SOLUTION SHEET

DIGITALGUARDIAN®

Zix®

Digital Guardian is a next generation Data Loss Prevention (DLP) platform designed to stop data theft. Digital Guardian enables companies to effectively discover, monitor, control and secure sensitive data, whether on the network, at rest on network servers, or stored in the cloud.

Our approach is recognized for delivering the lowest total cost of ownership with no dedicated resources required to manage. It utilizes our Data Base Record Matching technology that is the industry's most accurate for identifying and controlling structured data types such as PHI and PCI. By focusing on protecting personally identifiable and confidential information, we provide hospitals, banks and other organizations with the lowest false positive rate of any technology available.

The Digital Guardian (DG) suite includes Network DLP, Discovery DLP and Cloud DLP.

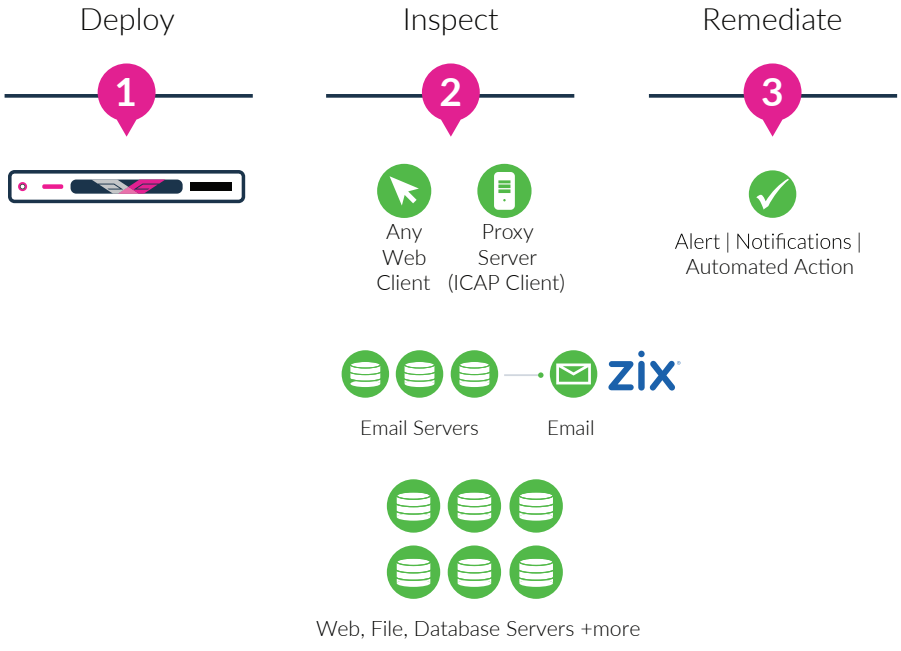
DG FOR NETWORK DLP

PREVENT NETWORK DATA LOSS

Digital Guardian Network DLP monitors and controls network communications to prevent sensitive data from leaving your network and support compliance efforts. It's enterprise DLP without the complexity. Digital Guardian monitors and controls communications channels, inspecting network traffic then enforces policies to ensure protection. Policy-based actions includes: allow, prompt, block, encrypt, reroute and quarantine.

BENEFITS

- Enable secure business processes
- Support secure data communications and compliance
  - Email, Webmail, Web apps
  - HTTP/S, FTP/S, TCP/IP
- Educate users with real-time prompts
- Log violations for administrators
- Zix Email Encryption with Best Method of Delivery



