Datasheet

Data Loss Prevention

with WatchGuard® XCS Solutions

PROTECT CONFIDENTIAL DATA AS IT MOVES OUTSIDE YOUR ORGANIZATION'S

WatchGuard XCS email security solutions automatically incorporate powerful data loss prevention (DLP) capabilities to ensure that the content of outgoing email messages is in strict accord with your organization's confidentiality and regulatory compliance policies. Adding an XCS Web Security subscription (available for all XCS models) extends those capabilities to your web-based traffic as well, for comprehensive coverage across protocols.

DATA LOSS PREVENTION IS BUILT INTO ALL WATCHGUARD® XCS APPLIANCE MODELS AS A POWERFUL BUSINESS TOOL FOR CONTROLLING CONFIDENTIAL INFORMATION AS IT MOVES ACROSS NETWORK BOUNDARIES.

This allows you to protect the growing volume of private data that traverses your network to prevent accidental or malicious data leakage in a single solution, without the need for multiple point products.

Data loss prevention and privacy tools give you the ability to both secure information as needed to maintain policy compliance, as well as share authorized sensitive information securely with business partners outside the company.

With a WatchGuard XCS appliance, you have an automatic, extensive risk management and policy enforcement boundary of outbound content. This ensures privacy and compliance, but does not impede the flow of your legitimate electronic business communications.

HOW DATA LOSS PREVENTION WITHIN YOUR CORPORATE EMAIL SYSTEM WORKS

SIMPLIFIED AND EFFECTIVE POLICY MANAGEMENT

- **DLP Wizard** guides administrators through DLP configuration controls quickly and simply, allowing you to gain privacy and compliance and define remediation actions with a few simple clicks.
- **Centralized policy** management provides a single point of administration for creating, managing and enforcing content security and data loss policies to eliminate data loss gaps.
- **Pre-defined compliance dictionaries** streamline the policy-setting process for HIPAA, PCI, GLBA and other regulations, and are customizable to conform with your unique business requirements and compliance regulations.
- **Custom policies** for groups or individuals can be set to control who can send what and to whom without impeding critical business processes. Content controls include flexible and granular tools including the ability to set complex rules and even nest rules within one another.

POWERFUL CONTENT & CONTEXTUAL ANALYSIS ACCURATELY DETECTS POLICY VIOLATIONS

- **Defense-in-depth** methodology scans all outbound content (including files and attachments) and inspects context of the traffic (who is sending the data, where or to whom) to determine if there is a policy violation.
- **Attachment scanning & control** provides the ability to apply existing content scanning policies to more than 400 file attachment types. Compressed file attachments can also be scanned to ensure sensitive information does not leave the organization.
- **Applied intelligence** learns from previously allowed content to make future decisions more accurately and faster.
- **Data discovery and classification tools** allow you to protect known confidential or sensitive data files, thereby training the system on what to look for and subsequent remediation actions to be taken upon discovery of such data.

