DATA SHEET

INSIDER THREAT PREVENTION.

ENTERPRISE-CLASS DATA LOSS PREVENTION FOR EMAIL.

> Our Insider Threat Prevention solution breaks new ground by delivering enterprise-class DLP features in a highly flexible cloud service.

ABOUT BAE SYSTEMS APPLIED INTELLIGENCE

BAE Systems is the expert provider of messaging and security solutions. We have a strong heritage of hosting and protecting the critical communications and infrastructure of governments and companies around the world.

And, as a technology innovator with numerous security patents, BAE Systems is leading the global information security market by delivering Security-as-a-Service to the commercial market.

Our secure solutions are easy to buy and easy to use, offering built-in compliance and reliability you can trust.

"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

EMAIL DATA LOSS OVERVIEW

Email is the dominant form of business communication. And highly confidential and personal information must be transferred through it. Most organisations 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 organisations. 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 organisations cannot afford to staff to the levels required for secure email communications. Smaller companies cannot achieve the same economies of scale that larger organisations 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 BAE Systems Applied Intelligence Insider Threat Prevention solution, CIOs and IT managers can guard against motivated malicious insiders and accidental negligence by employees to greatly reduce corporate security threats. BAE Systems 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 our Hosted Exchange. Insider Threat Prevention provides:

+ Ready-made and programmable granular policies 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

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 CUSTOMISABLE RULES FOR MESSAGE ACTIONS:

+ Blocking
+ Encryption*
+ Quarantine
+ Redaction

WE DELIVER A COMPLETE SOLUTION

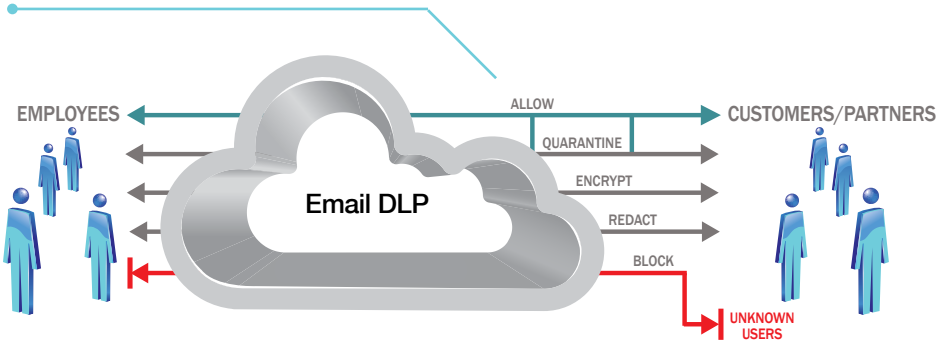
+ Comprehensive end-to-end email security
+ Tailor-made Policy Packs to help customers in highly regulated markets with the compliance of GLBA, HIPAA, and PCI DSS
+ Policy-driven rules engine integrated into the intuitive Security Management Console
+ Real-time message tracing and reporting

* Requires BAE Systems Email Encryption. Additional charges apply.

To learn more about our Insider Threat Prevention solution and how it integrates with existing products to help stop important information from leaving companies, contact us at learn@baesystems.com

HOW INSIDER THREAT PREVENTION WORKS

Insider Threat Prevention from BAE Systems Applied Intelligence 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
Customisable 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 customised 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 BAE Systems Email Protection Services, the 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 customised policies specific to your organisation. 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.

BAE Systems Applied Intelligence, Surrey Research Park, Guildford, Surrey GU2 7RQ, UK

T: +44 (0) 1483 816000 | E: learn@baesystems.com | W: www.baesystems.com/ai.com

www.linkedin.com/company/baesystemsai

www.twitter.com/baesystems_ai