



MXtreme™ prevents email threats and controls outbound information to protect against malicious attacks and enforce compliance regulations. MXtreme takes a multi-layered approach to threat prevention with advanced anti-spam, anti-virus, image spam protection and a threat prevention engine. MXtreme controls outbound information and protects against regulatory compliance and corporate violations; theft and leakage of confidential information or intellectual property.

Product Features

- **Intercept Engine** – prevents incoming threats by combining the industry’s most effective anti-spam, anti-virus, image spam and threat prevention technologies
- **BorderWare Security Network (BSN)** – real-time proactive protection from next generation attacks through behavior-based reputation services
- **Privacy & Compliance Engine** – secures email communications with an end-to-end, single server, email encryption solution that ensures protection from data leakage
- **Clustering** – process millions of email messages to handle the most demanding networks
- **Message Redundancy** – never lose a message with the industry’s only email firewall to provide message-level redundancy and queue replication



Product Benefits

- Lowest false positive rate
- Zero day protection
- Proactive threat prevention with real-time defenses
- Meet compliance regulations by controlling outbound content with integrated encryption
- Mitigate risk by eliminating a single point of failure
- Ensure that no email message is ever lost
- Increase email throughput, maintain service levels and ensure resiliency

Business Challenge

Today, organizations face a set of challenges no one ever imagined when email was first introduced. Now that email is a business-critical application, challenges have expanded from spam, viruses, and other threats, to include compliance and regulatory requirements. While organizations struggle with new breeds of threats and blended attacks, the impact of security breaches, regulatory compliance violations, theft and leakage of confidential information or intellectual property are increasing in severity and continue to grow. In an effort to address the rising number of security issues, many organizations have built up cumbersome networks using a patchwork of point solutions that require constant maintenance and upkeep. Organizations need to look at email solutions that reduce costs and easily scale to meet growing company needs – across hundreds or thousands of users. Losing an important, time sensitive email such as a sales order or contract negotiation can impact business productivity and revenue, reinforcing the importance that no message is ever lost.

Solution

MXtreme is BorderWare’s market-leading appliance for email security, privacy and compliance. MXtreme delivers next generation email security using a multi-layered approach to preventing threats with an advanced anti-spam, anti-virus and threat prevention engine. MXtreme has granular policies, attachment scanning, encryption capabilities and industry compliance toolkits enabling customers to comply with corporate and industry regulations. MXtreme is the only email security solution available with message-level redundancy, on-demand clustering and F5 and Cisco device integration. MXtreme’s integrated approach provides a complete solution for email, consolidating disparate point solutions to prevent all email-based threats in one system and controls both inbound and outbound messages while addressing the key issues: security, privacy and usability.

Proactive, Real-Time Threat Protection - Intercept™ Engine & BorderWare Security Network (BSN)

MXtreme uses the Intercept™ Engine to protect against all email threats, including spam, image spam, virus, spyware, phishing, Denial of Service (DoS), Directory Harvest Attacks (DHA), and a variety of blended threats. The Intercept Engine incorporates a sophisticated analysis engine that blocks upwards of 98% of unwanted inbound email at the perimeter, allowing organizations to only receive legitimate email. The Intercept Engine, works together with the BorderWare Security Network (BSN) to take threat prevention to the next level providing zero-day protection against all email threats. The BSN proactively gathers and collates threat data in real-time from more than 8,000 BorderWare customer systems deployed worldwide. MXtreme uses the reputation and behavior information provided by BSN to identify malicious senders and prevent 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.

