

**MXtreme™
Overview**

MXtreme™ Overview

MXtreme™ is a comprehensive email security, privacy and compliance solution that enables organizations to prevent inbound threats, control outbound content and centrally manage the email infrastructure. MXtreme is the only highly available email security solution with F5 and Cisco device integration, message-level redundancy and on-demand clustering capabilities. MXtreme allows organizations to:

Prevent

- Eliminate threats at the perimeter
- Reduce email volume
- Lower operational costs
- Consolidate point products

Control

- Control inbound and outbound content
- Comply with regulations
- Protect confidential information
- Reduce risk

Manage

- Advanced content management and policy enforcement
- Message-level redundancy
- On-demand scalability and resiliency
- Centralized audit and compliance-specific reporting

Prevent – attacks and block malicious and unwanted traffic for both inbound and outbound content to reduce risks and email volume

Control – both inbound and outbound content and confidential information to enforce corporate policies and reduce legal liability

Manage – email security and policies centrally to ensure appropriate policy enforcement, operational efficiency and optimal Quality of Service (QoS)

MXtreme Email Security Solution

The MXtreme Email Security Solution takes a new multi-layered approach to email security to proactively detect and prevent all email threats, including blended attacks and zero-day exploits. MXtreme offers an integrated approach that is a complete solution for email, consolidating disparate point solutions to prevent all email-based threats in one system.

MXtreme Privacy and Compliance Solution

The MXtreme Privacy and Compliance Solution provides unprecedented granular content management that is integrated with secure content delivery to ensure information is secure and regulatory requirements are met. By controlling both inbound and outbound messages while providing a balance between privacy and usability, MXtreme enables organizations to enforce corporate policies while controlling and protecting the confidentiality and integrity of information required by corporate and regulatory requirements.

Prevent...

“Over half of all viruses these days are created to launch other attacks, such as Denial of Service or Spam.”

Radicati, 2005

“Spam traffic comprises 74% of all consumer email traffic. This number is expected to rise to 85% by 2009.”

Radicati Group, March 2005

“The volume of spam continues to increase for companies, and Gartner clients routinely report 80 to 90% of all incoming email they believe is spam.”

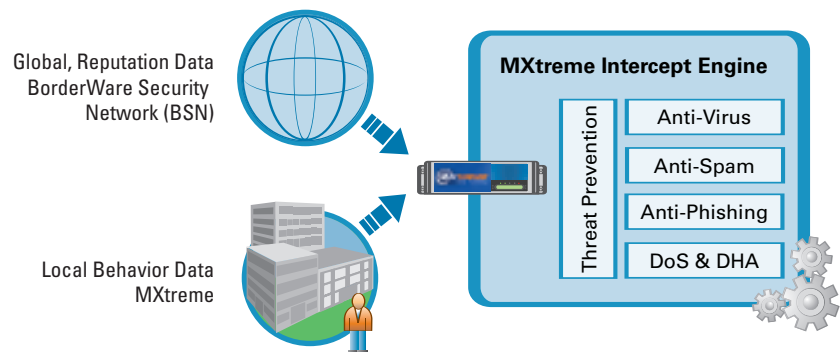
Gartner, 2005

MXtreme Email Security Solution

Market Leading, Proactive, Real-time Threat Protection with the MXtreme Intercept™ Engine

While most anti-spam products incorporate anti-virus capabilities as part of their solution, they fail to properly address new and evolving email threats such as Denial of Service (DoS), Directory Harvest Attacks (DHA), phishing, and blended threats. As organizations are increasingly exposed to these attacks, blocking all email security threats in one solution before they damage a corporate network and hinder employee productivity has become increasingly important.

The MXtreme Intercept™ Engine takes a new and innovative approach to block upwards of 98% of unwanted inbound email by allowing organizations to detect and block incoming threats in real-time at the email boundary. By making real-time decisions based not only on sender reputation but also on message content and email server behaviour, the MXtreme Intercept Engine provides a new level of precision and performance for threat detection and zero-day protection.



Combining global, reputation data from BorderWare Security Network (BSN) with local information from the MXtreme Intercept Engine provides dynamic, real-time threat prevention.

