

DATA GUARD MAIL APPLIANCE

Discover and Protect Emails Containing Sensitive or Critical Data

Data protection is recognised as a critical corporate governance issue with increasing legislative and compliance standards requiring imperatives for action in this area. PixAlert recognises and understands the complexity involved in creating viable Data Leakage Prevention (DLP) solutions particularly for organisations starting out on the path of compliance programs.

PIXALERT'S DATAGUARD MAIL APPLIANCE SOLUTION

PixAlert's DataGuard MailAppliance is a proactive data protection tool which provides ongoing email safety for organisations, analysing and intercepting outbound mails containing exposed, sensitive and critical data. DataGuard MailAppliance is a hardware appliance which scans email messages in real time (including attachments), flagging suspect material for review and categorisation and protecting corporate reputation by eliminating risk caused by dissemination of unsecure data content via email.

PRODUCT FEATURES

* DISCOVERS

Scans emails to discover, identify and classify exposed and sensitive data, securing critical information

* RELIABILITY

Can be configured with back-up nodes for redundancy to ensure no downtime in mail traffic

* SCALEABILITY

Through its distributed architecture, the application has the capability to scale small to very large email systems

* COMPREHENSIVE

No other application scans as many file attachment types including movies, email, zip files, Microsoft Office files, PDFs

* AUDIT

Audits emails compatible with SMTP protocol such as Microsoft Exchange, Sendmail

* CONFIGURABLE

Enables administrator to reject, bcc or redirect flagged email

* REVIEW & CLASSIFY

Enables management to review scan results, categorise and preview reports

* DETECTION

Detection of sensitive or regulated information and client specific data

* CUSTOMISE

Rules engine for custom expressions, built to seek specific data needs

* NON-DISRUPTIVE

Zero impact on productivity or mail, only 'at risk data' stopped

* COMPATIBLE

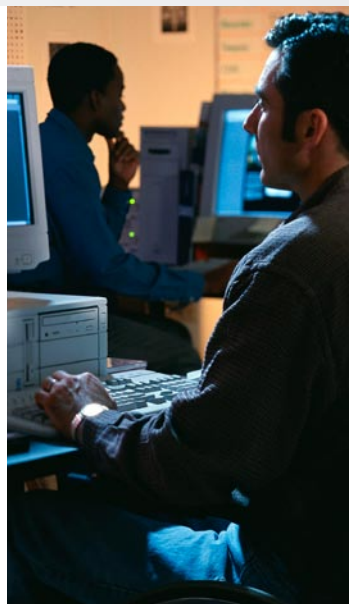
Compliments existing IT security, audit, governance and compliance measures

* SPEED

Rapid real time scanning of outbound emails and attachments

* REPORTING

Generates comprehensive reports with assessments of email related data leakage incidents and up-to-date management visibility



PRODUCT BENEFITS

* REDUCE RISK

Discover and protect emails containing sensitive and critical data

* ENFORCE COMPLIANCE

Assists with compliance capabilities with PCI DSS, ISO 27001, SOX and HIPPA standards; check's compliance with data retention, data protection acts and other legislation.

* COST

Reduce potential financial risk and exposure through measurably identifying and safeguarding intellectual property leakage through email.

* MANAGEMENT

Generate manageable and meaningful output through comprehensive management reporting features.

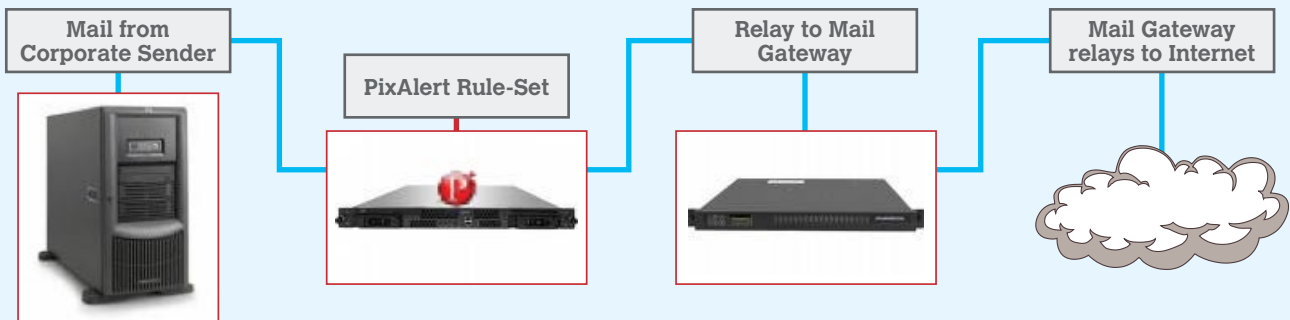
WHO SHOULD USE PIXALERT DATAGUARD MAILAPPLIANCE

- * Organisations embarking compliance programmes including:
 - * PCI DSS – Payment Card Industry Standard
 - * Data classification programs
 - * PII identification & consolidation
 - * Data protection compliance programs
 - * ISO27001 – continuous monitoring & reporting
- * DataGuard MailAppliance should also be considered by IT Managers, IT Security Professionals; Risk and Compliance Leaders.
- * Organisations who value risk visibility as a means of addressing and optimising operating efficiencies across their networks and who value the integrity of their brand and corporate reputation

DATAGUARD MAILAPPLIANCE CAN AID COMPLIANCE WITH SPECIFIC STANDARDS SUCH AS

- * Sarbanes Oxley Act
- * Basel II
- * EU data retention directive
- * UK Data Protection Act
- * EU Markets in Financial Instruments Directive
- * EU Audit and Privacy Directives
- * SB-1386: Security Breach Information Act
- * Gramm-Leach Bliley Financial Services Modernisation Act

HOW DATAGUARD MAILAPPLIANCE WORKS



FEATURES & SPECIFICATIONS

What Type Of Information Does DataGuard MailAppliance Search For:

PixAlert DataGuard MailAppliance can be used to detect both structured data patterns (such as credit card numbers, social security numbers and passport data) and occurrences of unstructured search terms (such as a company or product name, a specific social security number or address etc) within email.

Search types can be combined, for example DataGuard MailAppliance may be tasked to find all email documents containing any credit card number associated with a particular account holder or any mail containing specific data sent outside of the organisation from a particular email address.

Once a combination of search terms has been determined by the user, DataGuard MailAppliance can index all mails found matching the search terms. More refined searches may then be rapidly executed against the indexed data.

PixAlert DataGuard MailAppliance System Requirements

- * PixAlert DataGuard MailAppliance system is designed to run either as a stand-alone or distributed system.
- * Each node of the system is capable of handling up to 100,000 emails per day.