Meet Regulatory Compliance, Control Confidential Information & Prevent Intellectual Property Leakage

The MXtreme Privacy and Compliance Engine controls outbound content and ensures compliance requirements are always met therefore eliminating user error or oversight that could have put an organization in a liable situation. With messages being sent in clear text, organizations have no assurance that messages are not being intercepted and read, compromising private information. MXtreme provides complete granularity and the flexibility to scan any aspect of an email message allowing organizations to define policies to monitor sensitive information, private data or offensive language. MXtreme 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 this, MXtreme provides the ability to selectively encrypt email messages based on keywords or phrases found within an email message to trigger a policy violation prior to exposing a company to any liability. MXtreme

automates the enforcement of corporate or regulatory policies allowing messages to be encrypted, stopped or quarantined before they leave an organization, ensuring policies are being enforced and vital corporate data is being protected. MXtreme makes it easy to control outbound messages for compliance based on the many different types of email related regulations including SOX; Basel II; HIPAA; GLBA; PCI; PIPEDA; Freedom of Information Act; and Data Protection Act; and others.

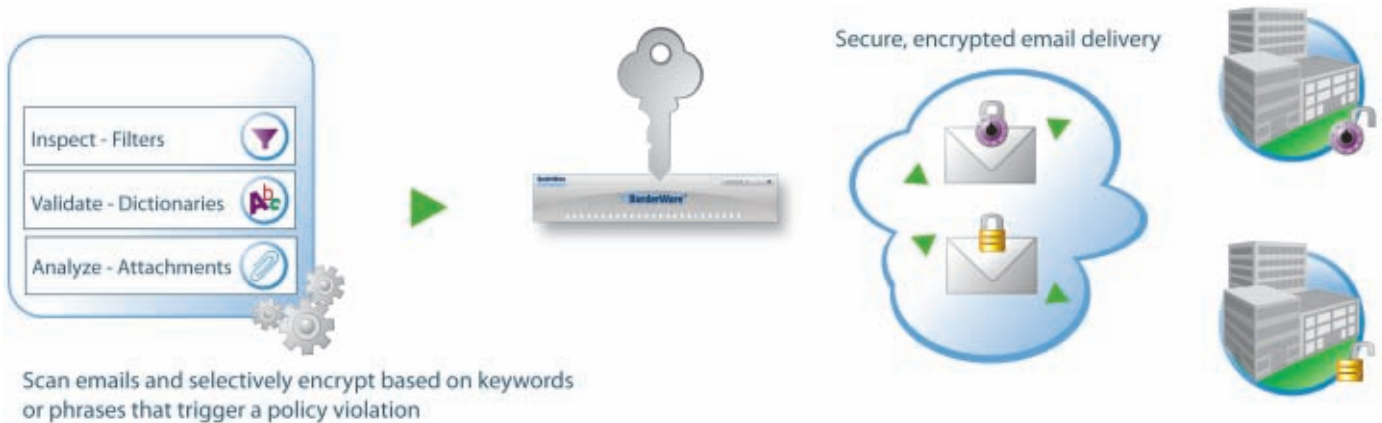
Easily Expand an Email Infrastructure as Organizations Grow & Ensure Email is Never Lost

As organizations grow and expand they must be able to respond with additional processing power to increase throughput, maintain superior service levels and ensure resiliency. MXtreme is the only email security solution that provides on-demand clustering technology that can scale to support millions of messages per hour. Clustering multiple email security appliances together removes a single point of failure and ensures that the network infrastructure is always up and running. This dynamic clustering technology dramatically reduces the time and effort administrators must spend configuring and maintaining systems. MXtreme provides further resiliency with message-level redundancy to ensure that no message is ever lost. By replicating email queues, MXtreme ensures that a copy of all undelivered email messages is kept on another system in the cluster. Should a system become unavailable, messages from that system can easily be retrieved and delivered, mitigating message loss or delivery interruption.

Block Attacks at the Network Edge - F5 & Cisco Integration

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. By leveraging existing network devices, organizations can reduce inbound email, increase network bandwidth, reduce risk and enhance service levels without the expense of purchasing additional hardware.

Integrated Encryption for Emailing Confidential and Sensitive Information



Headquarters. +1.905.804.1855 | Toll Free. +1.877.814.7900 | US Federal Office. +1.866.211.6789 | Europe. +44.20.8759.1999

www.borderware.com