SONICWALL®

BLUEPRINT: MODERN LAYERED SECURITY

Mapping the Must-Have Security Layers to Proactively Defend Your Business

Introduction

The notion of layered security has been around since the early days of network defense. The ideology 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, the technology that powers this thinking evolves as attack vectors shift — sometimes at alarming speeds.

To help, SonicWall has prepared a layered approach to strengthen your security posture while keeping your business objectives a priority.

While there are different schools of thought on which layers are most important (e.g., logical, most critical, easiest to implement, etc.) this blueprint offers a top-down look at the vulnerability gaps 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

SONICWALL®

LAYER 1

Security Awareness

It's cliché in the security and technology industries, but humans truly are the weakest link in the security change. Thus, it's no surprise that phishing and other social-engineering attacks have been so successful for so long.

But people can change. It does, however, require a top-down culture shift driven from the C-suite. Once each and every employee make cybersecurity their own responsibility, the organization is safer against potential cyberattacks that exploit human behavior or curiosity.

Security awareness should include:

- Consistent and always-evolving training to continue to educate staff
- 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 ramifications for non-compliance
- Using established best practices and training in the real world (e.g., 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

The use of email — particularly in business settings — is unavoidable. Because of this commonality, it remains one of the top attack vectors for cybercriminals, which leverage a salvo of phishing attacks and business email compromise (BEC) campaigns.

While commonplace at most security-conscious organizations, a secure email solution is still a necessary layer to ensure businesses are able to defend against email-based threats, including malware, ransomware, zero-day threats, spear-phishing and BEC.

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

Thankfully, a range of deployment options are available, including on-premise appliances to cloud 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 malicious attachments and URLs, as well as impostor-based attacks.

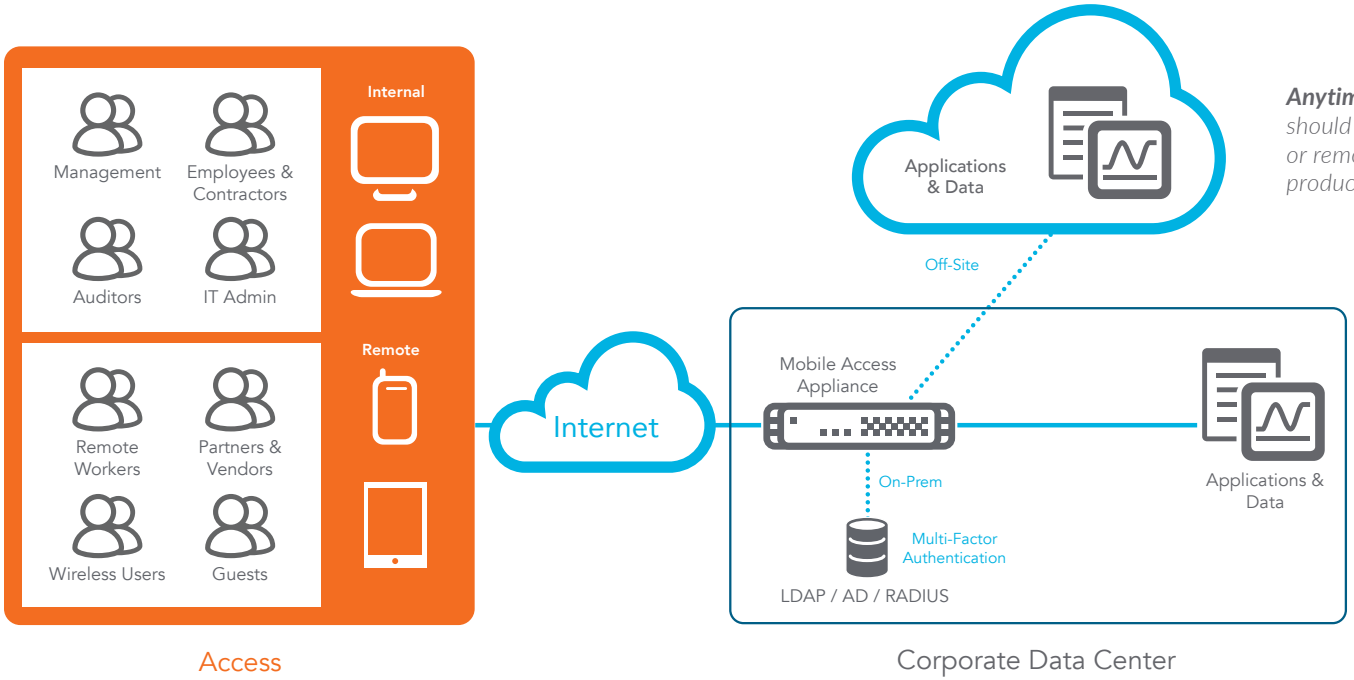
SONICWALL®

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.

