SONICWALL®

Boundless Cybersecurity for a Safer Healthcare Industry

Keeping critical infrastructure available, data accessible and patients safe.

ABSTRACT

The increasing number of vulnerability disclosures — as well as risks associated with unpatched critical systems, web applications and Internet of Medical Things (IoMT) — is challenging Healthcare Delivery Organizations' (HDO) ability to defend against their most concerning threats. In addition, human error and resource constraints are compounding these challenges to aggravate an already difficult situation.

In this environment, what's the best way for HDOs to protect their care delivery systems to ensure patient welfare is never at risk? By adopting the SonicWall Boundless Cybersecurity approach, HDOs can stop worrying about a breach and concentrate on their more important mission: providing quality care and better clinical outcomes for their patients.

Executive Summary

Patient care is shifting from treating acute medical problems to a new model: fostering ongoing wellness and quality of life. This transition is significantly transforming healthcare operational norms: today, there are many digital health innovations helping make patient-provider engagements more interactive, personalized and flexible throughout the patient-care continuum.

It's also accelerated digital transformation and medical technology advancements that improve clinical workflows, help ensure the accuracy of patient diagnosis and prognosis of diseases, and bolster treatment success. Much of this is facilitated and enhanced by the growing therapeutic applications of IoMT and breakthroughs in AI-driven algorithms and machine-to-machine (M2M) communications in healthcare systems.

Because of the unique nature of healthcare's critical infrastructure, the diverse roles of its personnel, and the demand for anytime, anywhere access to medical records, protecting data and computer systems is a complex mission. So when security risks increase in every threat category, healthcare organizations must establish a boundless defense-in-depth approach that they can depend on when providing safe, reliable and uninterrupted patient care. This approach should map into healthcare cybersecurity three fundamental care-critical missions guided by the Confidentiality, Integrity, and Availability (CIA) Triad security model as the standard for:

1. Safeguarding the confidentiality and privacy of personal health information (PHI) against misuse.
2. Protecting the integrity of electronic health records (EHR) for patient safety.
3. Ensuring the availability of critical infrastructure and business operations with a defense in depth security approach.

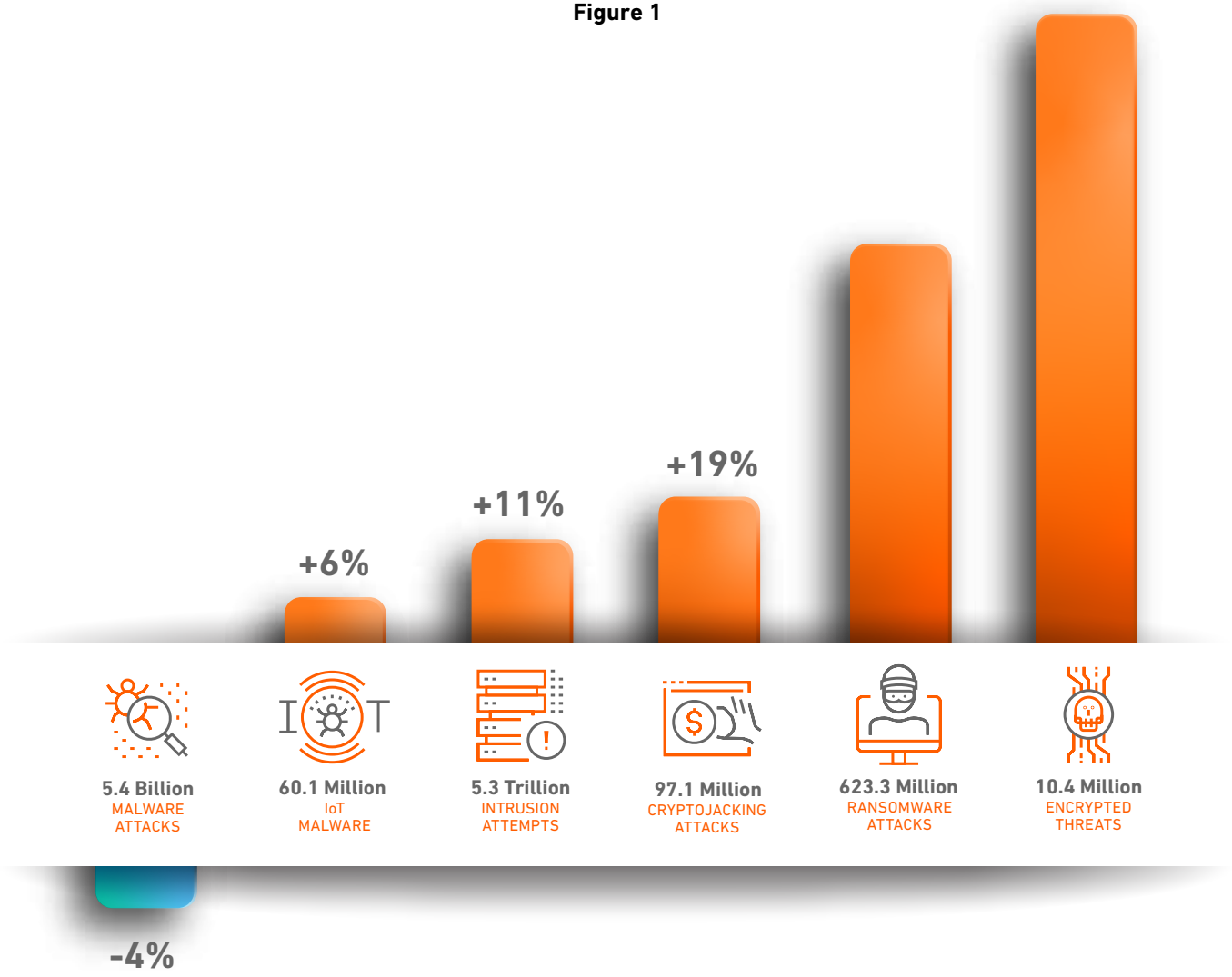
WHITE PAPER

Why Healthcare Needs a Boundless Connected Cybersecurity Approach

The increase in sophistication and frequency of cyberattacks continues to be a material risk. The security challenges HDOs collectively face are multi-dimensional (Figure 1).

SonicWall understands threats come in many different forms and are used by various threat actors who wish to do harm without regard for patient wellness. Whether socially, economically or politically motivated, the results of these attacks are the same: the loss of something of considerable value, such as PHI data or operational continuity, that puts patient lives at risk and providers out of business.

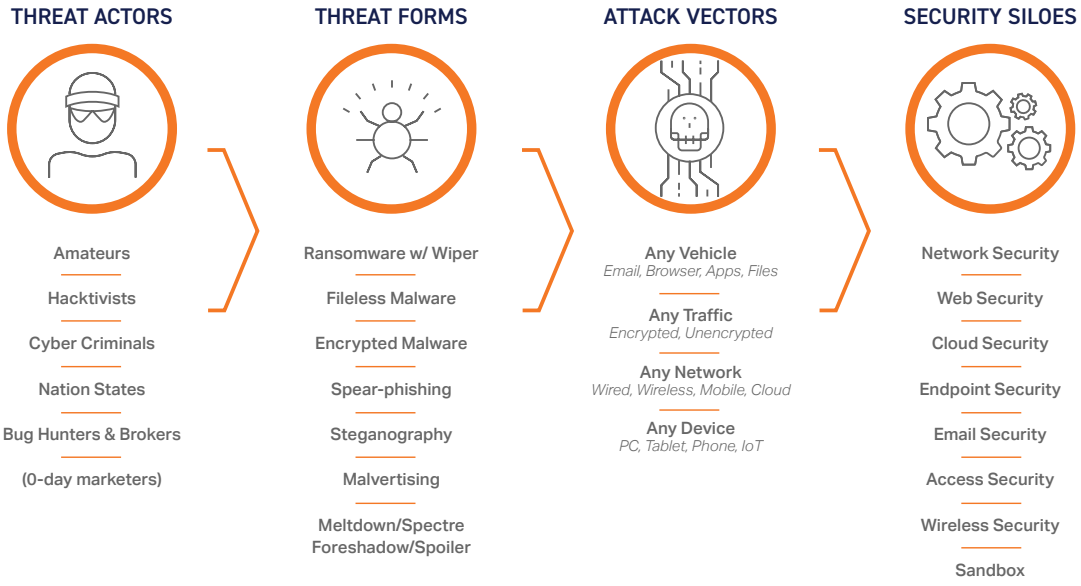
Figure 1



SONICWALL

Figure 2

Figure 3



The expansion of critical infrastructures and the proliferation of IoMT, mobile, wireless and cloud applications enlarge the attack surface with boundless exposure points (Figure 2). Threat actors can deliver ransomware using multiple attack vectors and hack your organization through any vehicle, traffic, network or device (Figure 3).

As cyber-defenses are a challenge at every enforcement point, from the endpoint to the network and the cloud, there has been a trend toward the proliferation of security tools pieced together to stop these threats. The resulting security tool sprawl is a big concern with regards to management, efficiency and cost. In addition, security teams with rigid lines of responsibilities and controls create security siloes, making it nearly impossible to work as a unified team. The less these units communicate with one another, the more threat intelligence is isolated.

