Datasheet

Trusted by Government, Defence, Enterprise and BFSI Customers

SecneurX
AI-Powered Proactive Cybersecurity

SecneurX Email Security Solution

Product ID: SNX_ATP_ESS_6100

AI-Powered Proactive Cybersecurity for Enterprise Messaging Infrastructure

SecneurX Email Security Solution is a VM Appliance–based messaging security platform designed to prevent enterprise email systems from becoming a vector for threat delivery. Built for government organisations, enterprises, and regulated environments, the solution protects against spam, phishing, malware, zero-day attacks, Advanced Persistent Threats (APT), Business Email Compromise (BEC), and data leakage incidents while ensuring regulatory compliance and operational continuity.

The platform integrates seamlessly with existing email servers and can be deployed as a Mail Gateway, in Transparent (Inline) mode, or as a Fully Featured Mail Server deployment. Whether implemented on-premises or in cloud environments, the architecture is built to support 500+ mailboxes with scalable performance and centralised administration.

Beyond traditional filtering, SecneurX combines signature-based detection, behavior-based analytics, AI-driven intent analysis, sandbox integration, Content Disarm and Reconstruction (CDR), and comprehensive Data Loss Prevention (DLP) into a unified security framework. This ensures that both inbound and outbound communications are continuously inspected, controlled, and protected.

SecneurX Email Security Solution is designed to proactively protect organisations against evolving email-based threats while ensuring operational efficiency and regulatory compliance.

Deployment Architecture and mail flow control

SecneurX Email Security Solution is available as an Appliance or VM-based Appliance, allowing flexible integration into existing enterprise infrastructure. The system supports Mail Transfer Agent (MTA) deployment mode and provides advanced Mail Queue Management capabilities. Administrators can monitor, inspect, release, or manage queued messages through centralised controls, ensuring complete visibility into mail processing workflows.

The architecture is designed to operate in complex network environments while maintaining high throughput, controlled message routing, and policy-driven enforcement across domains.

Advanced Threat Protection & Zero-Day Defense

Email remains the primary attack surface for sophisticated adversaries. SecneurX addresses this challenge through multi-layered Advanced Threat Protection (ATP) that combines signature-based malware detection with behavior-based and heuristic analysis. This layered model ensures detection of both known threats and previously unseen attack patterns.

To combat zero-day malware and Advanced Persistent Threats (APT), the platform integrates sandbox analysis (On-Premise Sandbox and Cloud-based Sandbox options). Suspicious attachments and payloads are detonated in a controlled environment where behavioral indicators are analyzed before delivery. Outbreak Protection mechanisms identify rapidly evolving spam and malware campaigns targeting new vulnerabilities.

The solution's Anti-Spam, Anti-Phishing, and Anti-Malware engines operate in conjunction with AI-driven intent analysis to detect Business Email Compromise (BEC) attempts and social engineering patterns that bypass traditional filtering.

Forged IP Scanner & Sender Validation

A critical feature of the solution is its Forged IP Scanner Tool. The system performs Reverse DNS validation by converting the sender's IP address to a canonical host name and comparing it against officially listed IP addresses associated with that hostname. This process enables detection of spoofed infrastructure and forged sender identities.

In addition, sender identity verification, IP reputation checks, and domain reputation validation strengthen protection against impersonation and domain spoofing attacks.

Datasheet

Inbound & Outbound Email Security with DLP and Encryption

SecneurX Email Security Solution provides comprehensive Inbound and Outbound protection under a unified security framework. All incoming and outgoing messages are inspected using Anti-Spam, Anti-Virus, Anti-Phishing, Anti-Malware, and Outbreak Protection engines. Anti-Blacklisting mechanisms further protect organizational reputation by preventing compromised outbound behavior.

Outbound mail scanning includes Spam Scoring with configurable Block or Quarantine actions. Administrators can apply IP Address Filtering, Sender Domain Filtering, Sender Email Address Filtering, Recipient Filtering, and Content Filtering across Header, Subject, and Body fields. Attachments are inspected using virus scanning, attachment filtering policies, Fingerprint Analysis, Image Analysis, and Intent Analysis to detect embedded threats or unauthorised content transmission.

Data Loss Prevention (DLP)

The built-in Data Loss Prevention (DLP) engine provides comprehensive data-loss prevention with file fingerprinting and sensitive data detection. Policies can be configured to prevent unauthorised data exfiltration by inspecting outbound communications for regulated or confidential information.

File Fingerprinting technology enables detection of sensitive documents even if they are modified, ensuring that protected information cannot be transmitted without authorization

Identity-Based Encryption (IBE)

To support secure communication requirements, the solution includes Identity-Based Encryption (IBE). IBE enables secure message encryption based on recipient identity and supports policy-driven encryption enforcement for sensitive communications. This ensures confidentiality in regulated and high-security environments.

Authentication & Directory Integration

The solution integrates seamlessly with enterprise identity infrastructure. It supports LDAP Integration, Active Directory (AD) Integration, RADIUS Authentication, POP3 Authentication, IMAP Authentication, and SMTP Authentication. These capabilities ensure secure access control and compatibility with enterprise messaging environments.

Datasheet

Policy Enforcement, Authentication & Centralised Management

SecneurX Email Security Solution provides granular policy differentiation capabilities, allowing administrators to define controls based on IP Address, Sender Email Address, Recipient Email Address, Sender Domain, or Recipient Domain. Policies can be enforced selectively across inbound and outbound traffic.

The platform includes a Dictionary Scanning Module that enables administrators to define multilingual keyword dictionaries containing prohibited terms. Emails can be blocked using Header, Subject, or Body filtering with support for exact word matches and regular expressions. This provides flexible content control aligned with organisational policies.

Visibility, Reporting & Integration

Comprehensive management features provide centralised control over messaging security operations. The platform includes Centralised Quarantine Management, Per-Domain Role-Based Administration Accounts, and Role-Based Access Control (RBAC) to support multi-domain deployments.

Administrators benefit from Built-in Reporting Modules, Detailed Message Tracking, Audit Logs, Message Trace functionality, and real-time security dashboards. For integration into broader security ecosystems, the solution supports External Syslog integration, SIEM connectivity, and an Open REST API for configuration and management.

Summary

SecneurX Email Security Solution delivers a powerful messaging security platform for all mailboxes, ensuring that email systems remain protected against modern threat vectors. By combining Advanced Threat Protection, Forged IP Scanner validation, Outbreak Protection, Data Loss Prevention with File Fingerprinting, Identity-Based Encryption (IBE), Mail Queue Management, LDAP/RADIUS/POP3/IMAP/SMTP Authentication, and centralised administrative control, the platform provides a complete enterprise-grade email security solution.

It is purpose-built to meet stringent compliance requirements while delivering operational efficiency, scalability, and proactive protection.

About SecneurX

SecneurX is a 100% Indian cybersecurity company offering advanced solutions like email security, sandboxing, Anti-APT threat intelligence, and file sanitisation. Powered by AI and behavioural analytics, we help organisations detect and neutralise advanced threats. Our solutions are designed for seamless integration and robust protection.