Spam, Virus & Denial of Service Protection with the MXtreme Intercept Engine

The MXtreme Intercept Engine provides the most powerful approach for detecting and eliminating unwanted email allowing administrators to make a more informed and accurate decision about the validity of incoming mail messages. MXtreme Intercept Engine combines the most effective anti-spam, anti-virus and threat prevention technologies together to deliver a system with the industry's highest effectiveness and lowest number of false positives.

Anti-Spam

MXtreme Email Security Solution provides complete control over the way spam and malicious emails are handled and actioned. With powerful default settings and simpler actions, administration is eased allowing IT administrators to get up and running faster, ensuring spam is detected immediately. By tracking multiple threat types in real-time, the MXtreme Intercept Engine has the ability to make a more informed and accurate decision by blocking more threats, more effectively.

Anti-Virus

In addition to spam, the MXtreme Intercept Engine addresses email-borne viruses, worms, Trojans and other types of malicious attacks that continue to pose a substantial threat to organizations. The MXtreme Email Security Solution provides several anti-virus options giving customers a choice of enterprise-class virus protection. The MXtreme Intercept Engine anti-virus protection scans both inbound and outbound messages for potentially malicious content. Administrators have flexible configuration options to determine how messages should be handled based on the results of the virus analysis from the MXtreme Intercept Engine.

Anti-Phishing

Phishing is currently a tremendous email security burden that results in email fraud and identity theft by deceiving a victim into providing confidential financial or personal information. MXtreme Email Security Solution reduces phishing attacks by combining DomainKeys with Sender Policy Framework (SPF) to validate senders with the MXtreme Intercept Engine. Together these technologies make an informed decision about whether a message is actually being sent by who it says it is, ensuring that imposters will not find victims in an organization that is protected by the MXtreme Email Security Solution.

Denial of Service & Directory Harvest Attacks

The MXtreme Intercept Engine provides the most comprehensive threat prevention to protect against new and evolving attacks such as DoS and DHA. These types of attacks are not used to communicate with end users, rather their purpose is to extract email user data and/or bring down email systems.

Zero-Day Defense

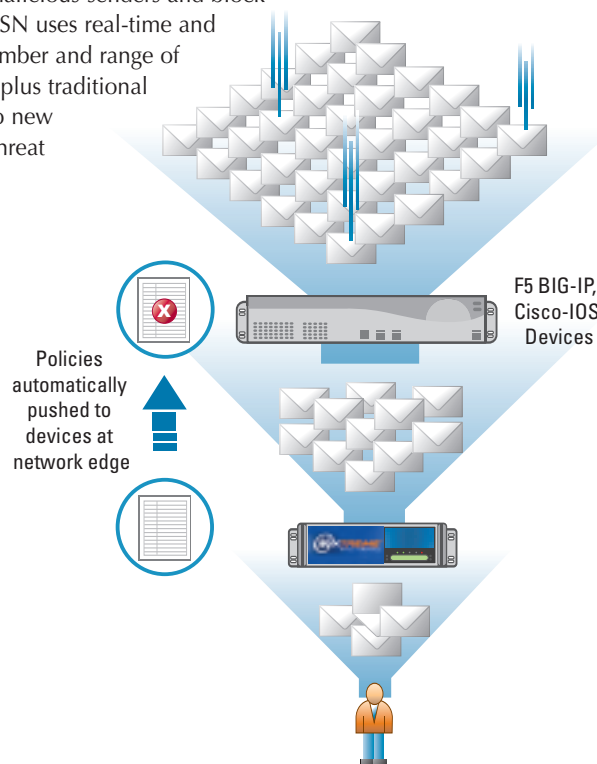
During any virus outbreak, there is invariably a period of time between virus detection and when the actual anti-virus signature is distributed. The MXtreme Intercept Engine takes virus protection beyond signatures and simple attachment filtering with its advanced virus protection. It closes the window of vulnerability that occurs when an attack first occurs and when a signature is available by protecting networks immediately.