For example, suppose one enforcement point managed to detect and record a new malware variant. If this critical information is not shared across other security controls in other areas of the network, those areas could remain vulnerable.

The danger behind unconnected security is that it creates a security system in which each independent enforcement point is only as strong as the weakest enforcement point in the collective defense. An integrated security system can aggregate information on threats and provide a more complete perspective on threat actors' Tactics, Techniques and Procedures (TTP), thus strengthening the overall security posture. A security system that is not interconnected can allow an attacker to succeed with multi-vector campaigns. To combat these attacks, healthcare organizations need a boundless, connected approach.

SONICWALL

Connected Defense-in-Depth Ensures Healthcare Availability

HDOs cannot afford extended downtime or abrupt interruption. That's why it's more important than ever to reevaluate your cyber defense systems as a whole when you're aiming to establish a connected security program consisting of multiple security tools. It is essential not only to examine the individual parts to see if they meet specific requirements, but also to ensure the entirety of the cybersecurity ecosystem is evaluated collectively to determine if the combination of tools meets all your objectives.

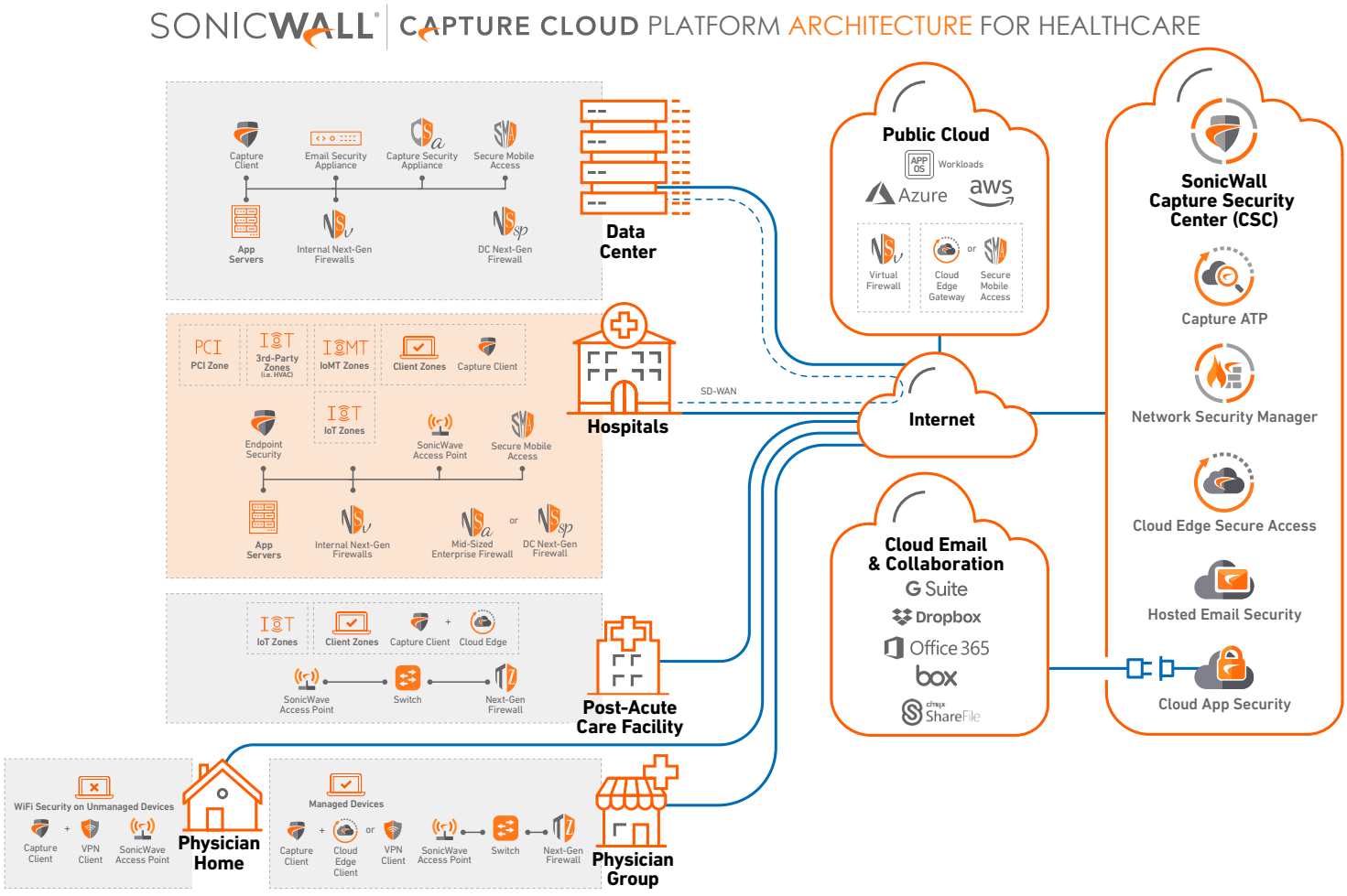
SonicWall understands these healthcare challenges firsthand through our ongoing collaborations with providers and managed service partners (MSP) serving the healthcare industry. Through those engagements, SonicWall Boundless Cybersecurity introduced the Capture Cloud Platform (CCP) to help HDOs quickly adapt and respond to cyberattacks and vulnerabilities using multiple countermeasure tools in an integrated, layered security approach.

The architectural reference diagram in Figure 4 gives you a high-level perspective of SonicWall's product portfolio inside the CCP. It illustrates where the individual part is positioned in the network to form one security system to protect the continuity of patient care. Every layer cross-shares its threat intelligence to bolster the overall security effectiveness against modern attacks. At the same time, CCP satisfies many of the required privacy and security controls defined in the NIST or HITRUST security framework.

The strength of this platform comes from the integration of three essential components:

1. Capture Security Center (CSC) with Unified Insights
2. SonicWall's Capture ATP with RTDMI™
3. Threat intelligence services of Capture Labs and Capture Threat Network

Figure 4

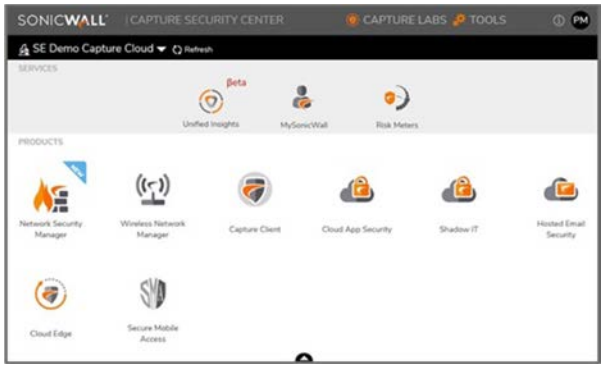


SONICWALL

Ecosystem Architecture Produces Healthier Healthcare Cybersecurity

SonicWall Capture Security Center establishes an ecosystem architecture that merges SonicWall solutions, forming a single integrated cyber-defense stack to help ensure a safer healthcare industry. In addition, it provides single sign-on (SSO) access to a cloud management interface where security admins can administer all security controls centrally from one easy-to-use cloud console (Figure 5).

Figure 5



Common management workflows and processes across network, endpoint, cloud, wireless, web, email, mobile and IoT security solutions reduce management complexities and administrative overhead. Security posture significantly improves from a federated defense and shared intelligence across a unified security framework. Moreover, analysts and incident responders gain deeper visibility into actionable analytics for proactive threat mitigation using CSC Unified Insights, a single-pane dashboard providing security insights across firewalls, wireless, and endpoint security products.

Accelerate Time-to-Insights, Reduce Healthcare Risks

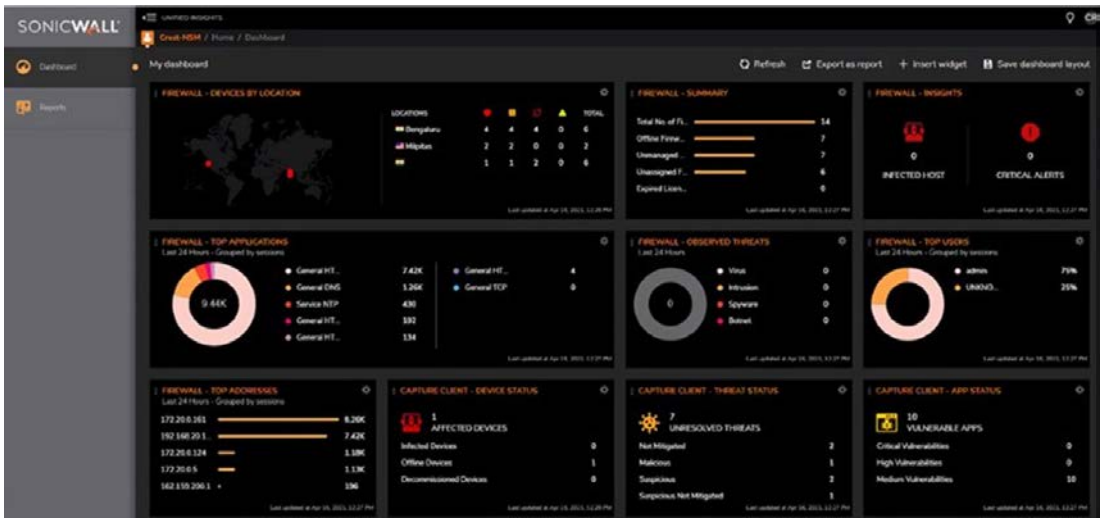
The healthcare industry is fighting a never-ending cyber tug-of-war. When bad actors develop something new, good guys quickly counteract. However, the gap in the response time for this typical scenario always puts healthcare SOC at a considerable disadvantage. Security admins are drowning in large data volumes from disparate cybersecurity products, leading to severe data fatigue and even costly oversight. Not having the capabilities to get to the correct information or stay on top of critical events further exacerbates the matter, resulting in organizations being exposed to otherwise preventable security risks.

