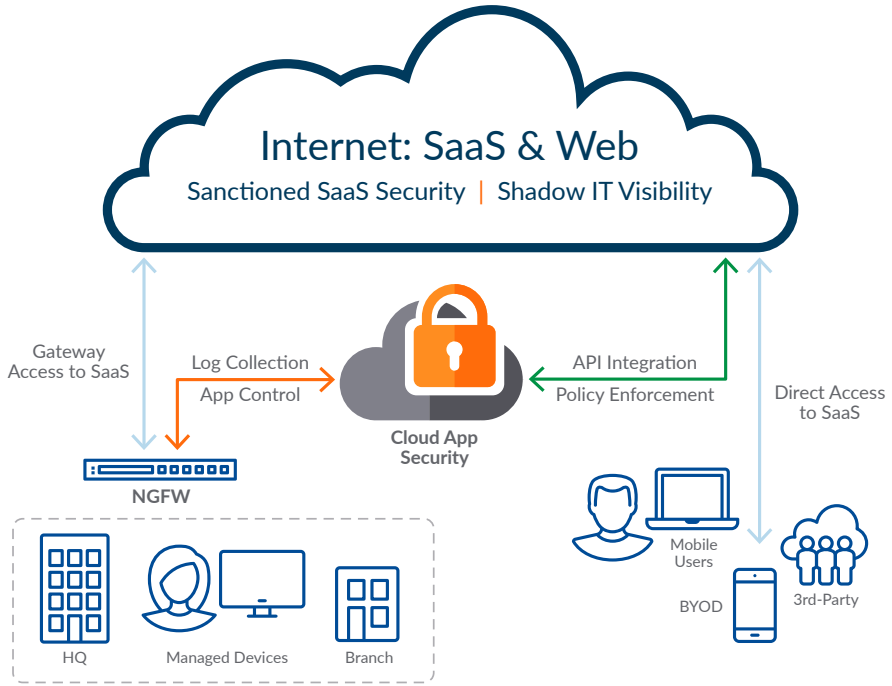
Real-Time Security for Cloud Apps & Services

Shadow IT is a growing risk for many organizations. Employees often don't have ill intentions and just want to complete their work, but nevertheless they can introduce unverified or untested applications or services into your network, leaving your organization vulnerable.

That's where cloud application security (CAS) solution comes into play. This type of solution plays a critical role in discovering and managing SaaS applications, including Office 365 and G Suite.

The solution should seamlessly integrate with the sanctioned SaaS applications using native APIs, providing: visibility, and compliance monitoring and auditing.

The approach empowers IT departments to roll out SaaS applications without compromising security and compliance. Administrators can set consistent policies across all the SaaS applications deployed within the organization from a single console. From there, they can use available DLP and compliance reporting templates to quickly close security gaps and set custom policies to fulfill business and regulatory needs.