Proactive Threat Prevention Beyond Reputation Services with BorderWare Security Network (BSN)

The BorderWare Security Network (BSN) works in tandem with the MXtreme Intercept Engine to take threat prevention to the next level with a highly accurate way to protect against more than just spam. The BSN proactively gathers data globally from more than 8,000 BorderWare products deployed world-wide to identify malicious senders and block threats across multiple attack vectors. The BSN uses real-time and historical data collected from the widest number and range of participating email and perimeter firewalls, plus traditional reputation-based services to react quickly to new outbreaks. By combining local and global threat data, customers benefit from dynamic real-time threat prevention, increased performance, improved QoS and lower operational costs.

Innovative, Multi-Layered Perimeter Integration with F5 & Cisco Connectors

MXtreme blocks attacks and unwanted email at the network edge through policy integration with F5 BIG-IP® and Cisco IOS® devices located at the perimeter of the network instead of requiring a separate “edge” device. This new integration further reduces inbound email, increases network bandwidth, reduces risk and enhances service levels without requiring additional hardware.



Block unwanted email at the network edge via policy integration which reduces inbound email without requiring additional hardware.

“The number of Directory Harvest and Denial of Service Attacks has increased 28% in 2005 and will increase, on average 30% per year until 2009.”

Radicati Group, 2005

F5 awarded BorderWare the First Prize in its iRules partner and customer award contest.



Control...

“Content filtering is quickly becoming a key complement to core anti-virus and anti-spam features. This functionality aids the enforcement of corporate policy, and is essential for many businesses in the regulatory compliance process.”

Radicati Group, 2005

“Organizations are finding that it is not enough to just scan inbound messages; they must now also scan outbound messages for things like content and confidentiality breaches... For instance an organization with a corporate compliance officer may want certain email to be routed to this person for approval, such as email that clearly violates the policy against disclosure of confidential information.”

Osterman Research, 2005

MXtreme Privacy and Compliance Solution

Unprecedented Granular Content Management with the MXtreme Privacy and Compliance Engine

The MXtreme Privacy and Compliance Solution provides unprecedented granular content management that is integrated with secure content delivery to ensure information is secure and regulatory requirements are met.

Deep Content Inspection with Email Filtering for Organization-Wide Protection

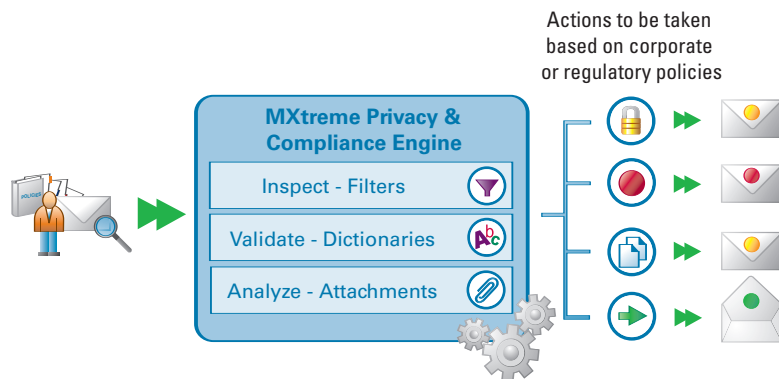
The deep content inspection email filtering within the MXtreme Privacy and Compliance Engine allows organizations to manage content entering and leaving a network for greater control and flexibility over email policy decisions. Scanning an entire email message allows organizations to enforce effective attachment policies, filter rules and encryption policies for users. This allows organizations to ensure that confidential information remains confidential and that inappropriate information does not enter or leave a network.

Detection of Regulated Content

The MXtreme Privacy and Compliance Engine controls and monitors all outgoing email and scrutinizes the text contained within an email message to ensure that no private information is present. In addition to email body text, attached files are also inspected. MXtreme attachment scanning is fully configurable offering flexible disposition actions based on the type of content found. This allows organizations to control the flow of both inbound and outbound information to detect unwanted, private, confidential or regulated content.