Unified Insights integrates into Capture Security Center's single-pane-of-glass cloud management interface as a value-add service, with no additional cost or licensing requirement. Its mission is to provide security admins with the power of centralized intelligence and global incident response by coalescing action-focused analytics from SonicWall firewall, wireless and endpoint security products into a single dashboard for central monitoring and troubleshooting (Figure 6).

It accelerates time-to-insight by providing intuitive visualizations across large data volumes, giving security stakeholders a top-down understanding of their security posture. But it also allows deep exploration into datasets, allowing incident responders to take corrective actions, tune security policies, and fix any problems they discover quickly and with greater accuracy.

Download the Capture Security Center Unified Insights datasheet for more detail.

Figure 6

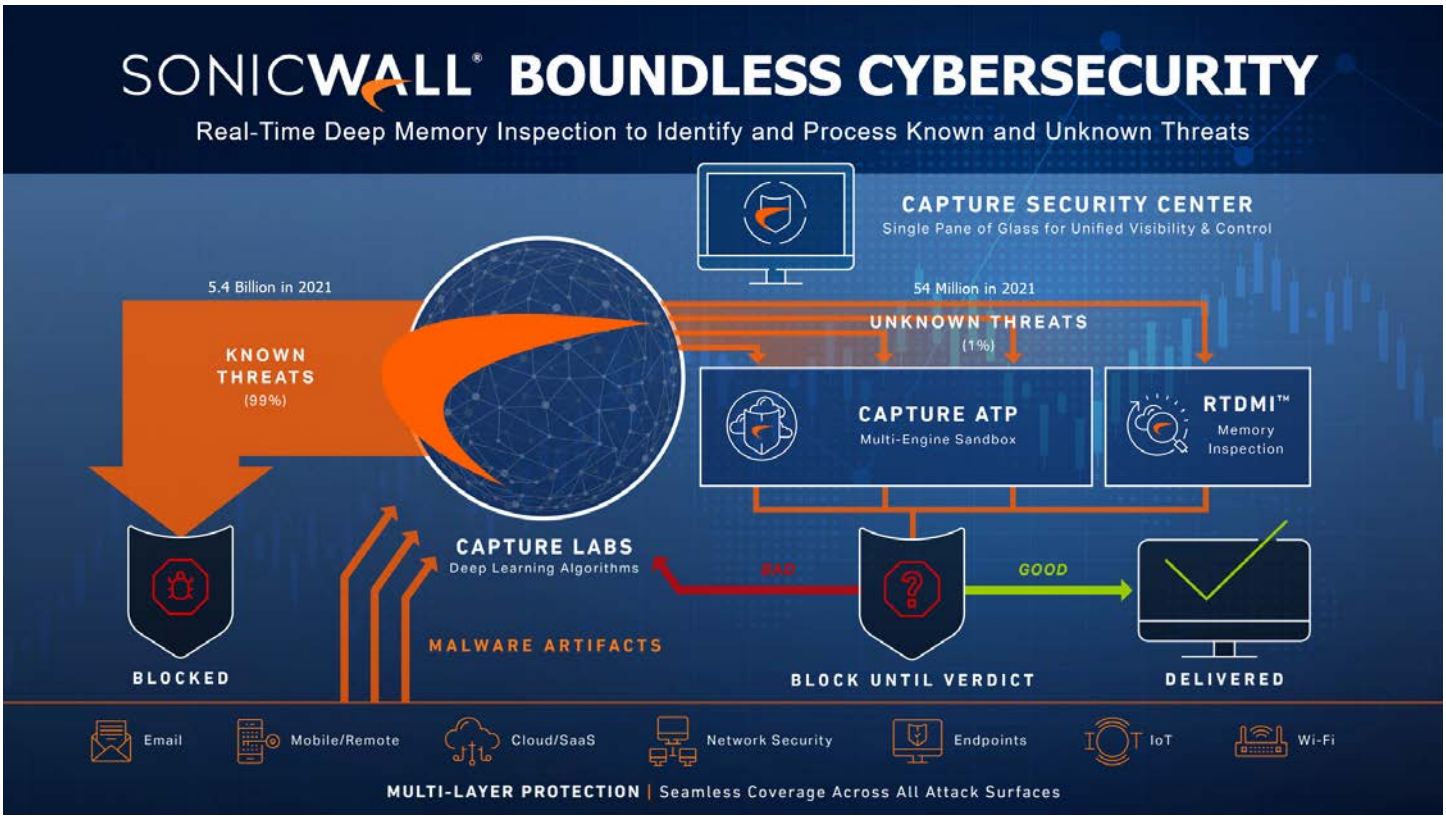


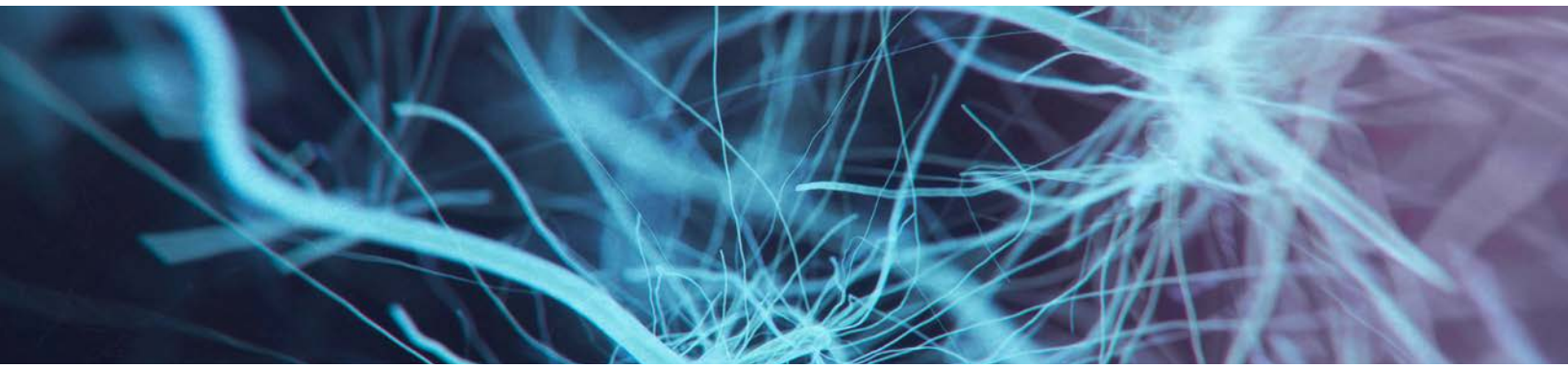
Capture ATP with RTDMI Keeps Ransomware Out Everywhere

Capture ATP is central to the SonicWall Capture Cloud Platform, working seamlessly across the entire SonicWall security stack for synchronous threat management. This security service is the industry's first award-winning solution that applies multiple sandboxing technologies, including SonicWall's patented Real-Time Deep Memory Inspection (RTDMI™), full system emulation and virtualization techniques to combat zero-hour threats. In addition, each sandbox engine performs deep behavioral analysis of suspicious code to unmask more never-before-seen ransomware variants than competing single-engine sandbox solutions.

Today's advanced malware contains built-in anti-forensic capabilities to effectively counter sandbox detection. But such tactics don't fool RTDMI™, which analyzes suspicious files in memory, where malicious intent and activities are revealed. It sees through all the delay, obfuscation and encryption techniques that modern malware may deploy to evade sandbox analysis, and yields extremely high-accuracy, low-false-positive detection of ransomware attacks — regardless of whether they come directly over the internet or are embedded in documents, executables, archive files or other file types.

Figure 7





Capture ATP with RTDMI™ is available as a security service subscription for SonicWall firewall, endpoint, email, access and wireless products, or as the standalone Capture Security appliance (CSa).

CSa provides an on-premises deployment option for healthcare organizations, satisfying data compliance laws forbidding the transmission of any healthcare-related files to a cloud service for threat analysis. It's also ideal for organizations that wish to run a closed network, without any direct connection to the internet, in order to ensure privacy data are unthreatened.

Synchronous Threat Management Elevates Healthcare Defenses

Capture ATP with RTDMI™ leverages threat data from sources such as reputation, static analysis and global hash checks across the threat intelligence industry, allowing it to deliver quick verdicts. SonicWall collaborates and shares threat intelligence with over fifty industry research organizations. We then combine that with threat feeds collected from over one million SonicWall security sensors transmitting home from around the globe to the SonicWall Capture Threat Network to prevent follow-on attacks from newly identified threats.