Advanced secure mobile access solutions, including virtual private networks (VPN, will ensure your users have access to the networks, applications and data they need — any time and from anywhere. Hindering this access diminishes productivity, gives rise to shadow IT and creates security gaps.



Anytime, anywhere access. *A robust layered security strategy should include capabilities to support and empower mobile or remote users outside the corporate network to accelerate productivity and reduce IT management overhead.*

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 have used on other unknown wireless networks.

Both scenarios can present new risks that should be identified and stopped by sound 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, 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.

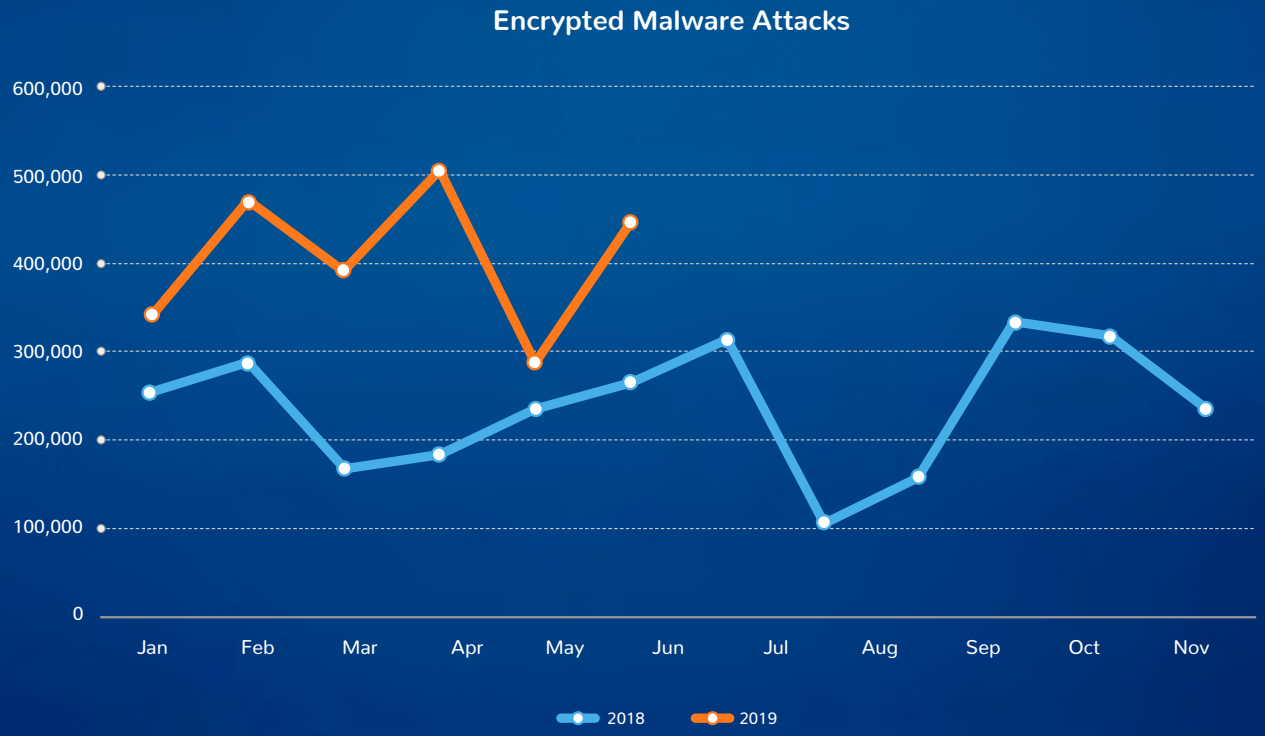
The more advanced endpoint security solutions will also feature automated 'rollback' controls to help administrators return a compromised device or machine to a safe state.

