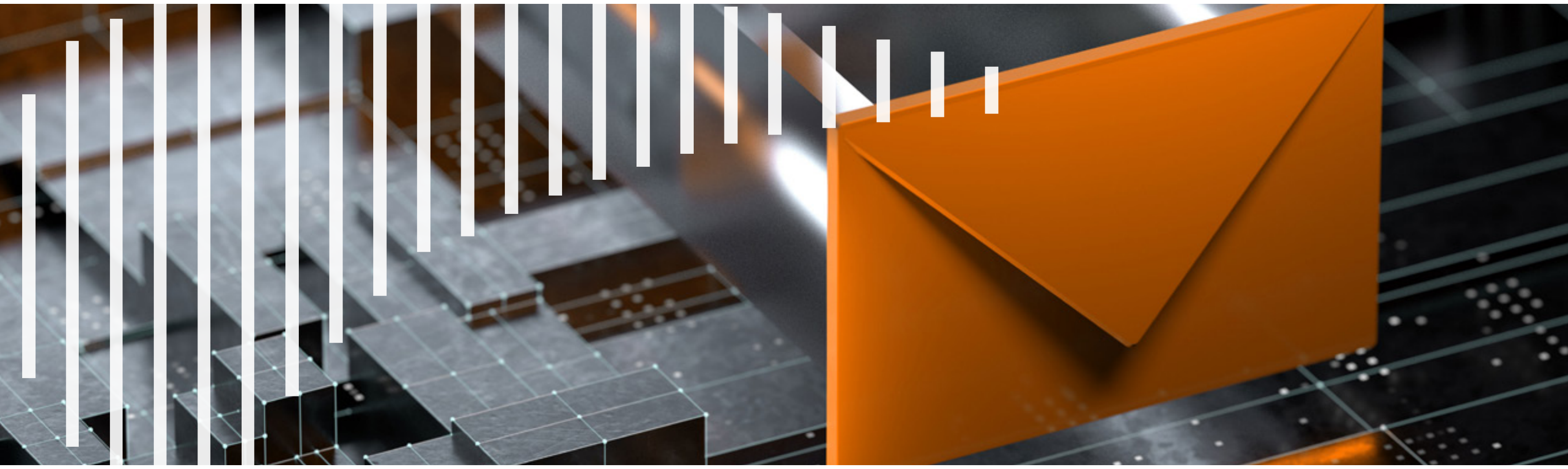


Adaptive Email Security for the Cloud Era

Essential capabilities for preventing email-borne threats from reaching the inbox.

ABSTRACT

The cloud is an unstoppable change agent. Its efficiency, elasticity and scalability are compelling enterprises to replace their on-prem productivity and back-office tools — including email, collaboration and file sharing — with the newer cloud versions. But there are two major concerns with the adoption of such apps: security and availability of service.

This brief examines how the SonicWall Email Security solution brings together the latest email security technologies to combat evolving threats, such as targeted phishing, business email compromise (BEC), account fraud, data leakage and ransomware.

Introduction

When it comes to email-borne threats, attackers are quick to adapt to mega-trends. The work-from-home (WFH) shift and the COVID-19 pandemic are two examples of trends that have led to a rise in the use of personal devices or less secure networks to access their work emails making them more vulnerable. Attackers have exploited these trends, finding that email communication has become a more lucrative attack vector for targeted phishing and ransomware. As we've learned from past data breaches, these attacks often involve using multiple tactics, techniques and procedures (TTP) to compromise the user entirely.

What was also proven repeatedly in those events is that email is the first to deliver:

- The initial embedded URL that links to an obfuscated phishing website or malicious download
- The attachment containing a malicious payload
- The beginning of a social engineering attack, such as with email fraud or credential harvesting attacks

To stop these sophisticated threats, organizations must deploy a constantly updated email content filtering system that learns and adapts to new phishing TTP. At the same time, the system's advanced threat analysis can effectively block high-quality, low-volume personalized phishing, business email compromise, impersonation and zero-day attacks with greater accuracy and fewer false positives.

