Abstract

Today’s advanced threats require a new set of email security features in addition to traditional capabilities. A multi-layered approach to email security ensures protection for business communications. Businesses need a next-gen email security solution that offers comprehensive threat prevention capabilities.

The increased importance of next-gen email security

Email has become the most critical vector for an assortment of threats, both inbound and outbound. Cyber threats are evolving rapidly from mass spam attacks to advanced forms of targeted attacks. Most of these attack campaigns use email as the choice vehicle to deliver the payload. According to the SonicWall Annual Threat Report, ransomware use grew by 167 times year-over-year and is the payload of choice for malicious email campaigns. However, traditional email security is not equipped to handle advanced threats such as ransomware and zero-day attacks. Today, you need a next-gen email security solution.

Critical capabilities of next-gen email security

The following are critical capabilities that a next-gen email security solution must provide for effective breach prevention:

Advanced threat protection

Most anti-virus solutions are signature-based and therefore ineffective against advanced threats such as ransomware and unknown malware. These types of malware are uniquely hashed and undetectable using traditional techniques. Hence, a sandbox environment is required to detect and prevent ransomware and zero-day attacks before they even reach your network.

Known threat protection

Cyber criminals carry out a number of attacks using known malware. The use of AV signature databases is a simple, effective way to screen such malicious inbound emails and prevent your employees from sending viruses with outbound email. For better
Next-gen email security solutions must provide:

- A comprehensive multi-layer protection for email communications
- Sandboxing and quarantining of any unknown files
- Dynamic reputation-based blacklisting
- Advanced content analysis and pattern recognition
- Strong encryption and DLP for compliance and regulatory requirements

Efficacy, we recommend using multiple virus-detection engines to scan email messages and attachments for viruses, Trojans, worms, and other types of malicious content.

**Phishing protection**

Phishing campaigns have emerged as a top vehicle to deliver payloads for ransomware attacks. Your email security solution must incorporate advanced content analysis that scans every email subject, body and attachment and leverage a sandbox environment for suspicious attachments. In addition, the solution must maintain a real-time dynamic IP blacklist list to filter emails with malicious links.

**Fraud Protection**

Hackers use advanced tactics such as spear phishing, whaling and CEO Fraud to solicit for PII or to carry out scams by impersonating and crafting emails that appear to be authentic. Granular configurations for email settings must be available to prevent illegitimate messages from entering your organization. Mail configurations such as SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting and Conformance), together with pattern recognition and content analysis, enforce proper validation on all incoming messages.

**Spam Protection**

Spam can clog inboxes and network resources, waste businesses time and increase operational costs. Email security should use multiple methods of detecting spam and other unwanted email. These methods include using specific allowed and blocked lists of people, domains and mailing lists; patterns created by studying what other users mark as junk mail and the ability to enable third-party blocked lists.

**Data Loss Prevention**

An organization’s most sensitive communications require the utmost protection. The best measure is to encrypt sensitive emails and email attachments. An encryption service feature must work in tandem with email security to protect emails.

**Conclusion**

Traditional email security solutions rely on static IP reputations and signature-based detection mechanisms, which simply cannot protect against today’s evasive and sophisticated malware. Detection alone does not suffice; often notifications are useless to prevent an ongoing attack. There is a need for email security solutions to move from detection to prevention and have the ability to stop attacks before they even reach your network.

SonicWall next-gen email security solutions use a multi-layer defense approach with award-winning Capture ATP sandbox technology. Capture ATP’s unparalleled breach prevention capabilities defend against advanced threats originating from emails. In addition, it delivers superior anti-phishing, anti-spoofing, anti-Spam, multi-engine AV and data loss prevention (DLP) for comprehensive protection.

To learn more, visit www.sonicwall.com/products/email-security-appliance.
About Us

Over a 25 year history, SonicWall has been the industry’s trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

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

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

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