Email Security Essentials

Advanced security and data protection for email

In today's complex cyber-threat environment, you need an email security solution that delivers comprehensive security against sophisticated attacks, while also being easy to deploy, configure, and manage. 3HUE's Email Security Essentials provides complete, cloud-based protection against advanced targeted attacks, helps ensure email continuity, and scans outgoing email to prevent data loss - all without need to install any additional hardware or software.

Comprehensive email threat protection
3HUE's Email Security Essentials protects against phishing, malware, ransomware, and other sophisticated, email-borne threats. Its multi-layered, cloud-hosted scanning engines include Advanced Threat Protection, which combines behavioral, heuristic, and sandboxing technologies.

This lets it protect your infrastructure against zero-hour, targeted attacks and ransomware variants like Locky and CryptoLocker. It automatically scans email attachments in real time; suspicious attachments are detonated in a sandbox environment to observe behavior. Link protection redirects suspicious and typosquatted URLs to protect email recipients against inadvertent malware downloads.

Protection from advanced attacks
Advanced Email Security delivered through 3HUE's Email Security Essentials includes Advanced Threat Protection, a vital security layer that scans email attachments in most commonly used file formats and compares them against a cryptographic hash database. Files of unknown status are detonated in a sandbox environment within the Cloud to observe its behavior, and the result is pushed into the Real Time System to provide protection for all other customers. Emails found to contain malicious content are quarantined and administrators and users can be notified. If no malicious content is found, reular mail processing rules apply.

Maintain compliance through outbound DLP
By scanning all outbound messages, you can ensure that each email leaving is legitimate, virus free, and does not leak private or sensitive information.

For health care providers, governmental agencies, and other entities who need to protect private, sensitive, and valuable information ommunicated via email, DataEndure's Email Security Essentials provides Data Leak Prevention (DLP) features using email encryption. DLP enables your organization to satisfy email compliance filtering for corporate policies and government regulations such as HIPAA and Sarbanes-Oxley (SOX).

Ensure business email continuity
3HUE's Email Continuity ensures that email can still be delivered during email outages or loss of connectivity. Email operations continue by failing over to a cloud-based email service in the event primary email services become unavailable.
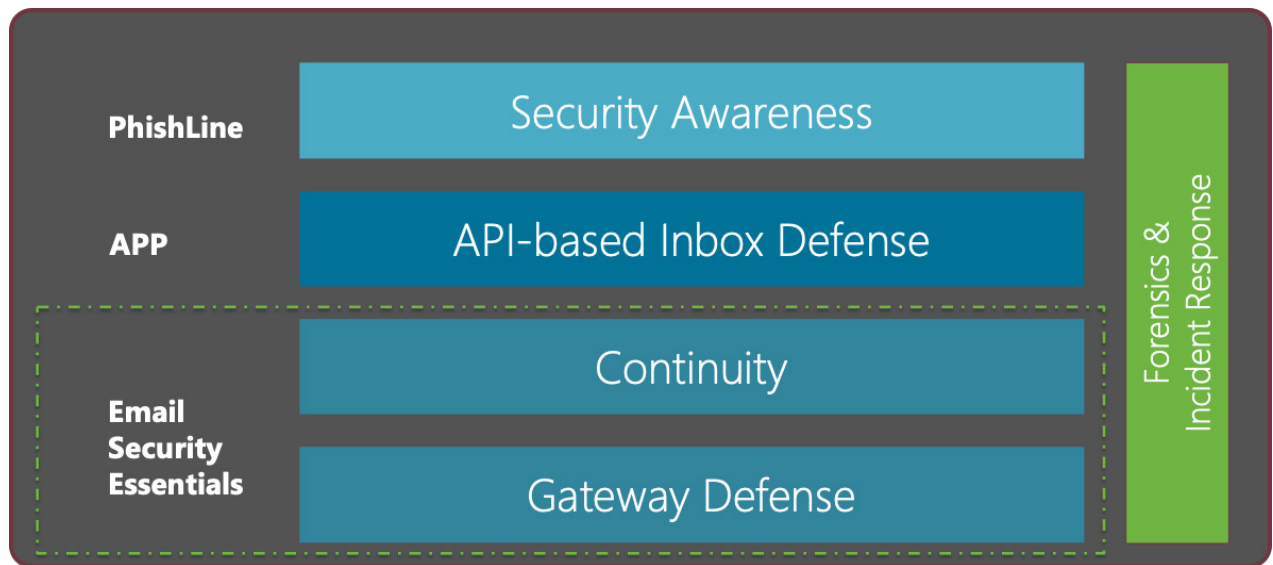
Key Features

Email Security

- Cloud-based protection against:
  - Spam
  - Email-borne viruses (inbound and outbound)
  - Email-based malware
  - Phishing emails
  - Undelivered emails
  - Unsecured emails
  - Denial-of-Service attacks

- Advanced Threat Protection using full-system emulation sandbox

- Agentless email encryption

- Link and URL protection against typosquatting

- Integrated end-user training and exercises to help identify advanced threats

Continuity

- Failover to cloud-based email service to continue operations

- Provides email continuity for up to 96 hours

- Emergency mailbox allows users to send, receive, read, and respond to email

PhishLine	Security Awareness	Forensics & Incident Response
APP	API-based Inbox Defense	
Email Security Essentials	Continuity	
	Gateway Defense	