SONICWALL®

LAYER 11

Next-Generation Firewalls

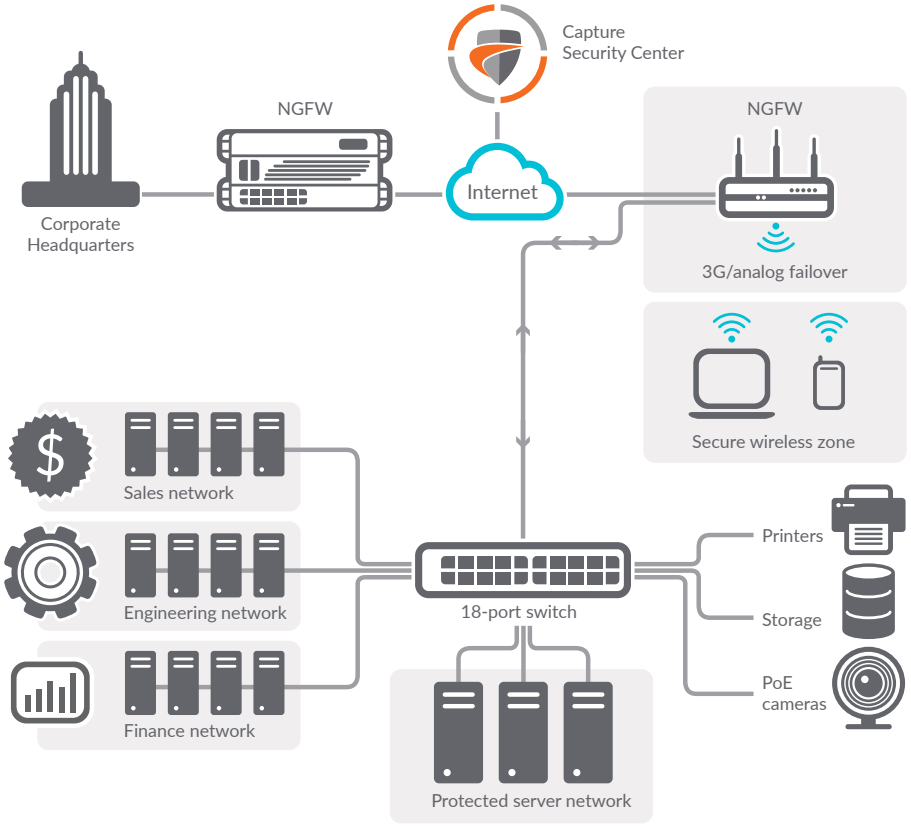
Next-generation firewalls (NFGW) are the massive, foreboding walls that defend your traditional core network. When properly deployed, next-generation firewalls are tremendously successful at stopping known cyberattacks.

When shopping for firewalls, consider the services that go with it. The firewalls itself will be labeled with various speed specifications, ports, power supplies, expansion modules, etc., but the true differentiation is often found in the accompanying security services.

Be sure to review each vendor for their offerings around SSL/TLS inspection, protection for non-standard ports, cloud sandboxing, gateway antivirus (GAV), intrusion prevention services (IPS), content filtering, anti-spam features and application controls — all of which should be consider the sub-layers of your security posture.

For distributed organizations requiring advanced flexibility in their network design, SD-WAN technology is a perfect complement firewalls deployed at the headquarters or at remote and branch sites.

Instead of relying on more expensive legacy technologies such as MPLS and T1, organizations using SD-WAN can choose lower-cost public internet services while continuing to achieve a high level of application availability and predictable performance.



The workhorse of network security. *Firewalls serve as the backbone to many security deployments. In this example, an enterprise uses next-generation firewalls to protect a wide range of assets, including endpoints, remote networks and locations, servers, IoT devices and more.*

SONICWALL®

Know Your Business for Optimal Security Effectiveness

Every business and organization is different. And many are at different phases of their path toward a sound, layered cybersecurity posture.

The aforementioned layers serve as a strong bedrock and will drastically reduce vulnerability gaps and mitigate even the most advanced cyberattacks — protecting your business, customers and brand.

While this overview has been focused on technology, it's important organizations also implement consistent processes to ensure policies are being adhered to, compliance mandates are followed, and the outlined security protocols are being monitored and enforced. A lapse in any drastically reduces the effectiveness of the preceding core layers.

"It's important organizations also implement consistent processes to ensure policies are being adhered to, compliance mandates are followed, and the outlined security protocols are being monitored and enforced."