The solution must:

- Scan all email traffic — not just inbound and outbound messages — as email-borne threats and data leaks can occur via compromised accounts or employee-to-employee spread.

SOLUTION BRIEF

- Apply machine learning (ML) and artificial intelligence (AI) capabilities to reveal hard-to-catch phishing attacks designed to fool users and bypass security filters. These include anomaly, fraud and BEC detection, natural language processing, identification of key indicators of compromise, and multifaceted attacks that thread pinhole vulnerabilities in known security layers.
- Scan emails inside the cloud before they arrive at the inbox. This allows organizations to enjoy the best of both worlds and brings the concept of perimeter-less security to each user's inbox.

SonicWall Email Security architectures

SonicWall Email Security solution offers a security stack that is both deep and wide, providing optimal protection coverage for either your on-premise exchange or cloud office system (i.e., Microsoft 365 or Google Workspace) environments.

You can choose between a gateway- or API-based approach based on your unique deployment requirement. Both provide the latest technology capable of catching complex forms of phishing, business email compromise (BEC), email fraud and impersonation attacks before they reach the inbox. Besides keeping users from being tricked by these malicious schemes, the solution also helps reduce human risks, removing the potential for any poor decisions or actions from users that could lead to ransomware infections, data leakage or compliance violations.

API-based email security

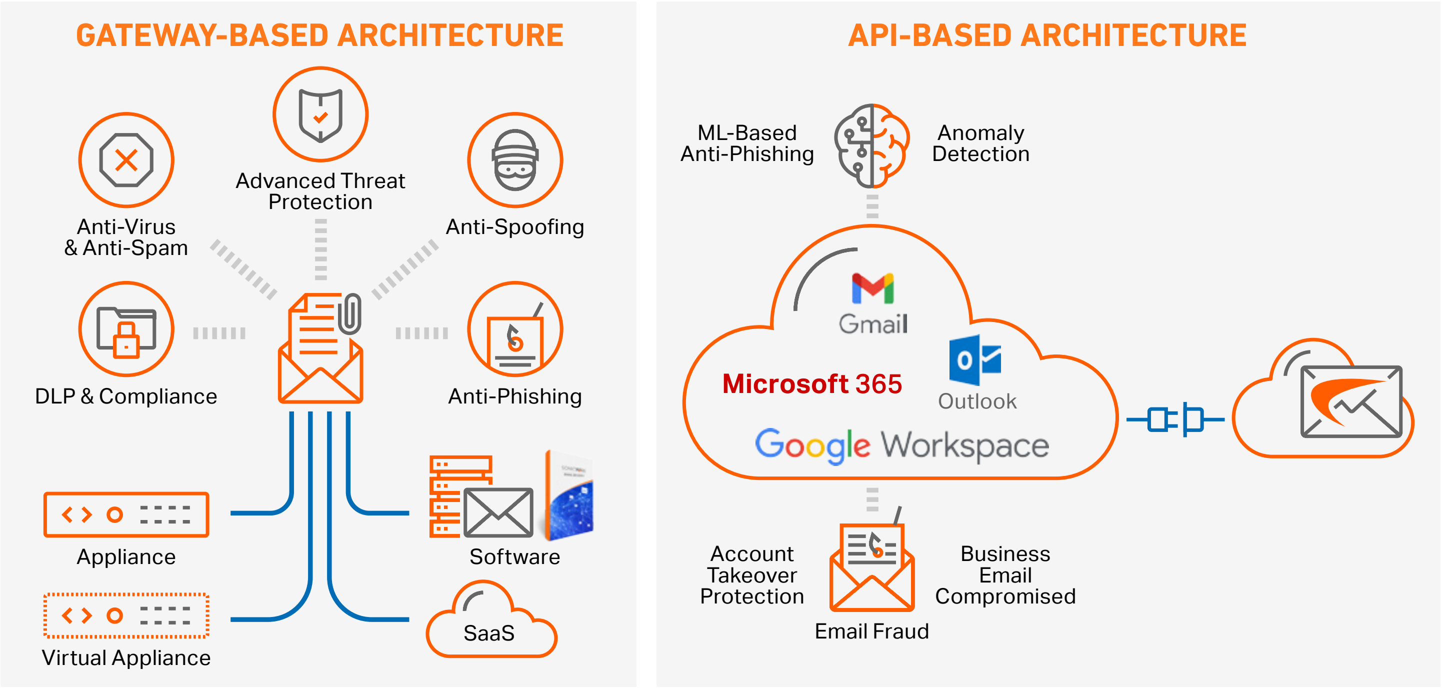
SonicWall Cloud App Security *(CAS)* is a cloud-native, API-based email protection solution designed to catch complex, high-quality phishing and zero-day attacks. These targeted, low-volume attacks are specifically field-tested for bypassing Microsoft's and Google's built-in security filters.

