SONICWALL

SOLUTION BRIEF: SONICWALL CAPTURE CLOUD PLATFORM

A security ecosystem that harnesses the power of the cloud

Abstract

The SonicWall Capture Cloud Platform tightly integrates security, management, analytics and real-time threat intelligence across the company's portfolio of network, email, mobile and cloud security products. This approach enables our complete portfolio of high-performance hardware, virtual appliances and clients to harness the power, agility and scalability of the cloud.

The Challenge

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.

Whether your organization is a Fortune 500 enterprise or a small business, the journey to the cloud is required to compete. Organizations that embrace the cloud are thriving and achieving greater levels of operational efficiency, elasticity and speed required to endure and succeed in a highly competitive and unforgiving business climate.

As security technologies and the cyber threats landscape 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.

Need for actionable cyber threat intelligence

To combat today's advanced threats, organizations need to proactively leverage real-time cyber threat intelligence. For example, in 2017, although the number of ransomware attacks overall declined, we saw twice the number of new variants created indicating that cyber criminals are retooling. This presents a challenge because in early 2018, on average, SonicWall customers were hit by malware on average over 90 times per day, with three of these being ransomware attacks.

More and more attacks are now being cloaked using SSL/TLS encryption, and on average of these 90 attacks per day, six are encrypted. Finally, the typical SonicWall customer must protect their network and users from 11 phishing attacks per day.

Too many siloes

Organizations are burdened with managing and operating legacy point products alongside modern cybersecurity solutions. Environments are siloed. Management is tedious. Processes are labor-intensive. This level of technology fragmentation has businesses struggling for an integrated approach for security, management, analytics and real-time threat intelligence.

A Unified Solution

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

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

Capture Cloud Platform is innovatively constructed to help make the cloud journey powerful, agile and safe. This cloud- and service-oriented architecture unifies current and future SonicWall security and management services that organizations and service providers need to run an enterprise-class security operations center (SOC) on a low, predictable annual budget. It eases and, in most cases, automates the governance of their network, endpoint and cloud security services all from one place.

Organizations are empowered by the Capture Cloud Platform to make the shift from the old on-premises world of IT into the new multi cloud, as-a-service world by unifying security solutions with simple, common management tools that not only achieves your security and operational goals but also delivers real business value.

Our keen focus and deep expertise in security, and security operations and processes means you're investing not just in a technology platform but also in the mutual trust of an experienced technology partner with an uncompromising mission to help its customers produce successful outcomes.

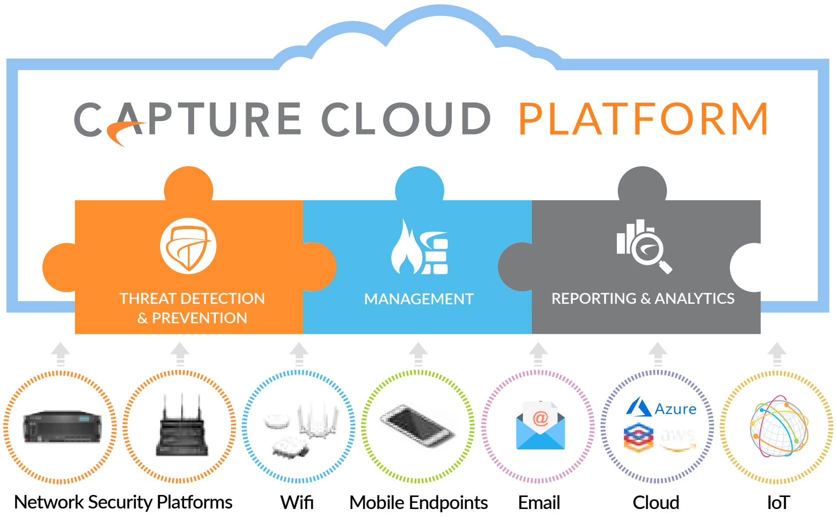
SonicWall Capture Labs researchers pioneered the use of artificial intelligence for threat research and protection over a decade ago. Today, machine-learning algorithms are used to analyze data and classify and block known malware before it can infect the network.