DIGITALGUARDIAN®

zix®

For more information, visit
www.zixcorp.com

DG FOR DATA DISCOVERY

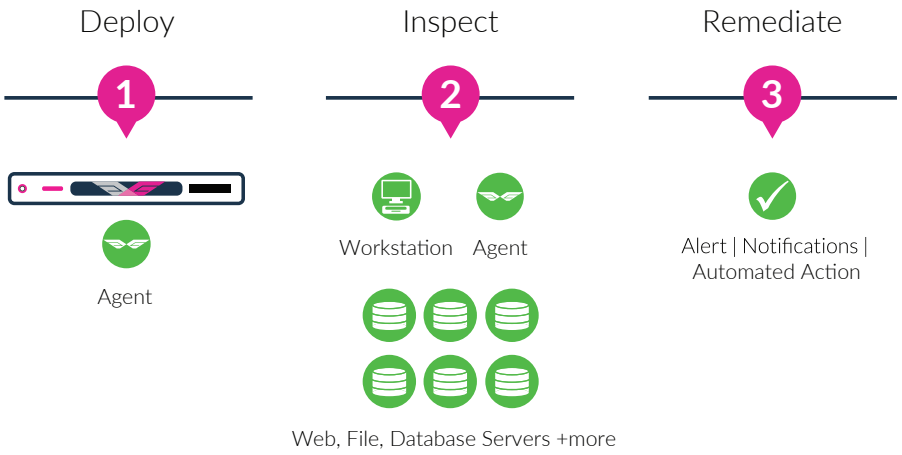
FIND, CLASSIFY AND REMEDIATE SENSITIVE DATA

Digital Guardian for Data Discovery provides visibility and auditing of potentially unsecured data.

Automatic, configurable scanning of local and network shares using specific inspection policies to ensure sensitive content is discovered where it is located. Detailed audit logging and reports provide you with the information needed to demonstrate compliance, protect confidential information and reduce data loss risk.

BENEFITS

- Locate and identify sensitive content on endpoints, servers, shares, and databases.
- Visibility into and reporting of sensitive content or data without appropriate controls
- Automatic remediation and removal of sensitive files
- Document data security and privacy compliance



DG FOR CLOUD DATA PROTECTION

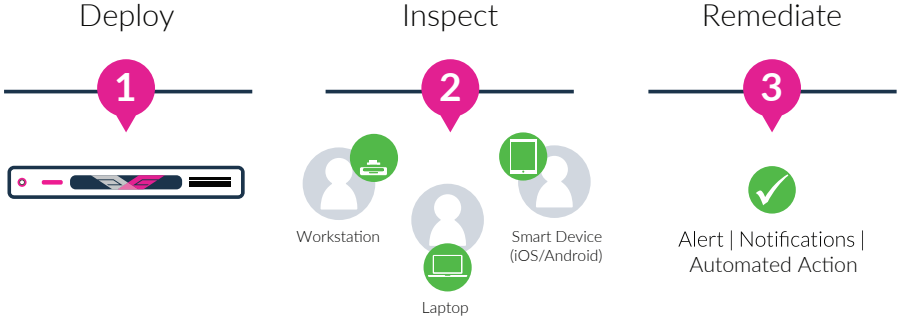
AUDIT AND PROTECT SENSITIVE DATA IN THE CLOUD

Digital Guardian Cloud Data Protection allows your organization to adopt cloud storage while maintaining the visibility and control you need to comply with privacy and data protection regulations.

Integrating with leading cloud storage providers such as Accellion, Box, Citrix, ShareFile, Egnyte and Microsoft, Digital Guardian scans file servers, enabling encryption, removal, or other remediation of sensitive data before the file is shared in the cloud. Data that is already stored in the cloud can be scanned and audited at any time. User data being placed in cloud storage is scanned in real-time to enforce policies before data leaves your control.

BENEFITS

- Enable compliant cloud storage adoption
- Visibility into cloud data
  - Administrator
  - Data Owner
- Educate users with real-time prompts
- Audit and remediate



DIGITALGUARDIAN®

zix®

For more information, visit
www.zixcorp.com

Digital Guardian and Zix

Digital Guardian and Zix have joined forces to provide the best of both worlds – powerful and accurate data loss prevention together with "secure send to anyone" email encryption.