Using APIs, the solution seamlessly integrates into the cloud office systems' security workflows, where it is tuned to identify attacks that bypass cloud office security filters. In addition, its inline multi-layered threat prevention system is invisible to hackers and enables full-suite protection for cloud email and SaaS applications.

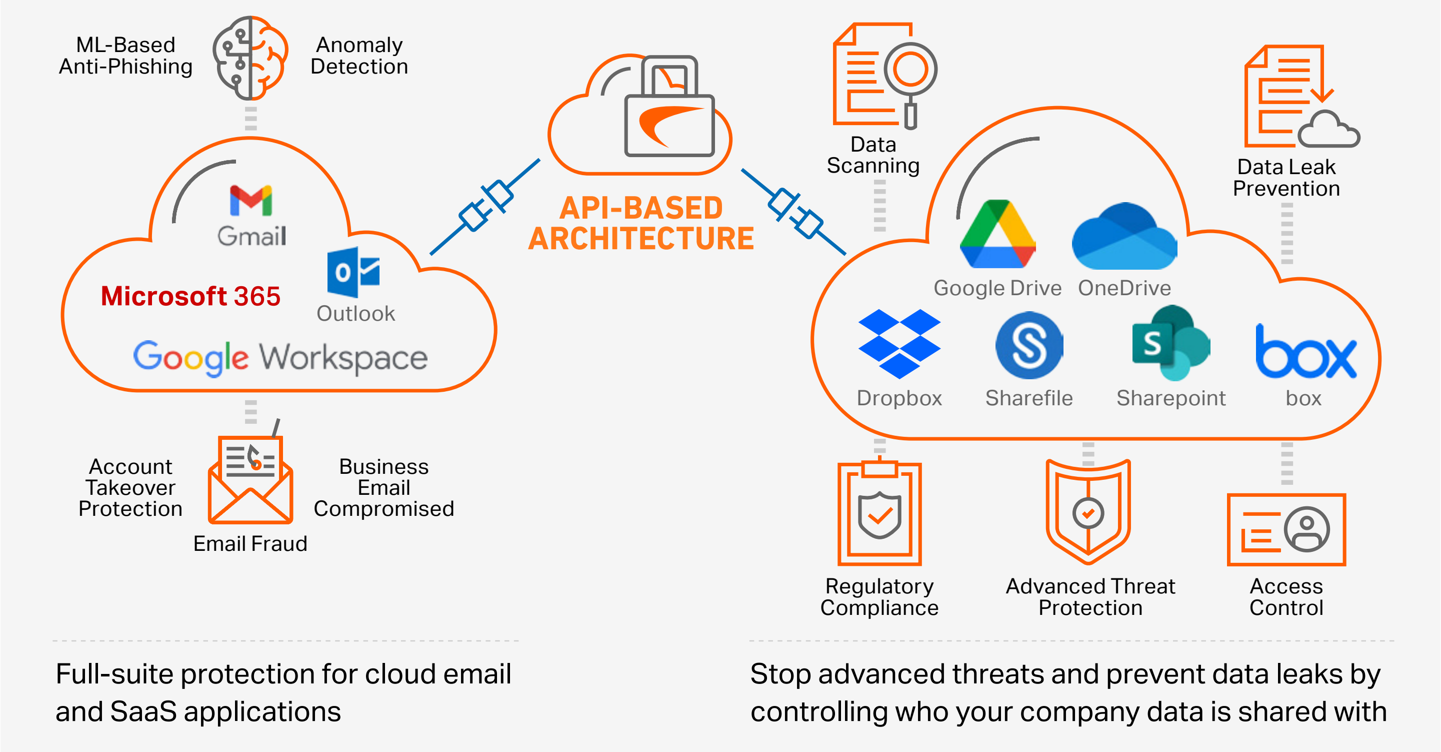
CAS deploys within minutes and employs the latest innovations in machine learning and artificial intelligence technologies combined with big-data analysis. The artificial intelligence dynamically and continuously trains multiple machine learning and threat emulation engines to recognize and detect new phishing behaviors and their tactics, techniques and procedures.