Core Components & Capabilities

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 long-term success for organizations. It is comprised of 10 key SonicWall service components:

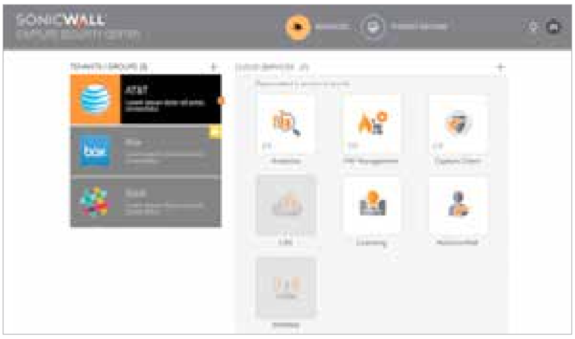
- Capture Security Center
- Real-Time Cyber Threat Intelligence
- Capture Client
- Capture Advanced Threat Protection (ATP)
- Cloud App Security
- Analytics
- NS*v* Series virtual firewalls
- NS*a* Series hardware firewalls
- Web Application Firewall
- MySonicWall

The combination of these services* delivers mission-critical layered cyber defense, threat intelligence analysis and collaboration, and common management, reporting and analytics that work synchronously together.



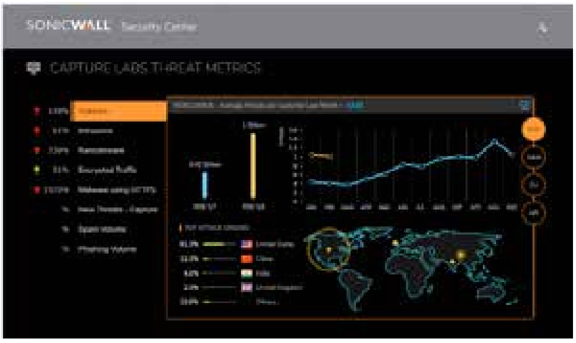
Capture Security Center

- Unified security governance, compliance and risk management security program
- Single pane of glass access to management, analytics and provisioning
- Automated workflows assure security compliance
- Reduced risk provided by a fast response to security events
- Precise security controls and policy decisions based on situation insights



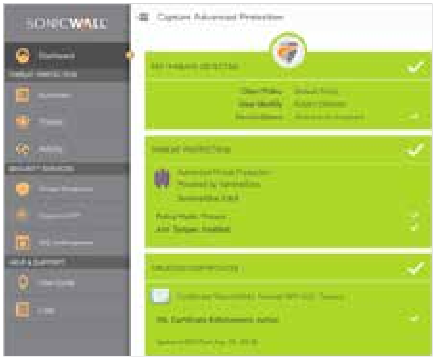
Real-Time Cyber Threat Intelligence

- Telemetry data that empowers you to take action to better protect your organization
- Regional drilldowns for North America, Europe and Asia to give organizations around the globe deeper insight
- Detail for malware attacks, intrusion attempts, ransomware, encrypted traffic, HTTPs-encrypted malware, new threats discovered by Capture ATP sandbox and spam/phishing activity



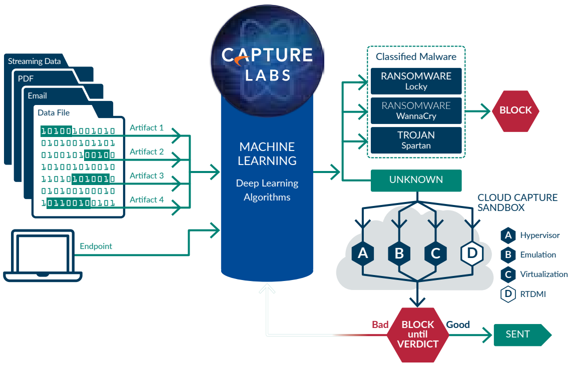
Capture Client Endpoint Protection

- Advanced attack detection using behavioral monitoring
- Highly accurate machine learning and multi-layered heuristic-based techniques
- Unique roll-back capabilities (*Capture Client Advanced only*)
- Endpoint security enforcement
- DPI-SSL certificate management



