BAE SYSTEMS
INSPIRED WORK

Insider Threat Prevention

Enterprise-class data loss prevention for email

Email data loss overview

Email is the dominant form of business communication, with highly confidential and personal information passing through it. Most organizations lack an end-to-end view of their infrastructure, which means email can leak and privileged information can inadvertently be disclosed. Safeguarding email is complex, and requires expertise and infrastructure that is cost prohibitive for most organizations. Threats, malware, laws, and regulations are proliferating on a daily basis, and implementing solutions to reduce company risk requires expertise and constant monitoring. Often unable to justify a return on security expenditure, most organizations cannot afford to staff to the levels required for secure email communications. Smaller companies cannot achieve the same economies of scale that larger organizations can, which leaves them the choice between unaffordable capital expenditures and unreliable, less secure service.

A multi-dimensional insider threat prevention solution

While strong oversight of inbound messaging is critical, strict control of outbound messaging is equally important. Insider Threat Prevention from BAE Systems offers content-aware policies normally reserved for standalone enterprise Data Loss Prevention (DLP) technology, and helps government agencies and companies of all sizes guard against insider threats.

With the Insider Threat Prevention solution from BAE Systems, CIOs and IT managers can guard against motivated malicious insiders and accidental negligence by employees to greatly reduce corporate security threats. Our solution breaks new ground in combining ease of use and sophisticated insider threat detection features to protect against confidential and proprietary information loss. It easily integrates with other existing messaging vendors, such as Google and Office 365, as well as any cloud or on-premise email system, including BAE Systems Email Protection Service and BAE Systems Hosted Exchange.

Insider Threat Prevention provides:

- Ready-made and programmable granular policies through an easy to use UI to block, quarantine, redact, or automatically encrypt inappropriate and risky messages using the highly tunable policy-driven rules engine
- Industry-specific Policy Packs to help customers in highly regulated markets with the compliance of GLBA, HIPAA, and PCI DSS
- Infinitely flexible search algorithms, regular expressions, and other advanced action types for best-in-class policy management and hardened protection against confidential and proprietary information loss
- Multiple, customizable tuning levels for effective false-positive reduction.

"Content-aware enterprise DLP deployments are seen more and more as business tools by the business units themselves to address compliance and IP protection mandates than in the past, where it was often seen as an IT/IT security solution looking for a need."

Gartner – Magic Quadrant for Content-Aware Data Loss Prevention, January 2013

Stops sensitive information from leaving your company

Insider Threat Prevention helps companies assess their risk and prevent data loss over the highest points of risk by safeguarding valuable and proprietary data against security threats.

Uses a data in motion approach to identify email messages for:

- Social Security numbers
- Credit card numbers
- Bank account data
- Electronic protected health information (ePHI) and other medical records
- Sensitive intellectual property (trade secrets, sales forecasts, financial disclosures, etc.).

Employs pre-configured and customizable rules for message actions:

- Social Security numbers
- Blocking
- Encryption*
- Quarantine
- Redaction.

We deliver a complete solution:

- Comprehensive end-to-end email security
- Tailor-made Policy Packs to help customers in highly regulated markets with the compliance of GLBA, HIPAA, and PCI DSS
- Policy-driven rules engine integrated into the intuitive Security Management Console
- Real-time message tracing and reporting.

* Requires BAE Systems Email Encryption solution. Additional charges apply.

How Insider Threat Prevention works

Insider Threat Prevention from BAE Systems has advanced analysis features including proximity checking, full redaction capabilities, and the ability to test policies before deploying them. You can easily build and enforce granular policies to block, quarantine, or automatically encrypt sensitive or inappropriate, messages using the highly tunable, policy-driven rules engine in the Security Management Console.

Capability	Customer benefits
Customizable policy libraries	Policy rules and libraries containing lists of words, terms, and advanced data structures, come pre-configured for immediate compliance with HIPAA and other highly regulated data types. Policy libraries and dictionaries can easily be customized for specific applications and targeted content isolation.
Advanced analysis	Proximity checking and advanced, content-aware fingerprinting identifies message headers, body content, and attachments – including, SMTP envelope, IP address, and country/city origin of sender – using industry-leading hash algorithm technology.
Flexible definition framework	Insider Threat Prevention offers the broadest set of risk management dispositions to match individual risk tolerance for extreme accuracy and unsurpassed flexibility – leading to fewer false-positive outcomes.
Security management console	Along with complete integration with the Email Protection Services from BAE Systems, our Security Management Console incorporates extensive rule-building capabilities, including: discovery crawlers, proximity engine, scoring algorithms, incident dashboard, workflow analysis, and comprehensive reporting actions.
Professional services	Our team of certified professionals can create tailor-made solutions and customized policies specific to your organization. Customers benefit from more than 18 years of expertise from a trusted partner that will do the heavy lifting. Throughout the process, customers have an experienced expert as a point of contact.

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

BAE Systems, 265 Franklin Street, Boston, MA 02110, USA
US: +1 (617) 737 4170
E: learn@baesystems.com | W: baesystems.com/businessdefense
linkedin.com/company/baesystemsai
twitter.com/baesystems_ai

CREST
CESG Certified Service Cyber Incident Response
CPNI Centre for the Protection of National Infrastructure