Healthcare organizations will benefit from the fact that these sensors act as a massive threat intelligence network. Once never-before-seen malware and ransomware variants are identified, they are used to create signatures for one part of the defense chain and subsequently benefit all other parts of the SonicWall layered defense ecosystem in real time. The entire process happens very quickly, reducing the exposure window across your environment and preserving the safety and availability of healthcare data, critical infrastructure and business operations.

Figure 8

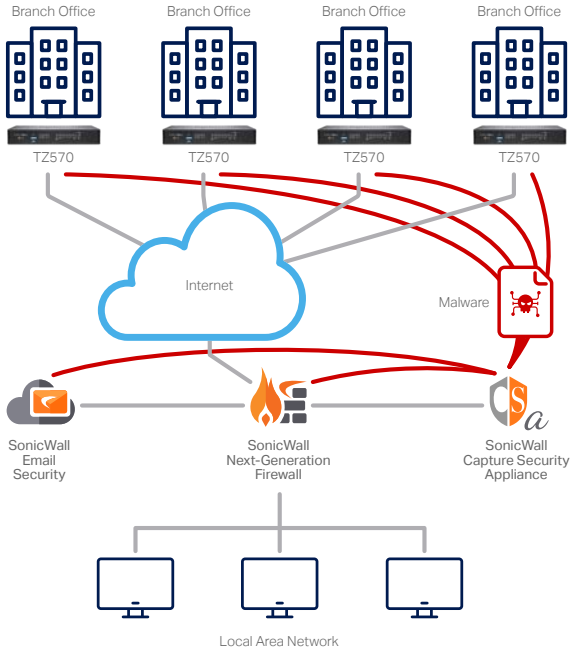


Figure 9

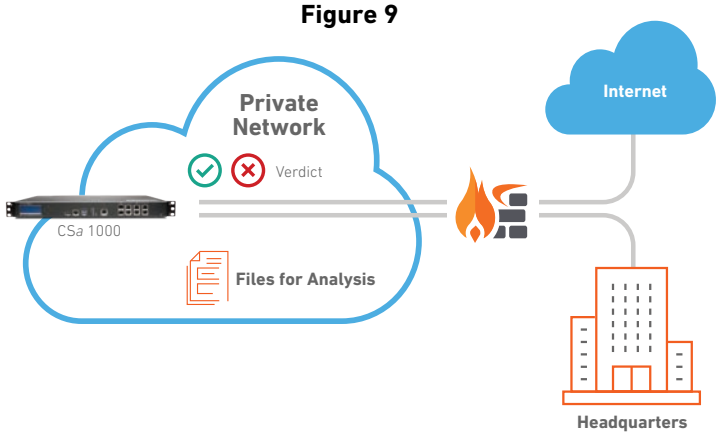
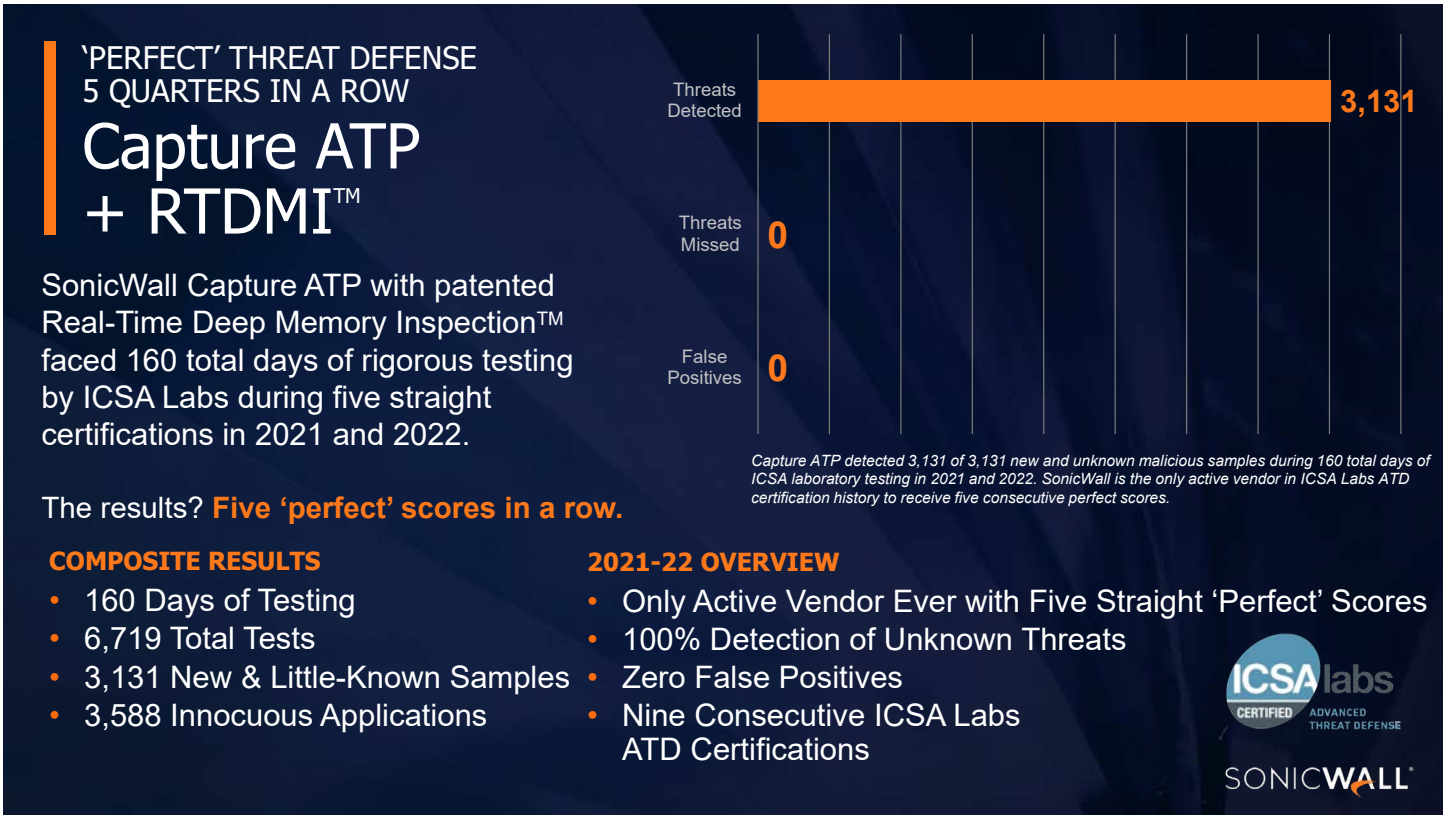


Figure 10



Perfect Threat Defense

To demonstrate how Capture ATP with RTDMI™ continue to deliver on its promises, SonicWall subjects the technology to continuous independent third-party validation. For the entirety of 2021 and into 2022, SonicWall Capture ATP maintained a perfect score in ICSA Labs Advanced Threat Defense (ATD) testing. In other words, over 160 days of continuous testing and 6,719 total test runs, consisting of 3,131 new and little-known threats and 3,588 innocuous applications, SonicWall identified 100% of the threats without triggering a single false positive on any of the innocuous apps.

SonicWall is the only active vendor in ICSA Labs ATD history to attain five consecutive perfect scores. To learn more about SonicWall's ICSA testing results, download our solution brief, "Perfecting Security Efficacy: SonicWall Sets New Standards for Threat Protection."