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.

Through June 2019, encrypted attacks were up 76% year to date over the same time period in 2018 according to the mid-year update to the 2019 SonicWall Cyber Threat Report. That's a growing attack that requires critical attention.



Source: *Mid-Year Update | 2019 SonicWall Cyber Threat Report*

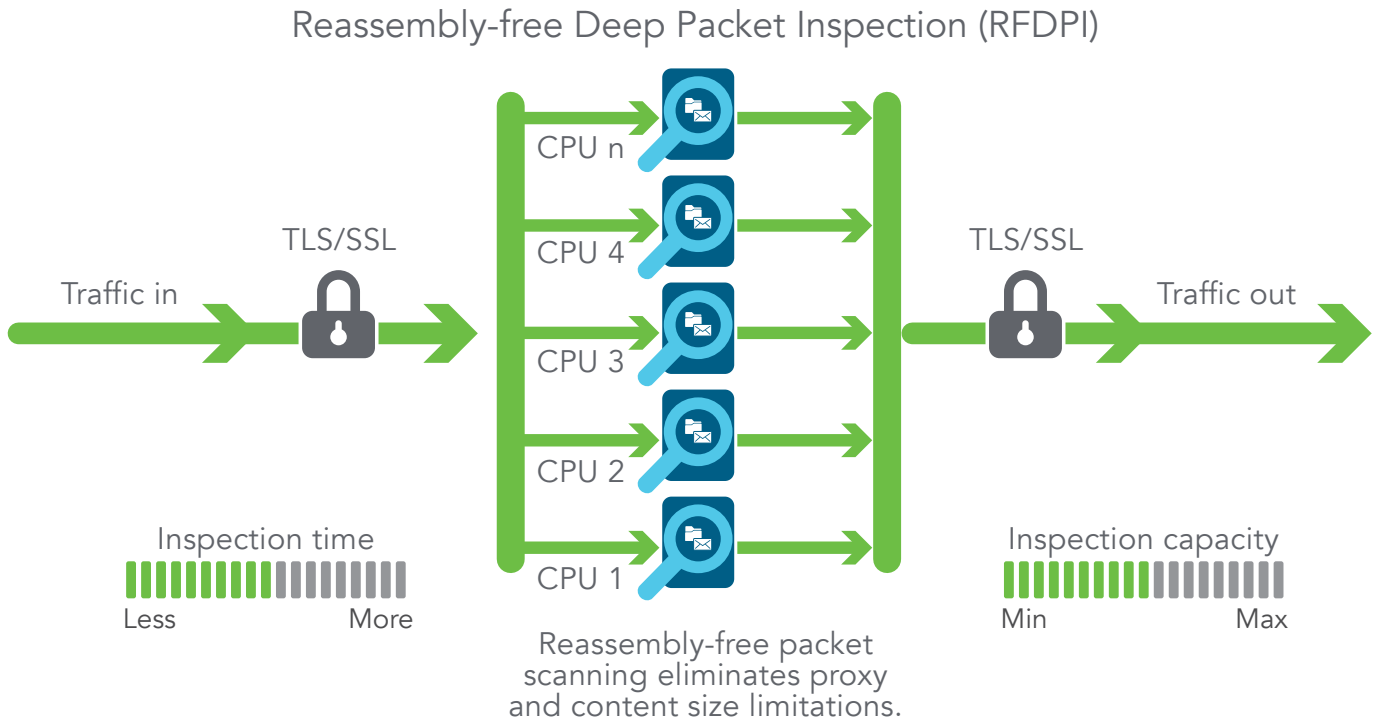
SONICWALL®

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."