Together, they analyze hundreds of unique threat indicators, providing effective protection against phishing, BEC, attachment sandboxing, time-of-click URL analysis and fraud.

SonicWall Email Security Technologies



SonicWall Cloud App Security


ML-Based Anti-Phishing
Anomaly Detection
Gmail
Microsoft 365
Outlook
Google Workspace
Account Takeover Protection
Email Fraud
Business Email Compromised
API-BASED ARCHITECTURE
Data Scanning
Data Leak Prevention
Google Drive
OneDrive
Dropbox
Sharefile
Sharepoint
box
Regulatory Compliance
Advanced Threat Protection
Access Control
Full-suite protection for cloud email and SaaS applications
Stop advanced threats and prevent data leaks by controlling who your company data is shared with

One machine learning engine is customized specifically for the organization — this engine is trained on the customer's particular environment to identify targeted threats against that organization in particular, allowing for a tailored response.

Another machine learning engine is specifically attuned to anomaly detection and user behavior analytics. This unique engine detects behaviors or actions that seem abnormal when observed in the context of an organization's and user's historical activities. This engine analyzes the behavior using machine-learning algorithms, which build a profile based upon historical event information, including login locations and times, data-transfer behavior and email message patterns. A security event is generated when anomalies are detected, providing the context and other information needed for the investigations.

CAS performs pre-inbox analysis of all messages, including inbound, outbound and internal emails. No emails, links or attachments can reach the inbox until CAS has examined them and determined they are 100% harmless. Alert settings keep relevant personnel, such as an admin or security analysts, notified of potential compromises for post-delivery remediation or recovery.