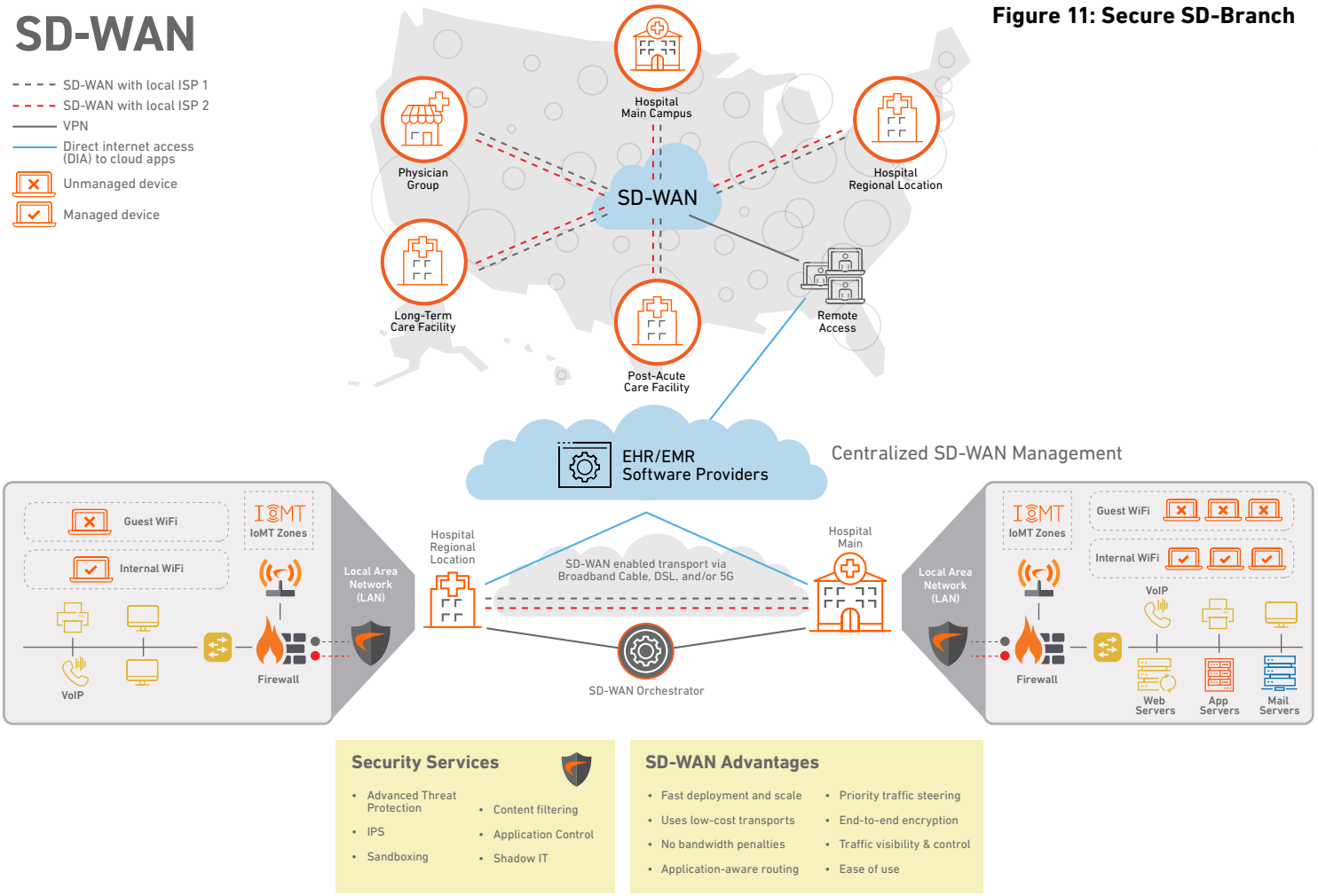
Always-on Secure Connectivity and Security Everywhere Healthcare

Network connectivity, availability and uptime are critical functions of a thriving healthcare operation. When these functions work, professionals can conduct care from multiple locations, including hospitals, private clinics, urgent centers and post-acute care facilities. And with telehealth, this list expands to include the home office or anywhere that personal mobile devices can achieve connectivity. On-demand, instant access to clear voice and video sessions for virtual visits, medical-enabling systems and patient information gathering is fundamental to enhancing the care experience.

As healthcare mergers and acquisitions continue to increase, however, so does complexity. In these cases, network capacity and connectivity must scale to support the merging of multiple healthcare-critical infrastructures to ensure services, communication and access are not interrupted. Any sudden loss or degradation of network connectivity has severe implications across patients, payers, providers and issuers. There is no time for downtime in healthcare, because losing access to remote health monitoring devices during intensive care recovery or radiology and lab results before a surgery delays life-saving intervention and treatment, leading to poorer outcomes.

Healthcare organizations need a more intelligent and cost-effective way to build a dependable WAN environment to support their growth and cloud transformation. SonicWall Secure SD-WAN is a key technology enabler to the larger SonicWall Secure SD-Branch approach. Secure SD-Branch combines SD-WAN capabilities with NGFW, wireless access points, secure switch and standard management tools to deliver consistent security controls and unfailing SD-WAN connectivity.

Figure 11: Secure SD-Branch



With Secure SD-WAN service, healthcare organizations can quickly and easily build or onboard new branch locations with affordable SD-WAN connectivity. New medical offices, clinics, hospitals, physician groups and urgent centers can now safely communicate over encrypted connections using low-cost public internet services instead of more-expensive MPLS circuits. Additionally, the service can add new bandwidth-intensive apps without worrying about poor performance or availability, because the service can scale quickly. So medical workers get direct, secured and reliable access to on-prem and cloud applications and resources for better performance and care experience.

The Secure SD-WAN service is available on all SonicWall NGFWs and centrally administered by SonicWall Network Security Manager (NSM), a cloud-native unified firewall management system. The service has inherent security integrated into the intelligent operating software running on every SonicWall firewall model. Adding security services, such as Capture ATP with RTDMI™, intrusion prevention system (IPS), gateway anti-virus, content filtering, application visibility and control, and shadow IT discovery and management further strengthen healthcare cybersecurity across all care delivery locations.

Securing traffic across distributed networks has been a core competency SonicWall has brought to customers for more than thirty years. The security stack within the SonicWall Capture Cloud Platform architecture protects all traffic traveling between sites and the cloud. So when healthcare adds new facilities to the network, SonicWall NSM enforces consistent security policies and applies zero-touch and SD-WAN orchestration workflows to bring up those sites quickly and securely.

Benefits of SonicWall Secure SD-Branch:

Business Benefits

- Business agility and speed
- Low risk of business disruption
- Business-critical applications never slow down or shut off
- Better user experience
- Big savings with lower connectivity costs

Operation Benefits

- Fast and easy deployment
- SD-WAN Orchestration
- Reliable and resilience connectivity
- Multi-path selection
- Deterministic application performance
- Applications always operating at peak performance

Security Benefits

- End-to-end encryption
- Enable all necessary security services to all SD-WAN traffic
- Catch new ransomware variants before entering the network
- Application visibility & control

Best to Err on the Side That All IoMT Are Vulnerable

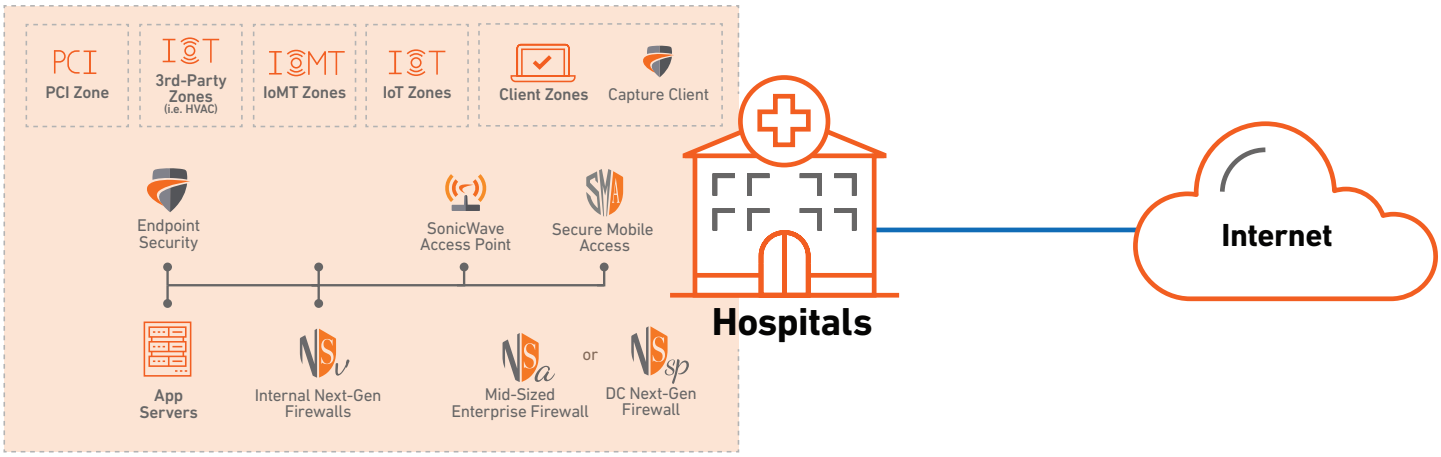
The expanding footprint of connected medical devices adds to the growing number of exposure points for healthcare cybersecurity. Vulnerability disclosures affecting IoMT have been growing strongly in recent years. So when and where these devices are connected can become open backdoors if they are not responsibly managed and promptly patched. Failing to keep a good inventory of all these devices can add significant security risk to an already stressful cybersecurity situation. Regulators like the U.S. Food and Drug Administration (FDA) put full responsibility on healthcare to ensure IoMT does not become weaponized to bring down critical infrastructure and harm patients.

SonicWall recommends treating every IoMT device as a potential risk to most efficiently combat this threat. Therefore, their connectivity must be isolated to dedicated network zones for segment-based security controls.

SonicWall next-generation firewalls (NGFW) can organize network resources into different segments and regulate traffic between those segments to keep the broader infrastructure safe. By controlling traffic to and from those devices and security zones, the threat of a beach is restricted to the zone to which compromised devices are connected.

Additionally, the NGFW can enforce segmentation restrictions based upon dynamic criteria, such as user identity, geo-IP location and medical devices' security stature. It can also integrate multi-gigabit network switching into its security segment policies and enforcement, direct those policies to traffic at switching points throughout the network, and globally manage segment security enforcement from a single pane of glass.