Pre-Defined Regulation-Specific and Customizable Dictionaries

A variety of regulatory-specific dictionaries for the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach Bliley Act (GLB) and other regulations are pre-defined within the MXtreme Privacy and Compliance Solution. The dictionaries are easily customizable and also include common terms and codes such as standard disease, drug, treatment, diagnosis codes, social security numbers, credit card numbers and phone numbers. Common expressions can be automatically flagged and quarantined by an organization’s IT department or compliance officer. In addition, custom scanning rules can be set to detect information in organization-specific formats, such as patient identification data and account numbers. The standard regulatory dictionaries can be expanded to include terms and codes specific to any organization.

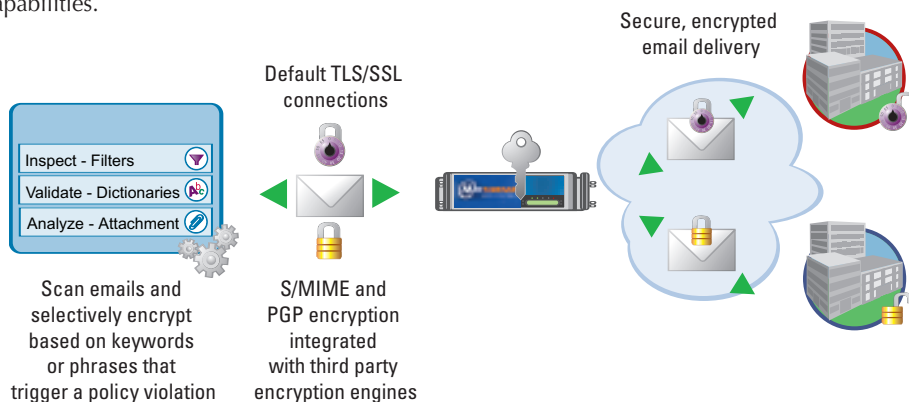


Automated enforcement of corporate or regulatory policies with regards to what messages need to be encrypted, stopped or quarantined before they leave an organization, ensuring policies are enforced and vital corporate data is protected.

Integrated Encryption for Emailing Confidential and Sensitive Information

Given regulatory oversight and privacy concerns, organizations need to become more diligent about safely sending confidential and sensitive information across the Internet. With messages being sent in clear text, organizations have no assurance that messages are not being intercepted and read, compromising private information. Encryption ensures that sensitive information remains confidential. To be truly effective, encryption must be managed by granular policies enforced on a messaging system. This allows automated enforcement of corporate or regulatory policies with regards to what messages need to be encrypted, stopped or quarantined before they leave an organization, ensuring policies are being enforced and vital corporate data is being protected.

The MXtreme Privacy and Compliance Solution controls outbound messages ensuring it is easy to comply with the many different types of email related regulations with no end-user intervention. By removing end-users from the decision making process, MXtreme ensures that the messages that require encryption are encrypted when transmitted and that user error or oversight does not put an organization in a liable situation. MXtreme provides the ability to scan emails and selectively encrypt email messages based on whether keywords or phrases found within a mail message trigger a policy violation. In addition to default TLS/SSL connections, the MXtreme Privacy and Compliance Solution uses industry standard S/MIME and PGP encryption integrated with third party encryption engines. MXtreme integrates powerful email policy compliance and encryption capabilities into an easy-to-deploy and manage solution that combines message scanning and policy enforcement with centrally managed encryption capabilities.



MXtreme integrates powerful email policy compliance and encryption capabilities ensuring that sensitive information remains confidential and policies are enforced so that vital corporate data is protected.

Centralized Audit and Regulatory-Specific Reporting

The MXtreme Privacy and Compliance Solution provides accurate and timely auditing and reporting of outbound information including the ability to create regulatory-specific reports to ease the burden of demonstrating compliance. The MXtreme Privacy and Compliance Solution reports are designed to consolidate information for compliance officers, senior executives and administrators in real-time with customized point-and-click reports generated at specified intervals or on-demand. MXtreme comes bundled with an extensive number of fully customizable reports that provide visibility into any individual system or group of systems to help manage an organization's entire email infrastructure. All messages are tracked eliminating the need for parsing logs and using third-party reporting tools. MXtreme also eliminates the need to invest in additional hardware and software by integrating with leading SNMP management tools. By combining this management with detailed audit and reporting capabilities organizations can monitor email activity, proactively pinpointing policy violations quickly and making it easy to find email messages when required.