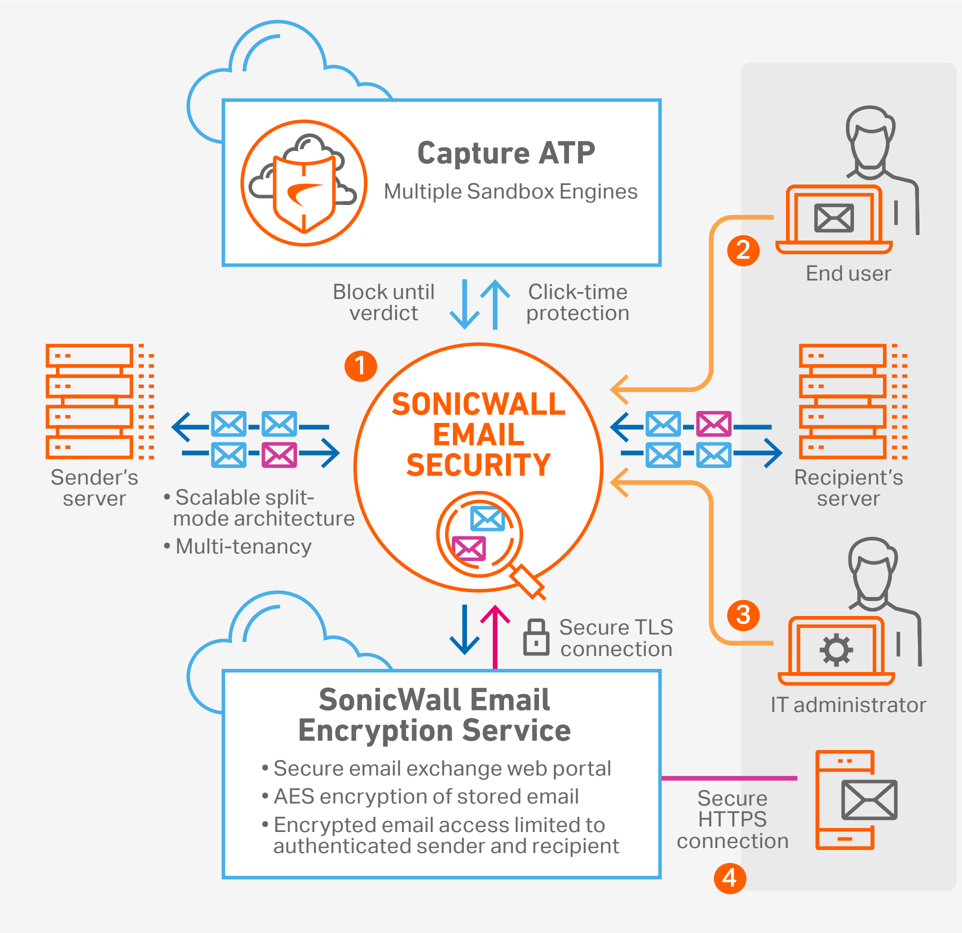
Gateway-based email security

SonicWall Email Security gateway solution combines artificial intelligence and machine learning techniques with heuristics, reputation and content analysis capabilities to deliver comprehensive protection against targeted phishing, spoofing and ransomware attacks.

The initial line of defense eliminates up to 99% of easy-to-detect spam at the connection level before it has a chance to enter the network. SonicWall's Advanced Content Management (ACM) then analyzes and filters any remaining bad email. The ACM scanning system effectively stops the more advanced phishing and impersonation campaigns by leveraging Adversarial Bayesian™ analyses. The techniques use advanced text and image parsing engines, lexicographical distancing, image analysis (white-on-white, tiny fonts, etc.) and gibberish detection to see through the TTP that phishing campaigns use to hide their malicious intent.

ACM scans every part of the email component (i.e., metadata, body, subject, attachments, URLs, etc.) to ensure compliance with corporate policy. The solution then blocks or re-routes noncompliant emails to appropriate LDAP-based groups or individuals for approval.

Email Security Gateway-Based Protection



1 Inspect and protect

- Multiple proven, patented techniques
  - » Anti-spam
  - » Anti-phishing
  - » Anti-virus

2 Managed by end-user

- Junk mailbox
- Allow/block list
- Junk summary settings
- Emergency inbox

3 Managed by IT administrator

- Set up and configuration
  - » LDAP integration
  - » Spooling management
  - » Threat protection management
- Allow/deny user self-management
- Configure and monitor secure exchange portal
- Reports
- Email continuity

4 Access to encrypted email

- Mobile and desktop access to encrypted email
- Read or download encrypted email
- Send encrypted reply

Email Security also integrates with your organization's LDAP to prevent Directory Harvest Attacks (DHA). It also leverages industry-leading anti-virus signature feeds that are continually updated to provide up-to-date protection against malware. At the same time, it enforces various email authentication standards, such as sender policy framework (SPF); domain keys identified mail (DKIM); and domain-based message authentication, reporting and conformance (DMARC), for stopping spoofing attacks, business email compromise and email fraud.