Figure 12



SONICWALL

Zero-Trust Is Reshaping Access Security for Safer Anytime/Everywhere Care

The digital transformation journey for healthcare had already gained tremendous momentum when COVID-19 threatened the wellness of the entire human race. Overnight, the pandemic began reshaping the future of healthcare services, expanding the front lines of healthcare at scale and flexibly connecting providers with patients outside of traditional care facilities.

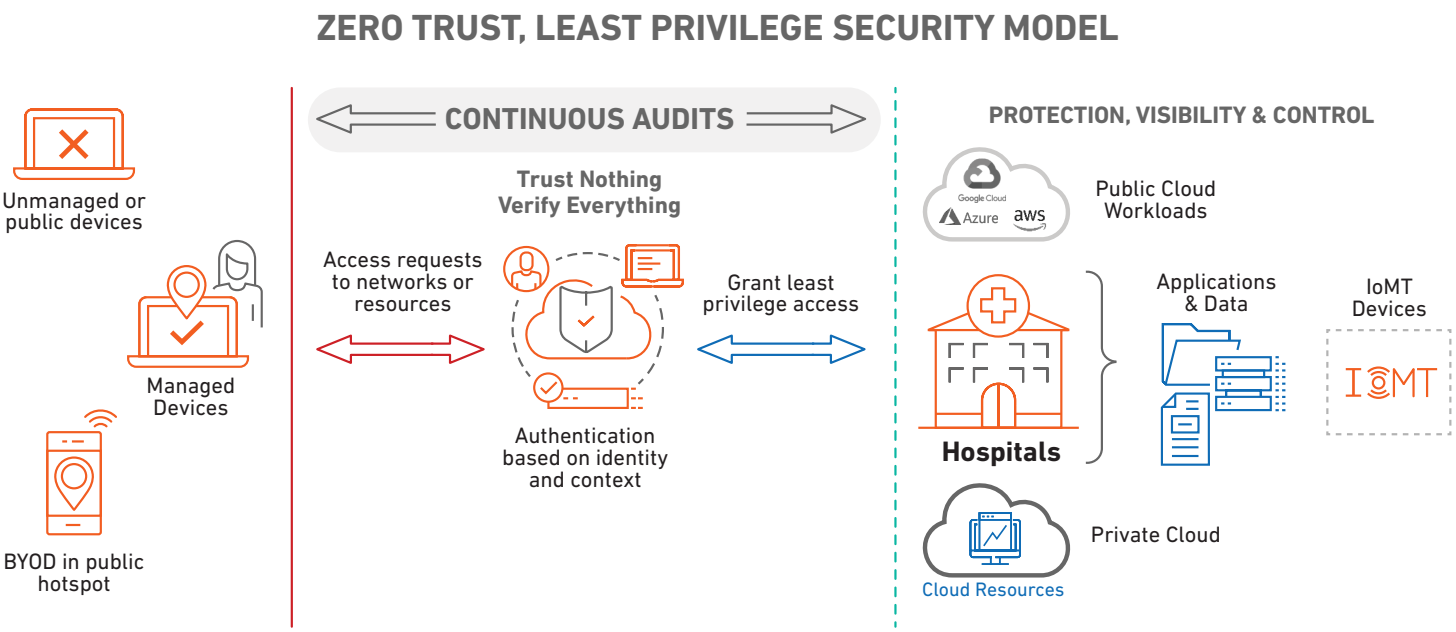
Advances in medical technologies, medical devices, electronic health informatics, cloud data exchange, and mobile and virtual communication enable this new "anytime/everywhere" care approach. Unfortunately, although these new capabilities improve the quality of care and patient satisfaction, they also raise significant privacy and security risks for healthcare organizations.

Healthcare personnel, such as doctors and nurses, often move from hospitals to other care facilities, workstation to workstation, and device to device with varying privileges to access patient health information. The addition of remote and mobile care workers accessing these same computer systems and digital records from virtually anywhere using unmanaged personal devices also adds to healthcare cybersecurity's growing challenges and complexities. In this environment, continuing with the outdated security model of "trust first and then verify" increases susceptibility to human error and data misuse, resulting in compliance violations, fines and class-action lawsuits.

Forrester Research states, "Companies cannot afford to trust internal network traffic as legitimate, nor can they trust employees and partners to always be well-meaning and careful with systems and data. To manage the complexities of their environment without constraining their digital transformation ambitions, many companies are moving toward a Zero Trust (ZT) security model — a more identity- and data-centric approach based on network segmentation, data obfuscation, security analytics and automation that never assumes trust."

SonicWall recommends healthcare organizations adopt a new zero-trust (ZT) and least-privilege security model to protect the integrity and privacy of patient health information. The foundation of this ZT security concept is the belief that organizations must always assume that attackers can be anywhere, inside or outside the perimeter. Therefore, without exception, no persons, machines or locations (even within the corporate network) should be inherently trusted; instead, verify every employee and device before granting access to care-critical resources.

Figure 13

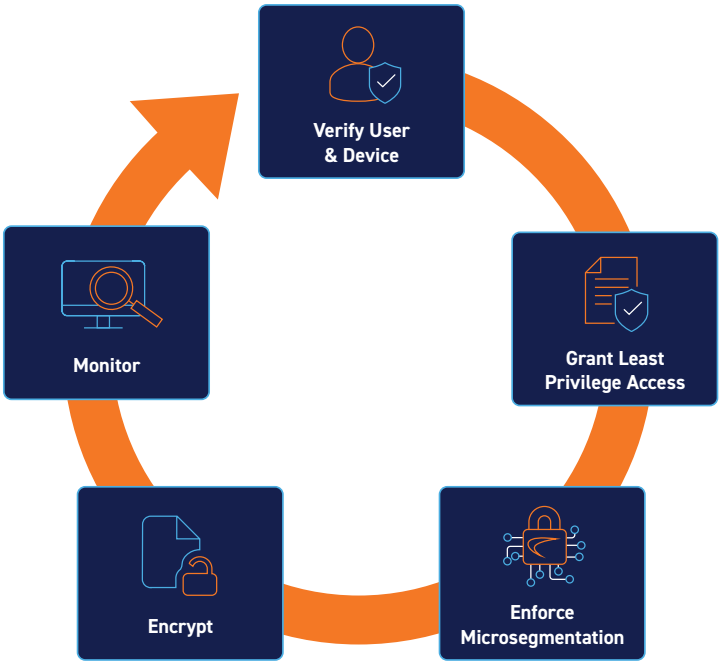


SONICWALL

Similarly, least-privilege access comes from the belief that users are given access only to what is necessary for their job role and responsibilities and nothing more, shrinking the risk surface as much as possible.

Whether you prefer the flexibility of a cloud service or the internal control of an on-prem deployment, you get both with SonicWall Access Security solutions. SonicWall's Cloud Edge Secure Access and Secure Mobile Access (SMA) products apply zero-trust and least-privilege security principles of "trust nothing, verify everything."

Figure 14: Zero-Trust Network Access (ZTNA)



ZT architectures grant trust only after user's credentials, associated multi-factor authentication (MFA) information, and permission characteristics based on contextual factors are known. These factors include the combination of network, device posture, location, work schedule and access time.

The combined user- and device-centric approach makes the verification of users and devices mandatory and without exceptions. It forms the foundation for reshaping access security via integrating identity-based controls, context-aware device authentication, micro-segmentation and access policy management for safer "anytime/everywhere" care.

Assuming All Endpoints are Risk Vectors is the Safest Policy

Healthcare professionals typically roam around, accessing various endpoint devices such as tablets, laptops and workstations to record medical notes and access health data during care engagements. If not managed, patched and protected with modern security, these endpoints are often open targets for threat actors to easily exploit and orchestrate an attack.

Additionally, the increase of remote workers coupled with the usage of personal devices has introduced countless exposure points into the healthcare environment. Encrypted threats are reaching endpoints unchecked, ransomware outbreaks are disrupting care and operations, and data breaches are causing irreversible harm. The consequences of a network or data breach are too dangerous to bear for both patients and providers, so treating all endpoints as risk vectors that must be tracked and monitored actively and constantly is the safest policy.

The management and security of endpoints are more mission-critical now than ever in protecting healthcare data and systems and, ultimately, patient safety. Healthcare must employ next-generation endpoint security that can stop all threat forms and methods of attack (Figure 15).