The Need

Instant messaging and file sync and share applications facilitate collaboration, but email remains the top business communication tool. As a result, email is the primary vector for data loss, either from users trying to steal sensitive data, or who are unaware that their actions may be risky. In a highly regulated industry such as Financial Services and Healthcare this can lead to fines; in others industries, there can be loss of competitive advantage. In either, negative publicity can lead to lost business, customer churn and damaged reputation. Organizations need an integrated and automated way to detect sensitive information and apply security controls in real-time and without complexity.

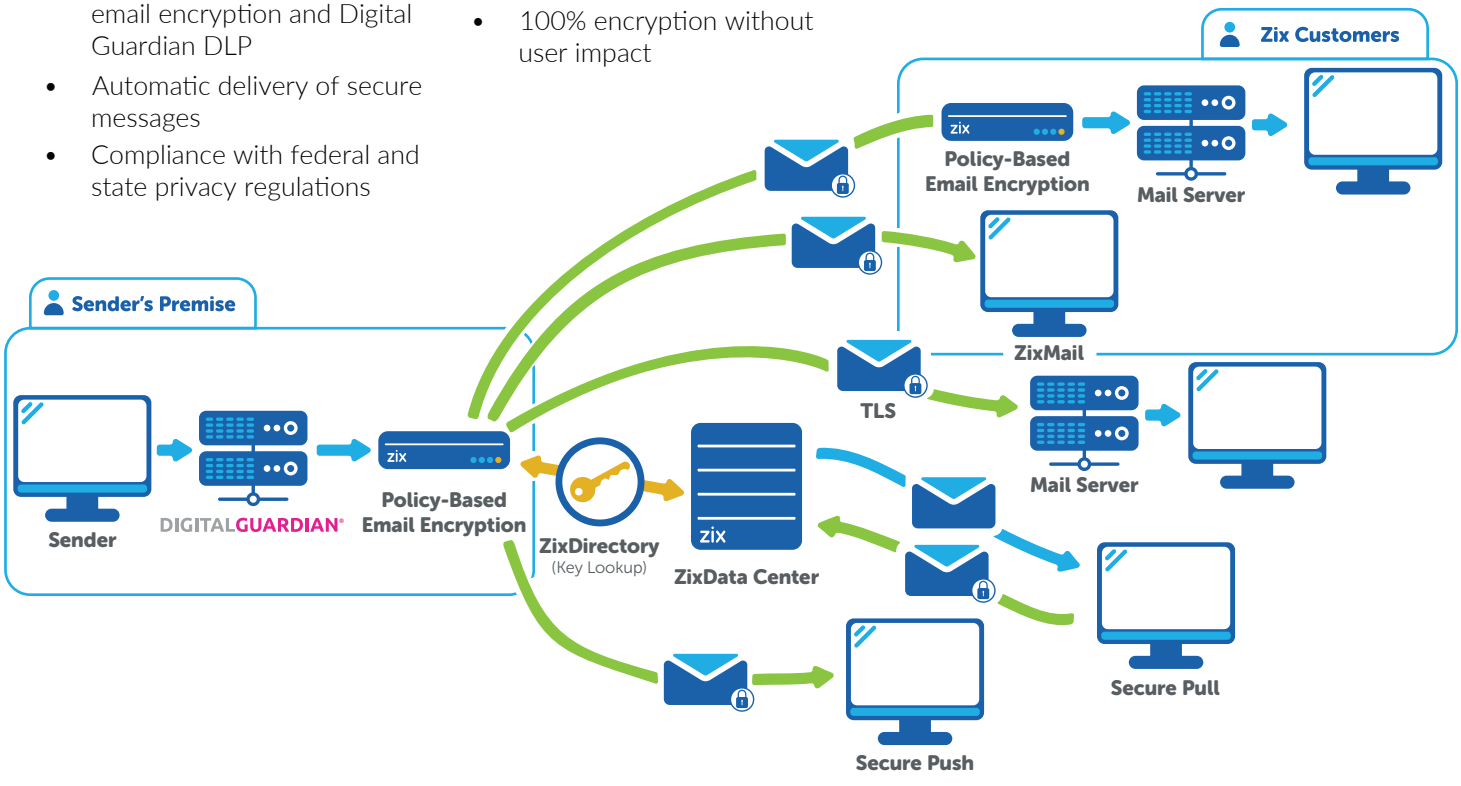
Integrate and Automate Email Encryption with Digital Guardian and Zix

Digital Guardian offers sophisticated content inspection and detection capabilities to recognize and protect sensitive data. The ability to accurately detect sensitive information using fingerprinting provides data loss protection that is extremely accurate and powerful.