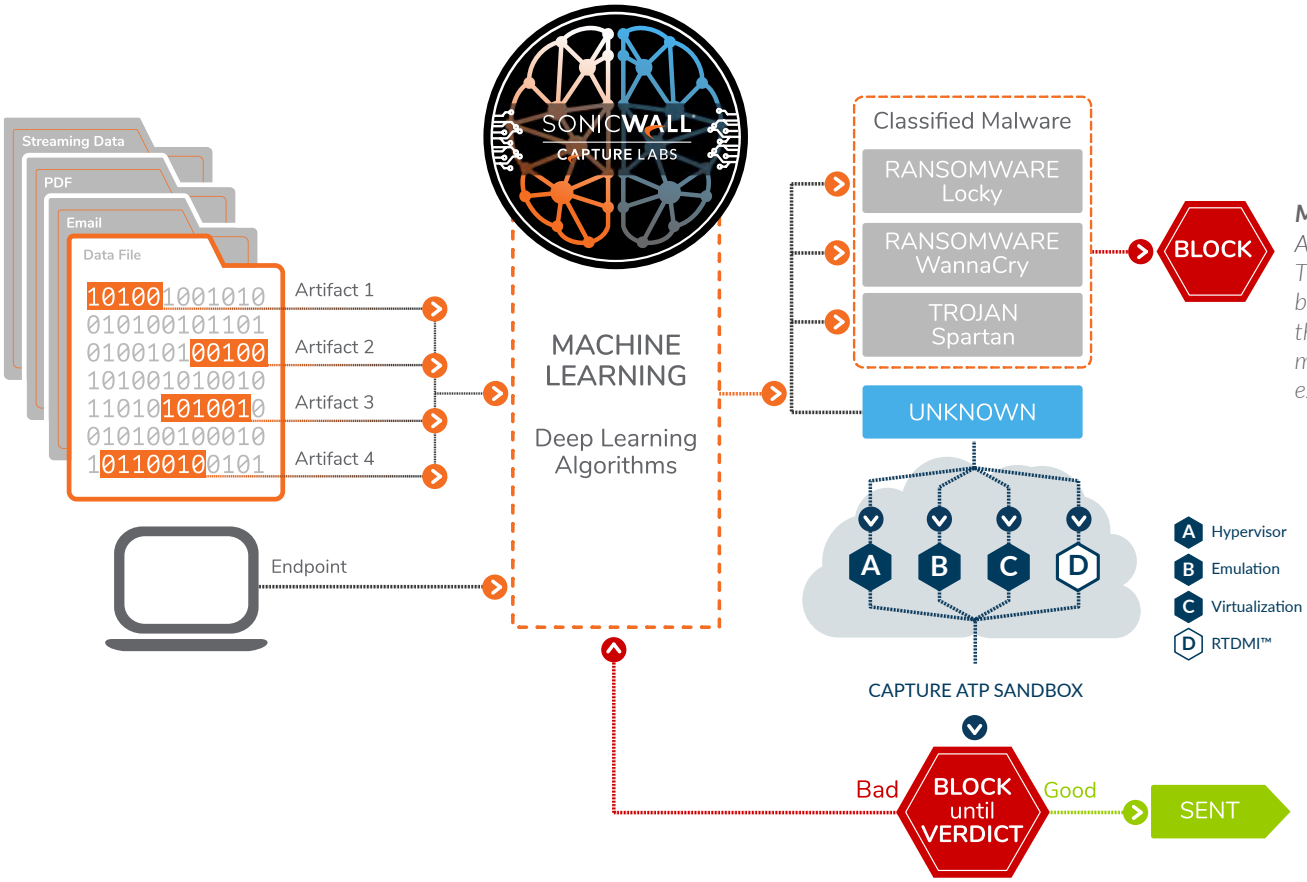
SONICWALL®

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, 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 are able to circumvent standard security 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., governments, nation-states 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.

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.

- In mid-2018, RTDMI identified a new malware campaign using malicious Microsoft Office document files. The files contained VBA macro code that decrypts a URL hidden inside an embedded form in the document and downloads a ransomware payload. SonicWall provided customers with a list of indicators of compromise (IOCs) immediately — before the threat was listed in VirusTotal or ReversingLabs.
- 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	Announced	RTDMI™ Detection Availability (Production)	RTDMI™ Detection Confirmed
MDS (ZombieLoad, RIDL, Fallout)	5/14/2019	5/23/2019	5/15/2019
Spoiler	3/5/2019	6/13/2018	3/5/2019
PortSmash	11/2/2018	6/13/2018	11/15/2018
Foreshadow	8/14/2018	1/30/2018	8/15/2018
Meltdown	1/3/2018	1/30/2018	1/30/2018
Spectre	1/3/2018	6/13/2018	6/13/2018