Capture Advanced Threat Protection Sandbox

- High security effectiveness against unknown threats
- Multi-engine advanced threat analysis
- Broad file type analysis
- Blocks until verdict
- Near real-time signature deployment protects from follow-on attacks
- Reporting and alerts

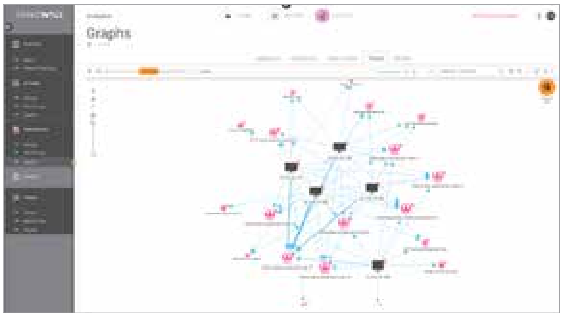


Cloud App Security

- Real-time visibility into cloud application traffic and the associated user activity
- Enforced granular access policies for risky applications
- Reduced shadow IT by discovering usage of Sanctioned and Unsanctioned IT applications
- Comprehensive reporting and analytics for actionable insights
- Reduced administrative overhead through easy deployment with SonicWall Capture Security Center

Platform Analytics

- Single-pane visibility and complete situational awareness of the network security environment
- Complete authority and flexibility to perform deep investigative and forensic analysis
- Deeper knowledge and understanding of potential and real risks and threats
- Remediation of risks with greater clarity, certainty and speed
- Reduced incident response time with real-time, actionable threat intelligence



NSv Series Virtual Firewalls

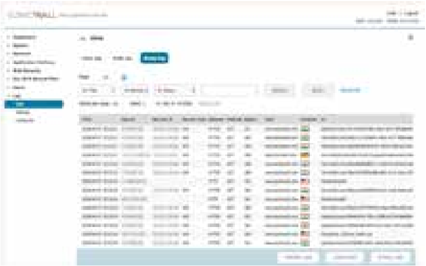
- Automated breach prevention for public, private and hybrid cloud environments
- Cross virtual-machine attack and side-channel attack defense
- Common network-based intrusion, application and protocol protection
- Elimination of unauthorized access to protected virtual data store
- Prevention of service disruption of virtual ecosystem

NS*a* Series Firewall Appliances

- Real-Time Deep Memory Inspection (RTDMI™) and Reassembly-Free Deep Packet Inspection
- Cloud-based and on-box threat prevention featuring multi-engine sandboxing, anti-malware, intrusion prevention, web filtering and more
- High port density with 10-GbE and 2.5-GbE ports
- Real-time TLS/SSL and SSH decryption and inspection
- Built-in wireless controller

Web Application Firewall

- Web application threat management
- Defense against OWASP top 10 web application security risks
- High-speed, highly reliable and secure web app delivery
- Data leak prevention
- Application delivery acceleration



MySonicWall.com

- Register all your SonicWall appliances and services in one place
- Access firmware and security service updates
- Get SonicWall alerts on services, firmware, and products
- Manage (activate, change or delete) your SonicWall security services online

Conclusion

SonicWall has been fighting the cybercriminal industry for over 26 years, defending small- and medium-sized businesses and enterprises worldwide. The award-winning Capture Cloud Platform, coupled with the power of tens of thousands of global channel partners, protects your network, email, cloud environments, applications and data.

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.

** Web, wireless, email, mobile and IoT security services will be fully integrated into this platform in future product announcements.*

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 Us

SonicWall has been fighting the cyber-criminal industry for over 26 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

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