Figure 15

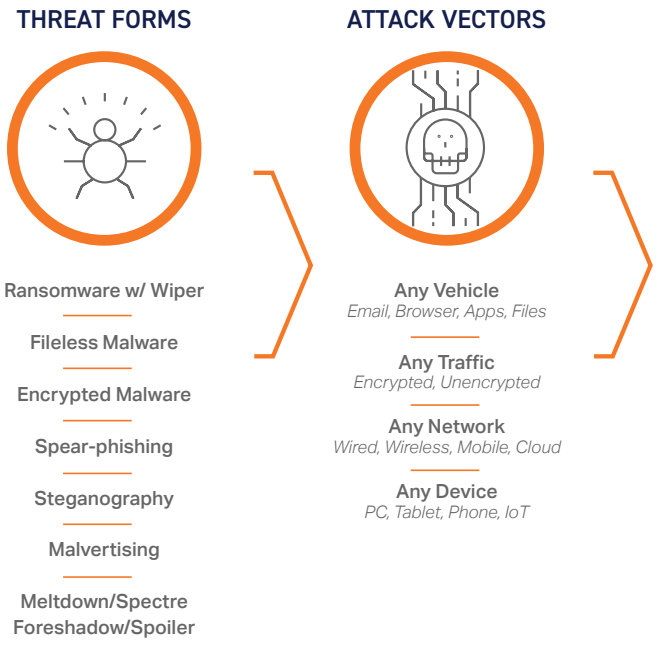
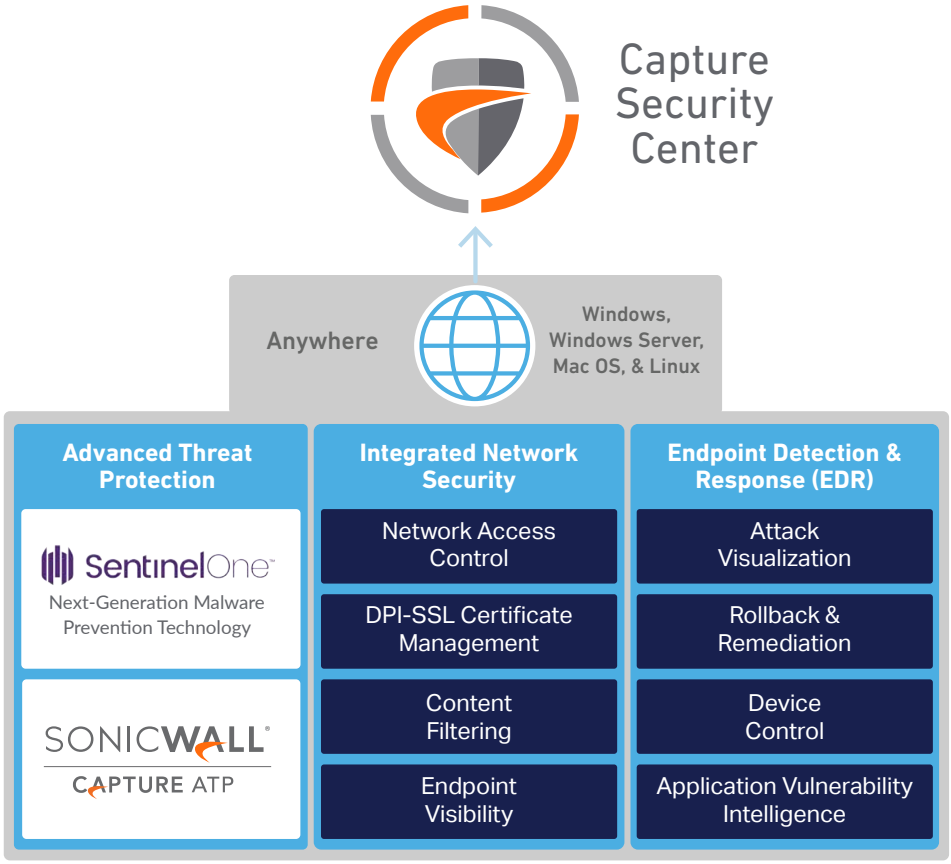


Figure 16

SonicWall Capture Client



SonicWall Capture Client is a unified client platform that delivers next-generation endpoint security with multiple Endpoint Detection & Response (EDR) capabilities, featuring behavior-based malware protection, advanced threat hunting, and visibility into application vulnerabilities.

The behavior-based anti-malware, powered by SentinelOne, constantly looks at changes in system behavior to stop attacks before and during execution. In addition, the quick one-click rollback feature easily facilitates full system recovery on the rare occasion that zero-hour malware compromises the endpoint.

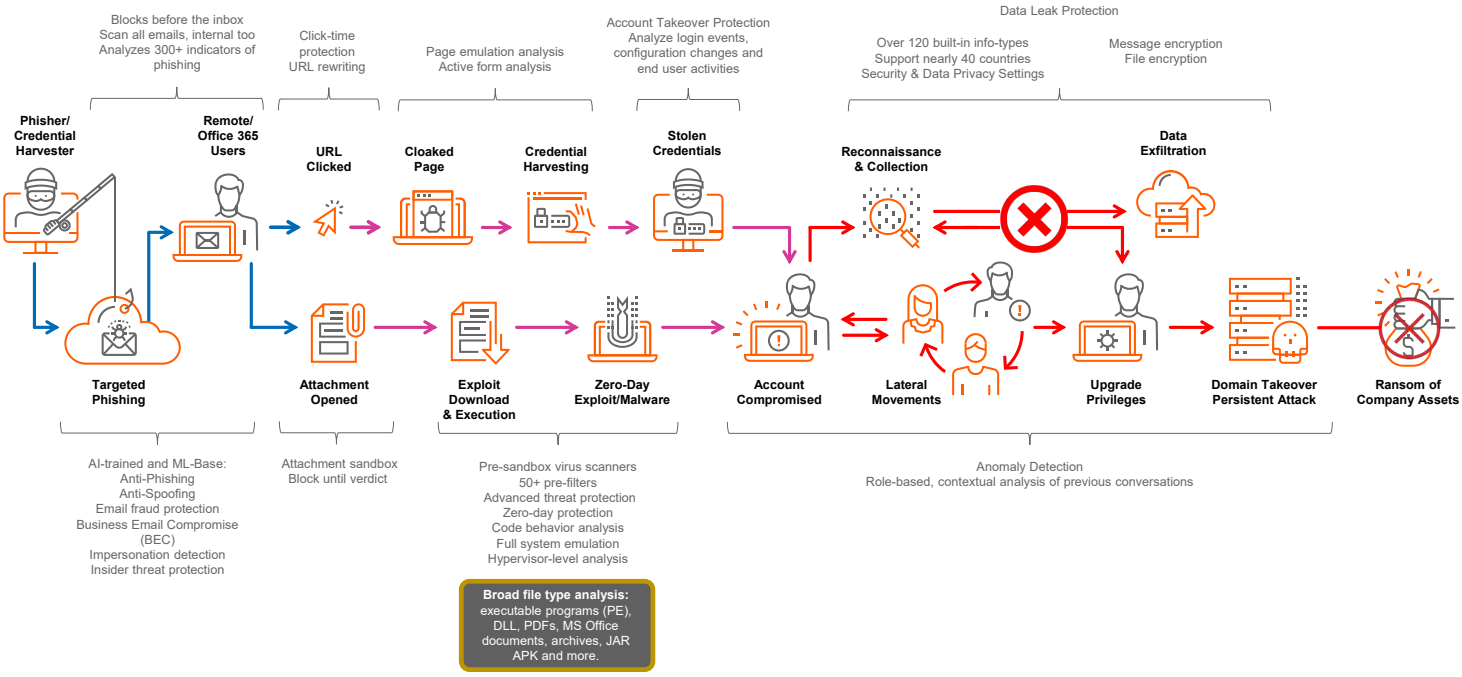
With the SonicWall Capture Cloud Platform integration, healthcare customers can take advantage of several points of synergy. For example, SonicWall NGFWs can enforce the use of Capture Client by directing unprotected endpoints to a download page before going out to the internet. Additionally, the DPI-SSL certificate deployment feature makes it easier for the NGFW to inspect encrypted traffic going to endpoints behind the firewall to prevent attacks coming through encrypted channels. Moreover, SonicWall Capture ATP with RTDMI™ can stop advanced threats the anti-malware engine cannot fully convict, such as dormant ransomware strains.

Capture Client also has scale in mind. Designed for the healthcare distributed environment with multiple tenants, the Global Dashboard provides a snapshot into the health of all tenants within a global view. Several factors measure the health of each tenant, including the number of infections, vulnerabilities present, the version of Capture Client installed, and what and who is being blocked the most by Content Filtering. The dashboard also shows which devices are online and operating.

Global Policy allows administrators to apply a single baseline policy to all tenants, making it easier to spin up new tenants. It can also create protections for new threats across all tenants on this baseline policy. All new tenants will acquire the Global Policy when the inheritance option is activated. Alternatively, exclusive policies can be created and modified for individual tenants when turned off.

Figure 17

BREAK THE PHISHING ATTACK KILL CHAIN



Reduce the Human Risks Factor

The growing adoption of cloud office applications like Microsoft 365 gives employees many different channels to access and share healthcare data that IT never intended to allow. Data exchanges — deliberate or accidental — between employees, partners and customers via emails, attachments and file sharing/collaboration platforms are not just customary but prevalent in today's remote workforces and cooperative business partnerships.

Regardless of roles and responsibilities, every healthcare worker, good or bad, is the custodian of the confidential data they have in their possession. However, while bad employees become insider threats, even good employees are not perfect. Someone is likely to make a bad mistake or take deliberate action in handling that information. The outcome is sure to be harmful and costly either way. Therefore, hoping users will not leak healthcare information is not a practical leak prevention strategy.

The sources and mechanics of data leaks are endless. Although employees pose the highest risk, account compromise, application vulnerabilities, social engineering and configuration errors are still the top root causes that companies must address.