LAYER 10

Real-Time Security for Cloud Apps & Services

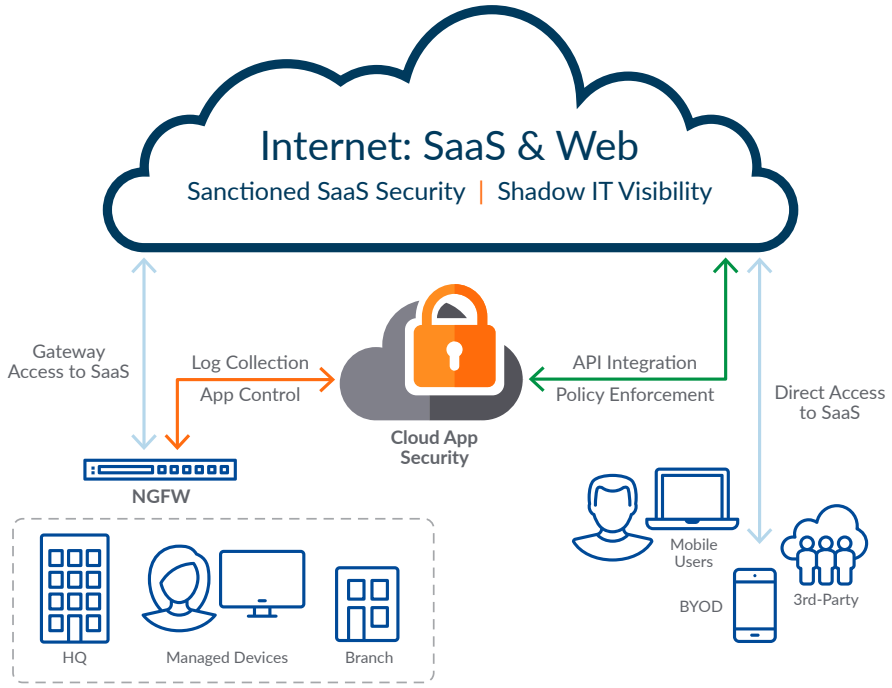
Shadow IT is a growing risk for many organizations. Employees often don't have ill intentions and just want to complete their work, but nevertheless they can introduce unverified or untested applications or services into your network, leaving your organization vulnerable.

That's where a cloud access security broker (CASB) or cloud application security (CAS) solution come into play. This type of solution plays a critical role in discovering and protecting unsanctioned cloud services or applications, including Office 365 and G Suite.

The solution should seamlessly integrate with the sanctioned SaaS applications using native APIs, providing CASB functionalities: visibility, advanced threat protection, data loss prevention (DLP) and compliance.

When deployed with a next-generation firewall (NGFW), a cloud application security solution should also provide shadow IT visibility and control for cloud usage on the network.

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

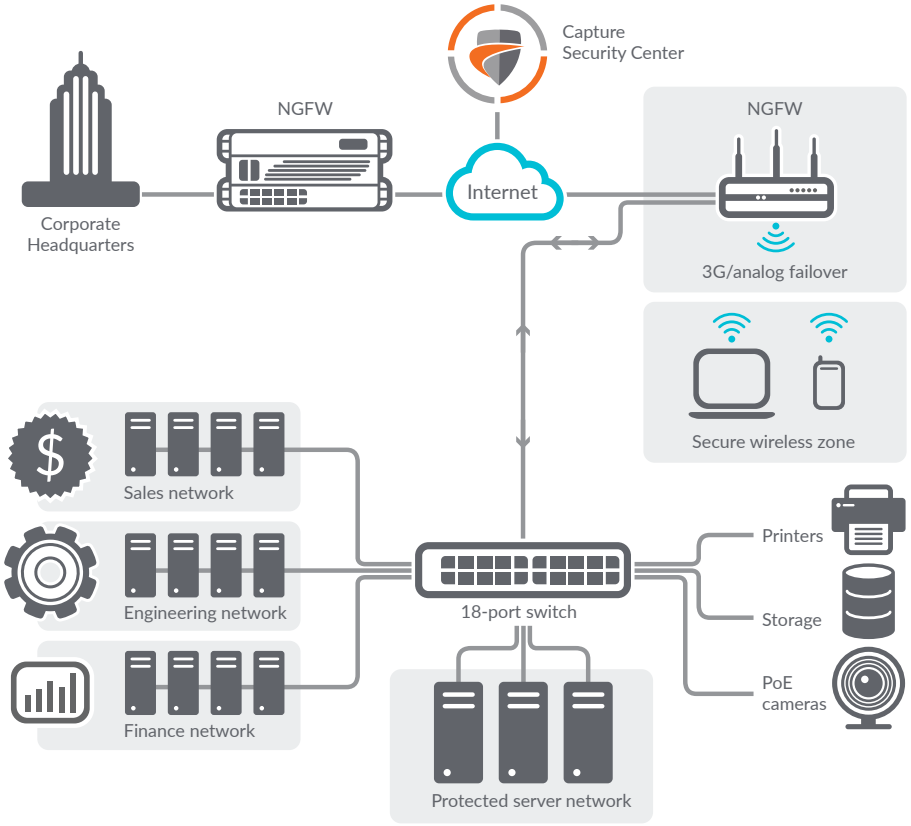
Next-generation firewalls (NFGW are the massive, foreboding walls that defend your traditional core network. When properly deployed, next-generation firewalls are tremendously successful at stopping known cyberattacks.