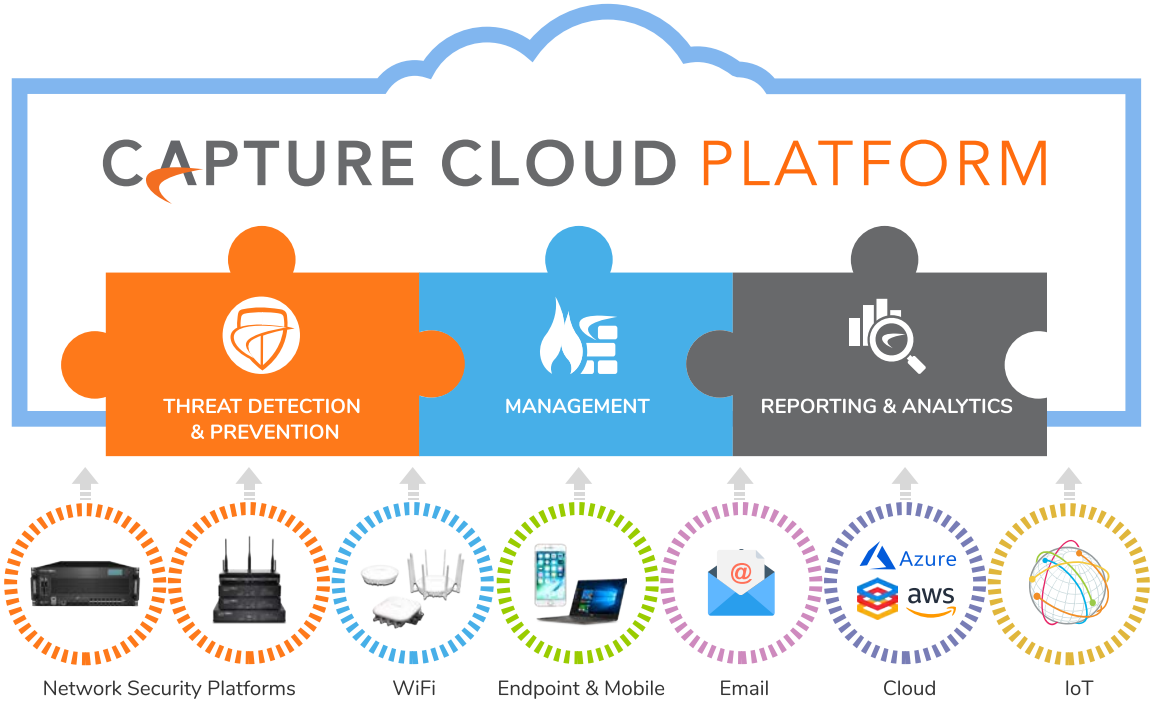
SONICWALL®

Best Practice: Automated Real-Time Breach Detection & Protection

The modern organization exists in an increasingly complex and globally connected world. Cybersecurity technology is both an enabler and inhibitor as organizations adapt to this rapidly changing environment.

As security technologies and the cyber threats evolve, a new cyber arms race has emerged, which places cloud-forward organizations and their cybersecurity solutions in the crosshairs of a growing global cybercriminal industry.

To protect your business, it's strongly suggested you avoid siloed security technology. In those scenarios, you'll spend more time integrating, configuring and managing the technology than you will actually stopping attacks and improving defenses. Instead, opt for a cohesive, unified platform that meets the specific security needs of your organization.



Unified and orchestrated cybersecurity. *The SonicWall Capture Cloud Platform tightly integrates security, management, analytics and real-time threat intelligence across network, email, mobile and cloud security offerings.*

SONICWALL®

SonicWall developed the Capture Cloud Platform to provide automated breach prevention and enable organizations like yours to stay ahead in the cyber arms race. The platform delivers security, management, analytics and integrated threat intelligence so you can:

- Drive end-to-end visibility and share intelligence across the unified security framework
- Proactively protect against both known and unknown threats
- Get the contextual awareness needed to detect and respond to security risks with greater speed and accuracy
- Make informed security policy decisions based on real-time and consolidated threat information

The Capture Cloud Platform strategy and vision for the future is continuous innovation and development of containerized as-a-service security applications that are easily programmable and provisioned on-demand to drive constant business value and ensure the long-term success of your organization.

SONICWALL®

Need A Security Consultation?

SonicWall has been fighting the cybercriminal industry for over 28 years, defending small- and medium-sized businesses and enterprises worldwide. The combination of our products and partners enables us to deliver a real-time cyber defense solution tuned to the specific needs of your business. This means more business and less fear for our customers.

If you'd like an assessment of your security strategy, or have specific questions about the SonicWall Capture Cloud Platform, call us at +**1-888-557-6642** or contact one of our cybersecurity experts. Or you can visit SonicWall.com to chat with a live representative.

CONTACT A SECURITY EXPERT

SONICWALL®

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era in a work reality where everyone is remote, mobile and unsecure. SonicWall safeguards organizations mobilizing for their new business normal with seamless protection that stops the most evasive cyberattacks across boundless exposure points and increasingly remote, mobile and cloud-enabled workforces. 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 or follow us on Twitter, LinkedIn, Facebook and Instagram.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com