"Secure messaging/encryption [will grow in the area of] policy-based systems that remove the decision from the end user. These systems will review outbound content and automatically encrypt those emails... that contain content deemed to be sensitive, such as social security numbers, corporate intellectual property and the like."

Osterman Research, 2005

Manage...

“Organizations are looking to decrease the amount of processing by blocking the traffic at the connection level or by reducing the amount of traffic hitting their email security device.”

Gartner, 2005

“Estimate[s] that email traffic volumes have increased 300% over the last year.”

Gartner, 2005

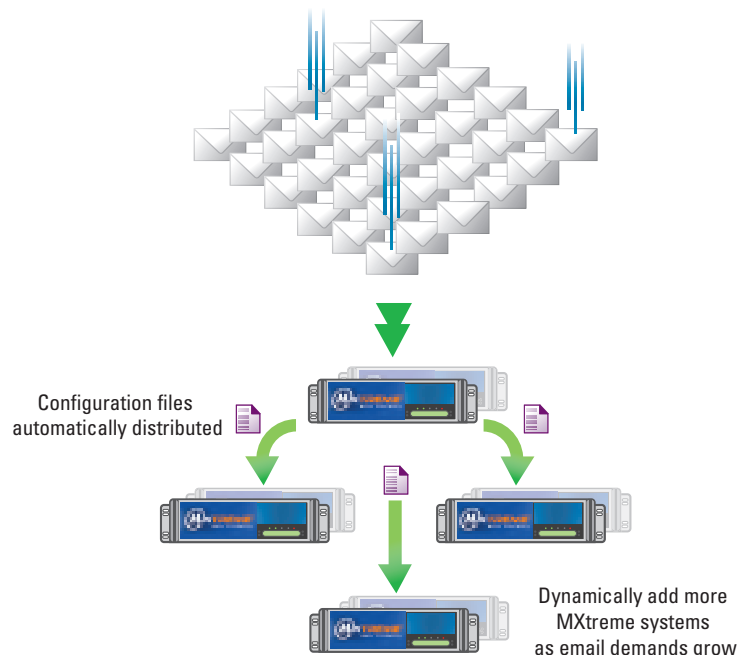
MXtreme Email Security & Privacy and Compliance Solution

Advanced Content Management with Sophisticated, Granular Policy Enforcement

Organizations have complete control over their email infrastructure including both inbound and outbound email message with the advanced content management and sophisticated policy enforcement in MXtreme. Complete granularity and flexibility on any aspect of an email message allows organizations to define policies, such as monitoring offensive language or limiting attachment types with an intuitive interface that simplifies the process of defining complex logical rules. Based on defined policies and classifications, MXtreme flags emails allowing an organization to take action including blocking, quarantining, encrypting, deleting, or any combination of these actions prior to exposing the company to any liability. MXtreme includes common filters and standard dictionaries to quickly establish policies and support existing corporate email policies, giving organizations an immediate benefit to control the most common email abuse issues. MXtreme seamlessly integrates into an organization by automatically uploading groups from existing LDAP directory services. This allows organizations to easily implement complex content and attachment policies.

On-Demand Scalability and Resiliency for Email Growth with Dynamic Clustering

Enterprises and service providers must be able to respond immediately with additional processing power to increase throughput, maintain superior service levels and ensure resiliency. MXtreme is the only email security solution providing on-demand clustering technology that can scale to support upwards of 10 million messages per hour allowing organizations to quickly add systems in minutes. Clustering multiple units together removes a single point of failure and ensures that a network infrastructure is always up and running. This dynamic clustering technology dramatically reduces the time and effort administrators must spend configuring and maintaining systems. The infinite scalability of MXtreme allows organizations to address both current and future demand.



Quickly add systems with dynamic, on-demand clustering - removing a single point of failure, reducing administration and providing infinite scalability.