SonicWall Email Security solution comes with a comprehensive data leakage prevention (DLP) compliance engine to stop unauthorized transmission of data via emails and cloud office system, such as Microsoft 365 or Google Workspace. The DLP configuration module enables security admins to granularly control which individuals health data can be shared with, as well as how that data gets shared. It also establishes and synchronizes DLP and encryption policies across email users and cloud office applications.

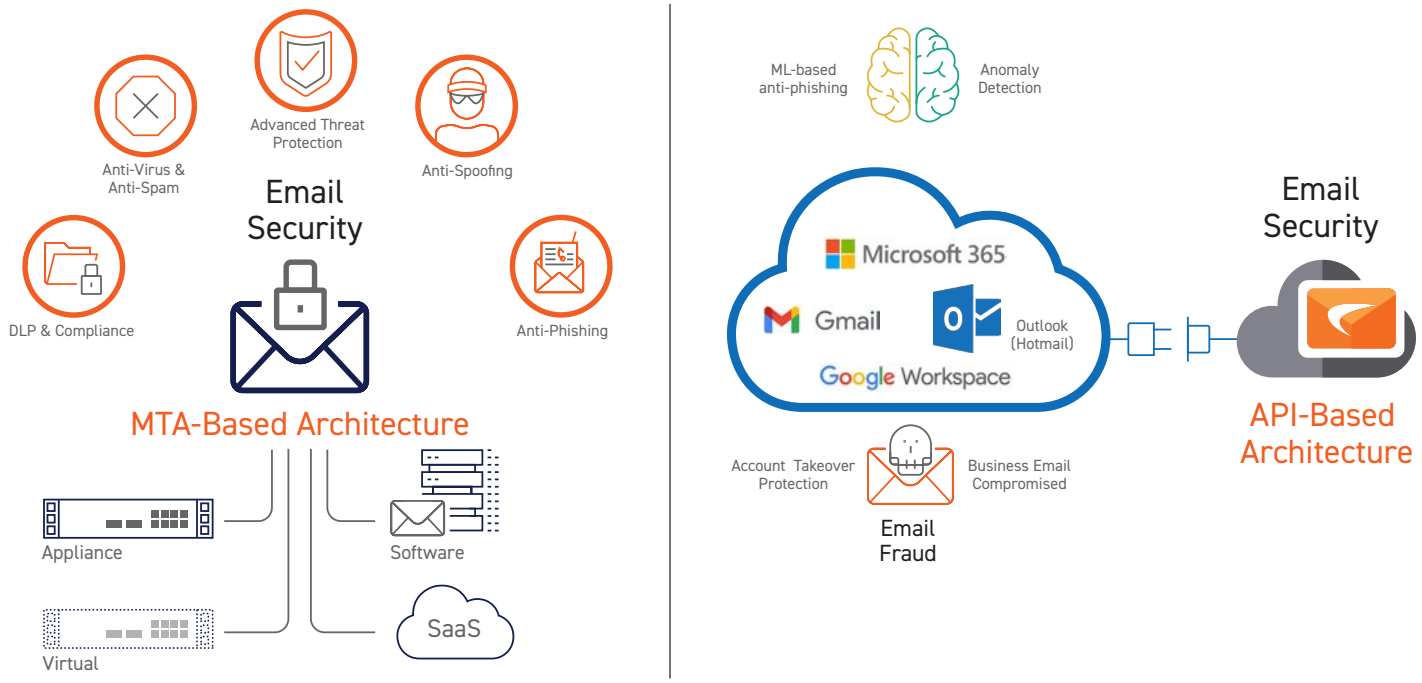
The DLP scanner supports over one hundred info types, along with data classifiers that span over forty countries. The solution scans all parts of the email and popular cloud sharing apps, including attachments, ensuring intellectual property, protected health information and other compliance data do not leak accidentally or willfully. Moreover, the solution provides policy templates that map to HIPAA, SOX, PCI, GDPR and other regulatory laws for audit and compliance readiness.

Keep Phishing Messages out of the Inbox

Phishing attacks are a top concern cited in healthcare despite the increase in security education provided to workers. Medical staff are focused on clinical analyses and treatment decisions for many patients, making healthcare systems highly vulnerable to phishing attacks that prey on distracted workers.

SONICWALL

Figure 18



Despite the presence of personalized and targeted phishing attacks that look like legitimate emails, security pros say they still see users clicking on theme- or event-based phishing emails. One of the many truths of email-borne threats is that attackers quickly respond to mega-trends. The work-from-home movement and COVID-19 pandemic are the latest examples that make email communication the most extensive channel for all forms of phishing as a precursor for ransomware attacks.

The phishing innovation curve is also happening post-delivery. Instead of putting the malicious payload or weaponized URL in the email, phishers link to a redirect server that acts as a gateway, sending queries from a security company to a benign site. In contrast, queries coming from the intended victims are directed to the phishing server. Unfortunately, many workers are still unable to discern legitimate emails from fake ones; recognize suspicious links; or take cautionary actions such as authenticating the URL, sender's identity and company website. But even the most trained and security-conscious users can be tricked by phishing emails that are crafted to look genuine and are sent from stolen or fake but known identities.

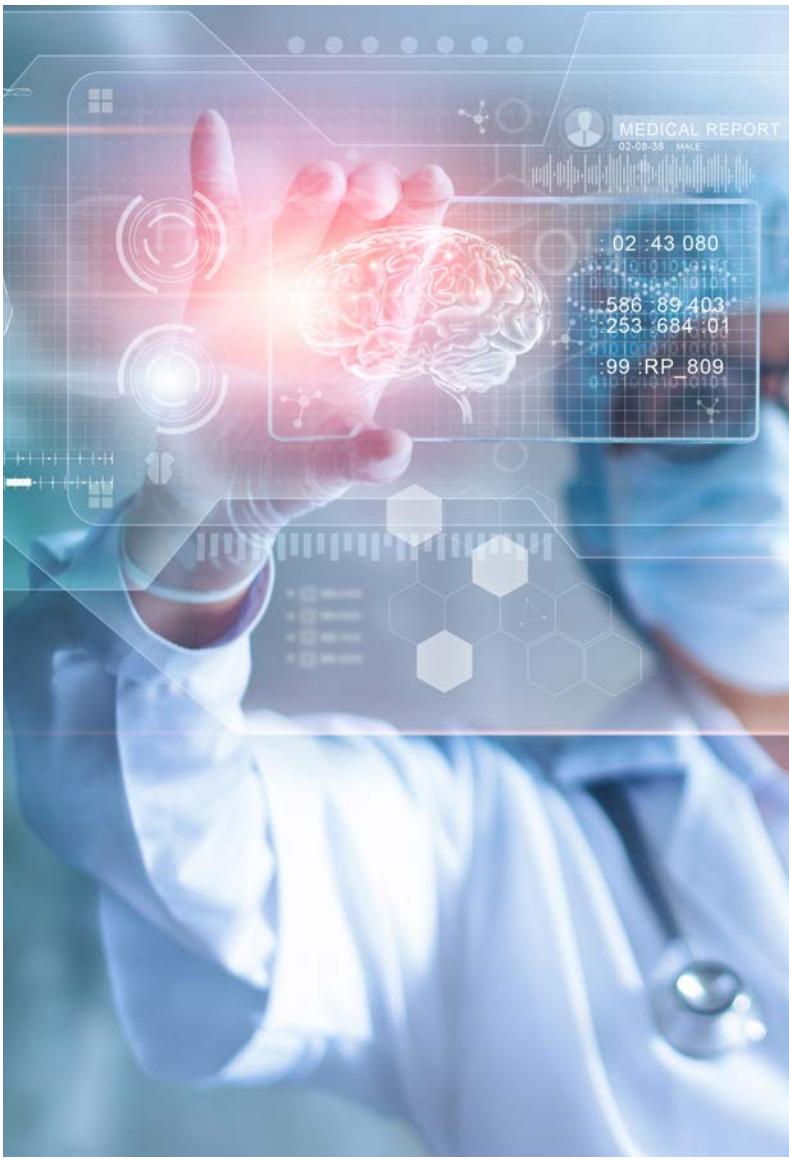
SonicWall Email Security solutions bring a layered security approach, providing multiple protection coverages for healthcare organizations' on-prem Exchange and Microsoft 365 or Google Workspace environments. It also gives you a choice between a gateway- or API-based approach to email security. Both methods come with the latest content analysis capabilities for detecting and catching complex forms of phishing before they reach the inbox, removing the potential for any poor decisions or actions from users that could lead to ransomware infections, data leakage or compliance violations.

Conclusion

SonicWall Boundless Cybersecurity approach is a scalable cyber-defense architecture that caters to healthcare IT needs. SonicWall provides flexible, easy-to-deploy tools to strengthen healthcare cybersecurity, making patient care delivery more efficient, resilient and secure.

This integrated, centrally managed security stack protects all assets and workers and ensures care continuity, patient safety and data confidentiality. Whether it is ransomware, targeted phishing, or vulnerability in healthcare systems, the Boundless Cybersecurity approach enables healthcare to counter all threat forms, attack vectors and exposure points with the highest security efficacy and performance.

- For a live demonstration, visit www.livedemo.sonicwall.com
- To start a trial and see the power of the SonicWall email solution, click here.
- For more information, contact us.



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