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."

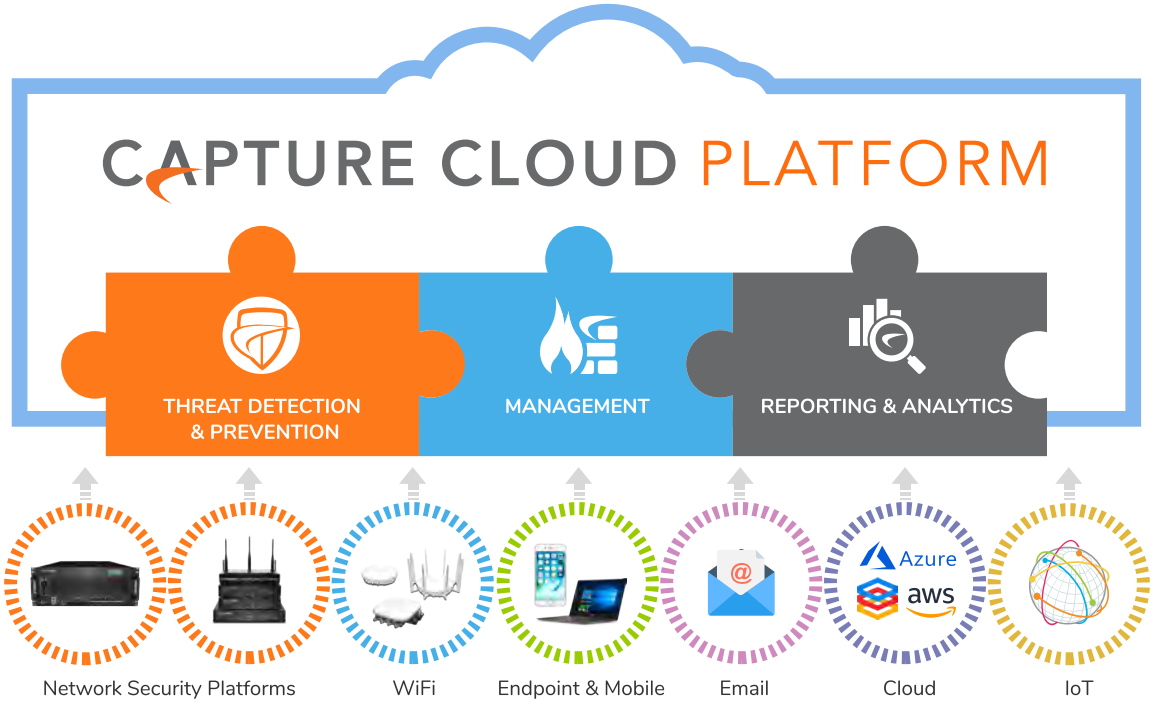
SONICWALL®

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.

SONICWALL®

© 2019 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 27 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award- winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security.

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

ZONES
First Choice for IT™

For more information, contact your Zones Account Manager, or call 800.408.ZONES.