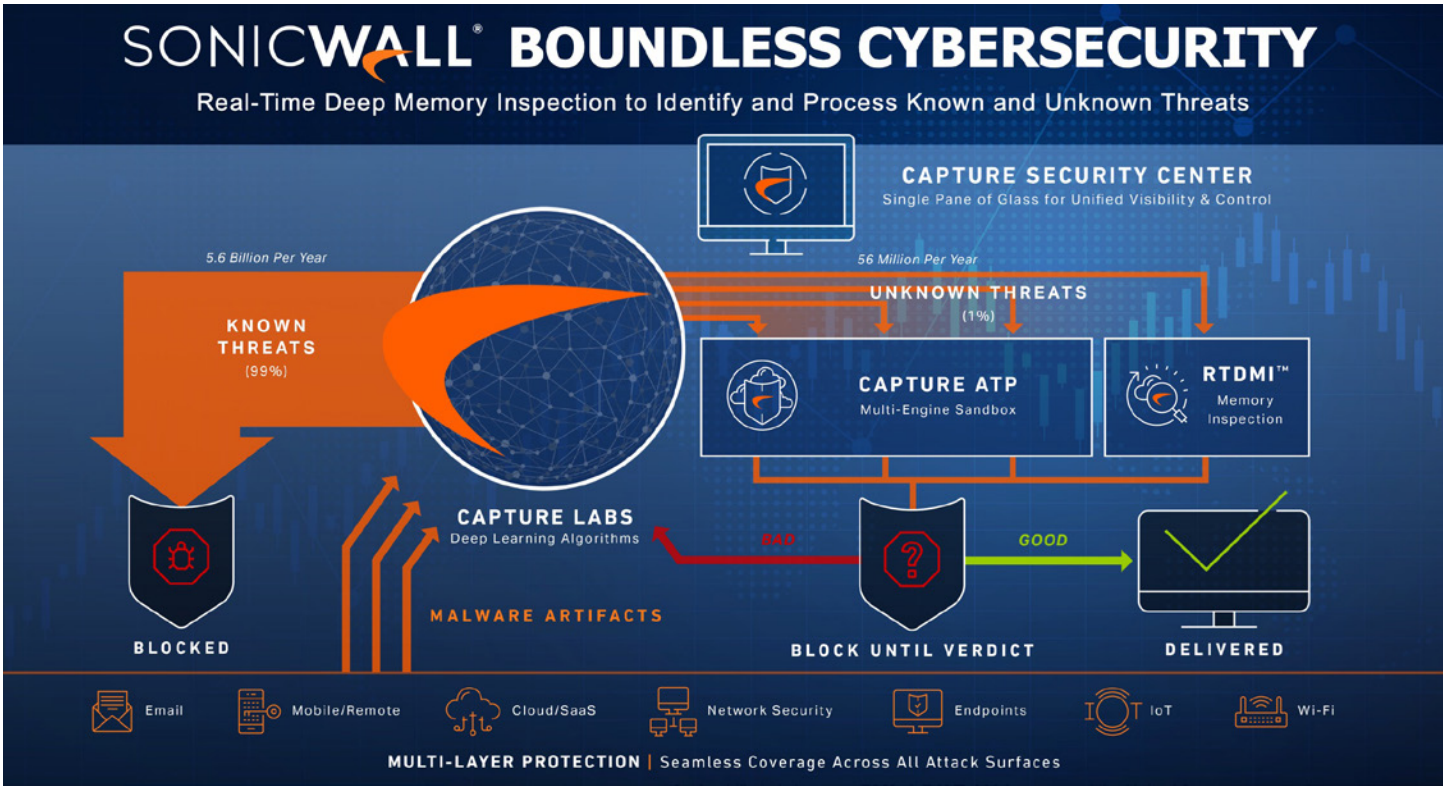
Business email compromise and email fraud detection

The science behind recognizing and stopping business email compromise, fraud and impersonation attacks is internal context. A primary benefit of deploying the CAS API-based approach within the cloud email service is immediate access to historical conversations. The CAS artificial intelligence scans up to five days worth of email dialogues within hours of deployment to establish senders' trust and authenticity.

At the same time, it also builds a reputation network with continuous learning of senders' relationships and behaviors, providing accurate business email compromise detection and reducing the number of false positives that plague most other email solutions. The tuning, which typically takes months with other security solutions, happens immediately and automatically using millions of historical email conversations. The solution can also recognize communications from users that are out of the ordinary, while it would be the first time other solutions would ever see such an email.