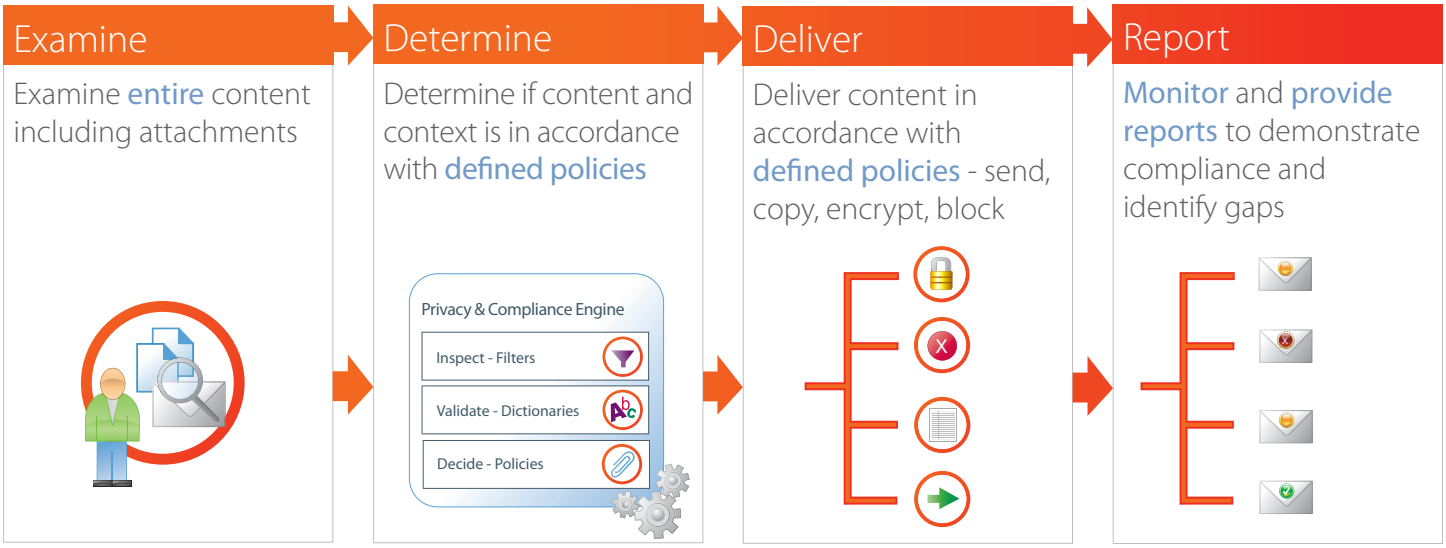
TRANSPARENT REMEDIATION PROVIDES UNPARALLELED CONTROL & VISIBILITY

- **Instant-on remediation actions** are instantly applied when policy violations are detected for transparent protection, control and visibility of information leaving your organization. Options include block, quarantine, allow, encrypt, blind copy, or reroute content.
- **Seamless email encryption**, easily added to your solution with a WatchGuard SecureMail Email Encryption subscription, allows you to securely transmit and receive private, sensitive, and regulated information without hindering the free flow of critical business communications.

GRANULAR LOGGING AND REPORTING FOR AUDIT REQUIREMENTS

- **Policy violation alerts** and the remediation actions taken are triggered instantly for immediate visibility.
- **Granular logs and one-click administration** for customizable reports of policy violations are easily accessible to meet audit requirements.

INTEGRATED PROCESS FOR PRIVACY AND COMPLIANCE PROTECTION



WATCHGUARD XCS INTEGRATED PROCESS FOR DATA LOSS PREVENTION

Data Loss Prevention is integrated into all WatchGuard XCS models. It provides comprehensive, instant protection from information loss. The system uses an integrated process for inspection, discovery, and remediation of policy violations for outbound communications containing sensitive content.

1. **Examine.** Outbound communications are checked for private or sensitive data, including personal information and intellectual property.
2. **Determine.** The sophisticated XCS policy engine determines the appropriate action to take on a message, based on pre-defined policies.
   - Policies are determined by the organization using customizable templates that aggregate internal policy with compliance-driven regulations
   - Industry-specific compliance dictionaries, including dictionaries for PCI, HIPAA and GLB, help make policy generation fast and effective.
3. **Take Action:** Take the appropriate action on the message instantly, without the need for manual intervention. Depending on pre-defined policies, the message can be allowed, blocked, encrypted, copied to a compliance officer, stamped, returned to sender, and/or entered in the audit/log.
4. **Report.** It is important to be able to easily document the policies that have been implemented to enforce the regulations, as well as tracking actual message traffic to ensure compliance. XCS solutions provide granular logs for customizable reports of violations and remediation action taken to meet audit requirements.

EXTEND DATA LOSS PREVENTION TO WEB TRAFFIC

The Web provides many exit points for sensitive information to leave your organization, including communications sent by popmail systems (hotmail, gmail, etc.), wikis, blogs, and social networks such as Facebook. Adding a Web Security subscription extends the data loss prevention capabilities of your XCS appliance* to include HTTP traffic, for comprehensive protection across protocols.

- Scans content in all outbound web traffic, including attachments, for policy violations.
- Inspects context in which communication is sent including who is sending the data, where it is being sent, and to whom.
- Uses the same policies developed for your organization's email communications to save time and ensure strong and consistent enforcement.
- Allows administrator to manage data loss prevention across protocols from one easy-to-use administrative console.
- Provides consolidated visibility and control so you can meet stringent compliance requirements.

* Web Security subscriptions are available for all XCS models.

For more information on Data Loss Prevention capabilities and our complete line of powerful WatchGuard XCS solutions, visit www.watchguard.com/xcs.

ADDRESS 505 Fifth Avenue South, Suite 500, Seattle, WA 98104 WEB www.watchguard.com U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895