Digital Guardian DLP inspects and classifies email as it is sent. If Digital Guardian determines that the message contains sensitive content, Zix encrypts email content and any attachments before sending. Zix automatically determines the most efficient way to securely deliver your email messages using our patented Best Method of Delivery. Through the Zix Best Method of Delivery, encrypted email is delivered to anyone, anywhere and often transparently. When you send an encrypted email to another Zix customer, the message and replies are encrypted without any extra steps or hassle for both senders and recipients.

BENEFITS

- Best-of-breed pairing of Zix email encryption and Digital Guardian DLP
- Automatic delivery of secure messages
- Compliance with federal and state privacy regulations
- Seamless mobile experience
- 100% encryption without user impact



DIGITALGUARDIAN®

zix®

For more information, visit
www.zixcorp.com

WHAT MAKES DIGITAL GUARDIAN UNIQUE

1 THE INDUSTRY'S MOST ACCURATE TECHNOLOGY FOR IDENTIFYING & CONTROLLING PII & PHI

Our unique fingerprinting technology is the industry's most accurate for identifying and controlling PII & PHI. By focusing on protecting PII/PHI, we provide the absolutely lowest false positive rate of any technology available. This allows your team to **focus on the real risks.**

"Within literally minutes of the appliance being plugged in, we started collecting data. Once we saw items that could become major issues for us, we were able to remediate potential problems right away."

- Steve Scott, Information Security Manager, Saint Charles Health System

St. Charles HEALTH SYSTEM

2 SINGLE APPLIANCE APPROACH SIMPLIFIES DEPLOYMENT & MANAGEMENT

Digital Guardian's Content Inspection engines combine content inspection, policy creation, and management in one, greatly simplifying deployment and management without sacrificing accuracy or effectiveness. our approach is recognized for delivering the lowest total cost of ownership with **no dedicated resources required to manage.**

"Implementation is greatly simplified by the single appliance approach, with average deployment times much shorter than other DLP products. Implementations can often be completed in a single day, with only minimal policy tuning required thereafter."

- Data Loss Prevention Leading Vendors Review, DLP Experts, Jan 2016

DLPX DATA LOSS PREVENTION EXPERTS

3 COMPREHENSIVE COVERAGE – NETWORK, ENDPOINT, DISCOVERY & CLOUD DLP

A complete data loss prevention solution – network, endpoint, discovery, and cloud – all managed from one pane of glass. Unlike others, our **DLP coverage extends to the cloud**, allowing your organization to adopt cloud storage while maintaining the visibility and control you need to comply with HIPAA, PCI and other regulations.

4 VISION

The Digital Guardian Network DLP and Digital Guardian for Data Discovery products cover network DLP, cloud data protection and data discovery and is an excellent choice for organizations with strong regulatory compliance concerns both today and in the future.

"Digital Guardian's vision demonstrates a strong understanding of the technology, security, threat landscape and industry trends that will shape its offerings going forward."

- Gartner, MQ for Enterprise DLP, Feb 2017

Gartner

ABOUT DIGITAL GUARDIAN

Digital Guardian is the only data aware security platform designed to stop data theft. The Digital Guardian platform performs across traditional endpoints, mobile devices and cloud applications to make it easier to see and stop all threats to sensitive data. For more than 10 years we've enabled data-rich organizations to protect their most valuable assets with an on-premises deployment or an outsourced managed security program (MSP). Our unique data awareness and transformative endpoint visibility, combined with behavioral threat detection and response, let you protect data without slowing the pace of your business.

SHARE