DIGITALGUARDIAN®

HPE SecureMail and Digital Guardian

> ## BEST-IN-CLASS POLICY-BASED EMAIL ENCRYPTION FOR AUTOMATED REGULATORY COMPLIANCE AND DATA PROTECTION

Key Benefits

- Enables secure communications: Provide secure communication to protect personally identifiable information (PII), protected health information (PHI), payment card information (PCI), and other sensitive information from external exposure.

- Supports compliance: Delivers secure communication for PCI, PHI, PII, and other regulated data.

- Automates encryption: Integrates HPE SecureMail and Digital Guardian without changes in workflow for users; encryption is automatic based on pre-defined classification rules to eliminate mistakes and protect against malicious insiders.

- Eliminates security gaps: Connects security solutions while eliminating gaps when handoffs occur; the combination of HPE SecureMail and Digital Guardian DLP create a best-of-breed pair for the ultimate in secure communication.

THE NEED

Despite the rise in instant messaging and file sharing, email remains the de facto method for business communication. With this flexibility comes the risk of misuse—either intentionally or inadvertently—that can expose sensitive information about clients, patients, customers, or internal business operations. This exposure can lead to penalties for non-compliance, loss of trust in the market, and even potential revenue loss. Organizations need an integrated and automated solution to protect this communication tool without slowing the speed of business or adding complexity.

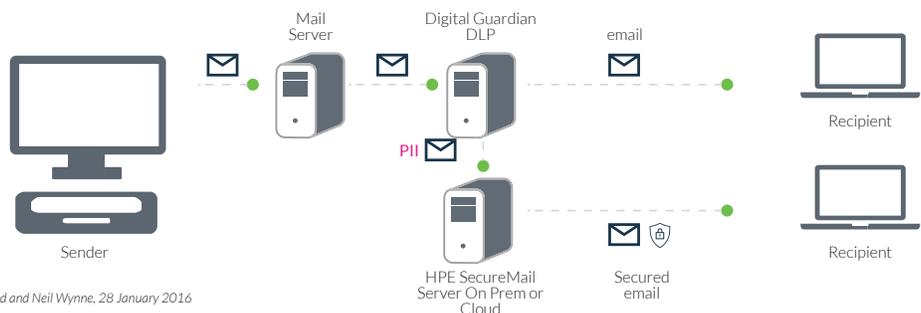### HPE SecureMail and Digital Guardian

Integrating the end-to-end encryption from HPE SecureMail and advanced Data Loss Prevention (DLP) from Digital Guardian provides an automated, policy-based email encryption solution with industry-proven data monitoring and protection policies. The solution helps companies maintain regulatory compliance and reduce the risk of data loss.

HPE SecureMail is the best-in-class encrypted email solution available for desktop, cloud, and mobile that easily scales to protect millions of users. HPE SecureMail is used by some of the largest banks, insurance companies, and healthcare organizations in the world to ensure email protection for sensitive information shared internally among employees and externally with customers and partners.

Digital Guardian is a leader in data protection, from the endpoint to the cloud and everywhere in between. The network data loss prevention (NDLP) solutions from Digital Guardian deploy quickly, require minimal ongoing support, and provide visibility to traffic as it moves through and exits your network. This platform is recognized as a leader in the 2016 Gartner Magic Quadrant for Enterprise Data Loss Prevention[1].

SOLUTION OVERVIEW

Digital Guardian DLP inspects and classifies email as it is sent. If Digital Guardian determines that the message contains sensitive content, HPE SecureMail automatically encrypts it. HPE SecureMail can be deployed either on-premise or as a cloud service. Digital Guardian delivers a comprehensive library of pre-defined, industry-specific policies to help organizations immediately protect their sensitive data and comply with regulatory requirements.

USE CASES

HIPAA COMPLIANCE: ENSURE SECURE COMMUNICATION OF SENSITIVE PATIENT INFORMATION.
Physicians routinely consult with specialists about patient care, which may necessitate emailing patient lab results with other physicians. This communication requires data encryption to prevent unauthorized viewing. When a physician sends unencrypted email, the Digital Guardian appliance inspects the content and if sensitive information is found, it forwards the document for encryption with HPE SecureMail prior to sending to the intended recipient.

PII PROTECTION: MAINTAIN CUSTOMER TRUST BY PROTECTING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.
Customer databases are one of the most valuable assets to an organization; the entire list can be exported and sent either via a well-meaning or malicious actor. Digital Guardian analyzes messages for PII if sensitive information is found the email and attachment are marked and sent to the HPE SecureMail service for encryption prior to sending to the recipient.

ABOUT HPE SECURITY - DATA SECURITY

HPE Security—Data Security drives leadership in data-centric security and encryption solutions. With over 80 patents and 51 years of expertise, we protect the world's largest brands and neutralize breach impact by securing sensitive data at rest, in use, and in motion. Our solutions provide advanced encryption, tokenization, and key management that protect sensitive data across enterprise applications, data processing IT, cloud, payments ecosystems, mission-critical transactions, storage, and Big Data platforms. HPE Security—Data Security solves one of the industry's biggest challenges—how to simplify the protection of sensitive data in even the most complex use cases.

ABOUT DIGITAL GUARDIAN

Digital Guardian's unique data awareness and transformative endpoint visibility, combined with network security, behavioral threat detection and response, and cloud data protection secures organizations' sensitive data by enabling a data centric security strategy. The company's flagship product, the Digital Guardian Data Protection Platform, is purpose built to stop data theft and make it easier to see and stop all threats to sensitive data.

For more than 10 years, Digital Guardian has enabled data-rich organizations to protect their most valuable assets with an on premises deployment or an outsourced managed security program (MSP). The company operates in more than 60 countries while servicing seven of the top ten global patent holders and seven of the ten largest global automobile manufacturers are customers.

**Hewlett Packard
Enterprise**

Data
Security
Tested

Learn More at
voltage.com
hpe.com/software/datasecurity
DigitalGuardian.com

SHARE