Anomaly and account takeover detection

Anomalies are likely indicators of an account being compromised. CAS has a specific anomaly detection engine that monitors behaviors or actions that appear abnormal when observed in the context of a user's historical activities. Using machine-learning algorithms, it analyzes those irregularities, building profiles based on each user's historical event information, including login locations and



times, data-transfer behavior and email message patterns. Security events are generated when anomalies are observed, and alerts with context and other needed information get sent to analysts and incident responders for investigation and remediation.

Advanced threat protection

SonicWall email security products are components of the SonicWall Capture Cloud Platform framework. This allows them to work seamlessly across the entire SonicWall security stack, including firewalls, endpoint protection and access security products for synchronous threat management.

In addition, they leverage the SonicWall Capture ATP service with Real-Time Deep Memory Inspection (RTDMI™) technology, the only award-winning advanced threat detection system that uses multiple sandboxing engines for analyzing suspicious attachments and URLs within emails.

SonicWall's patented RTDMI file analysis engine analyzes suspicious files by monitoring for malicious behavior of an application in memory. RTDMI sees through any obfuscation or encryption techniques that modern malware may deploy to evade sandbox analysis, yielding extremely high-accuracy detection of attacks embedded in documents, executables, archive files and a variety of other file types.

RTDMI also works in concert with reputation, static analysis and global hash checks across the threat intelligence industry to deliver quick verdicts. Once never-before-seen malware and ransomware variants are detected, they are used to create signatures for one part of the defense chain, but these also benefit all other parts of the SonicWall layered defense ecosystem instantly in real-time. **The entire process is done within seconds, reducing the window of exposure significantly**.

Post-Inbox Delivery Protection

The 2020 COVID-19 pandemic created the most extensive distributed workforce in human history, with billions of people using email daily in the comfort of their homes. Unfortunately, many of them haven't been well trained to discern legitimate emails from fake ones or recognize suspicious links. What is so frightening is that phishing emails can be now be crafted well enough to appear genuine to even the most security-savvy users.

We know good employees are not perfect. All it takes is one bad click, one bad download or one act of carelessness and the infection process kicks into high gear. To effectively mitigate the human risk, SonicWall has added **Click-Time**

Protection (CTP). Also known as Time-of-Click Protection, this post-delivery security feature was specially designed as an additional safety measure to protect unknowing users from themselves and subsequently save the organization from a potential disaster.

CTP's primary function is to examine every URL and attachment when the user clicks on a link or downloads a file embedded in an email, even if it's forwarded to someone else. A real-time scan detects and quarantines bad URLs, then informs users via a notification screen. Additionally, if the suspicious URL is linked to a phishing campaign, CTP can retract and remove harmful email messages used by the same campaign.

Data leakage prevention

Email Security gateway and CAS solutions each come with their own respective security compliance module, enabling you to control who your company data is shared with and how it is shared. Both allow you to establish and synchronize unified data leakage prevention (DLP) and encryption policies across users and cloud office applications. They also leverage over a hundred info-types and support data classifiers that span over 40 countries.

The solution scans all parts of the email and popular cloud sharing apps, including attachments, to ensure intellectual property, personal identifiable information (PII) and other compliance data do not leave your organization's network accidentally or willfully. Moreover, for audit and compliance readiness, the solution provides policy templates that maps to HIPAA, SOX, PCI, GDPR and other regulatory laws.

Conclusion

With email as a primary target for threat actors around the globe, it's crucial for both organizations and individuals to take proactive measures in enhancing email security. It's important to recognize that not all email security solutions are alike. The selected solution should possess the essential capabilities enabling it to effectively adapt in response to the continuous changes of the cloud era.

SonicWall Email Security solutions utilize cutting-edge artificial intelligence and machine learning technologies to proactively combat targeted phishing, Business Email Compromise (BEC), and email impersonation attacks. These proactive measures ensure that such threats are intercepted and neutralized before they even reach your inbox.

Learn more about how SonicWall Email Security solutions can protect your organization from advanced email-borne threats.

www.sonicwall.com/email-security

Contact Sales

https://www.sonicwall.com/customers/contact-sales

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

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.