Message-Level Redundancy and High-Availability with Failover and Queue Replication

Email is used for business-critical transactions and communications that require message-level redundancy for queue replication to ensure that no message is ever lost – because simple load balancing is just not enough. For example, losing an important time sensitive email such as a sales order or contract negotiation can cause an organization both lost productivity and lost revenue. By replicating email queues, MXtreme ensures that a copy of all undelivered mail messages are kept on another system and all outgoing messages can be easily retrieved and delivered when a system goes down mitigating message loss or delivery interruption. When MXtreme is configured in a cluster, all configuration settings and message queues are replicated across the entire cluster. MXtreme delivers an unbeatable return-on-investment by reducing operational costs and guaranteeing the delivery of business-critical email.



MXtreme message-level redundancy with queue replication and failover ensures no message is ever lost. Copies of all undelivered email messages are replicated in the cluster and messages are easily retrieved when a system goes down.

End User Anti-Spam Control with Seamless Integration for Microsoft® Exchange

The MXtreme Intercept Plug-in for Microsoft® Exchange seamlessly integrates with an organization's existing Exchange environment to provide effective quarantining and end user functionality without any administrative involvement and effort. This removes the need to manage user accounts, logins and storage for third party quarantine servers by taking advantage of existing Microsoft services.

Secure Remote Access to Microsoft OWA & Lotus iNotes with Secure WebMail

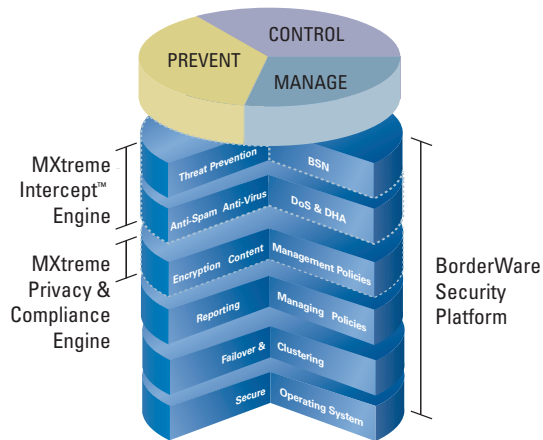
An increasingly large number of organizations provide remote access to email using WebMail servers such as Microsoft Outlook Web Access and Lotus iNotes. Due to the nature of WebMail being accessed externally, security is imperative. Integrating a high-performance proxy with secure access technology, intelligent analysis tools and an array of attack detection and blocking capabilities, MXtreme Secure WebMail functionality provides protected access to external users at any time, from anywhere in the world.

MXtreme™ Overview

Integrated, Underlying Architectural Foundation with the BorderWare Security Platform

Hackers no longer restrict attacks to specific IP traffic types and are launching blended attacks targeting email, Web, VoIP and other SIP-based applications. Organizations can no longer afford to purchase point solutions – they need a comprehensive solution that leverages an integrated security platform to prevent attacks, control content, and manage the network infrastructure. BorderWare is the only company that is able to address these threats with perimeter, email and SIP-based firewalls, which are all powered by the BorderWare Security Platform.

MXtreme is based on the BorderWare Security Platform which includes S-Core, a UNIX-based hardened and optimized operating system. The patent-pending Stateful Failover and advanced Queue Replication capabilities included in the BorderWare Security Platform ensure message-level redundancy and high availability. The dynamic clustering in the BorderWare Security Platform rounds out the unique combination of market leading technologies. The BorderWare Security Platform delivers an unbeatable return-on-investment by reducing operational costs and guaranteeing the delivery of business-critical email.



MXtreme is built on the BorderWare Security Platform, a sound technological foundation to prevent, control and manage email.



About BorderWare Technologies Inc.

BorderWare Technologies makes Internet communications safe. The company's perimeter and “application-specific” firewalls for email and SIP enable customers to prevent IP-based threats, control content and centrally manage the network infrastructure. Founded in 1994, BorderWare has more than 8000 customers in 65 countries that have selected BorderWare's solutions for their superior security, scalability, business continuity and lower total cost of ownership.

Headquarters: +1.905.804.1855 | Toll Free: +1.877.814.7900 | Europe: +44.20.8538.1750

Affiliations and Partnerships

