VIPRE EMAIL SECURITY
Server

SECURE YOUR #1 THREAT VECTOR

The biggest security vulnerability within any organization is its employees, and they are more often targeted through email than any other threat vector. Deploy the protection you need with enterprise-class email security that doesn't slow you down.

VIPRE Email Security Server is an advanced, powerful, policy-based email security solution that defends networks against spam, phishing, viruses and other security threats transmitted via email.

VIPRE Email Security provides:

- Anti-spam, antivirus, anti-phishing, anti-spyware and malicious attachment protection
- Powerful policy-based SMART attachment filtering
- Dedicated PDF and image-spam engine
- Message disclaimers
- Reporting and message tracking

Robust and Efficient Email Defense

VIPRE Email Security provides a single solution for anti-spam, anti-phishing, antivirus, attachment filtering, malware protection and disclaimers, so you can:

- Stop malware targeting your users via email
- Improve the performance and reliability of your Exchange servers by eliminating spam
- Cut expenses by reducing the time and complexity of managing your email security
- Enforce stronger security with policy-based email security framework

VIPRE Email Security provides a layered approach for secure email inspection, cleansing and management. By using multiple scanning engines for anti-spam and antivirus, while integrating other email security rules, all treatment of messages occurs at the server, not at the endpoint – no client software needed.

EMAIL SECURITY GIVES CONTROL AND FLEXIBILITY

Prevent Ransomware

VIPRE bolsters your defense against phishing attacks, the #1 attack vector for ransomware.

Crush Email Threats

Powered by multiple spam and virus-scanning engines with settings displayed in a single tab.

Supports Microsoft Active Directory and Granular Based Policies

Provides a full set of administrative quarantine controls, leveraging powerful filtering and reporting.

The Report Viewer enables insight to quarantined elements with easy configuration. User and group based policies allow Active Directory integrations to enable VIPRE to support various security measures such as Data Loss Prevention, and continuous monitoring addressing the risk feature-by-feature.

End-User Managed Spam Quarantine

Gives users the ability to review spam and create their own Allowed and Blocked Senders list right from the inbox. This allows users to review and determine what is spam without the learning curve associated with other, more complex spam filters.

Take Charge of Your Email Security

Better defend your network from data-breaching malware and sophisticated phishing scams targeting your users with VIPRE Email Security Server powerful array of security features.

- **Improve Exchange Performance** – Stopping spam before it hits your Exchange server saves processing resources and improve performance.
- **Comprehensive Email Defense** – Multiple spam and virus scanning engines efficiently and accurately detect spam, phishing attacks and malicious attachments.
- **Optimized for Microsoft Exchange** – Seamless integration ensures minimal resource impact, securing inbound and outbound email without slowing delivery.
- **Easy Management** – Easy to install, configure and manage from a single console, robust default email security settings can be customized for your unique requirements such as internal policies or regulatory compliance.
- **Greylisting** – Identifying legitimate mail servers to prevent the download of email from non-legitimate sources decreases spam volume to improve system performance.
- **Auto-Whitelisting** – Adding outgoing mail recipients to a user-specific or network-wide whitelist reduces false positives and user complaints.
- **Robust Reporting** – At the system, group and/or user level, reports include number of inbound mail messages scanned, spam deleted, viruses intercepted, filters triggered, percentage of viruses by threat name and more.
- **Disclaimers** – Create global disclaimers for all outbound email, or configure policies to add disclaimers to emails from specific users, groups, domains or public folders.
- **Message Tracking** – Search for any message to identify blocked or allowed email, and adjust settings as needed.

SoftGen Australia Pty Ltd
828 Pacific Highway, Gordon, NSW 2072
E: sales@sgen.com.au | P: +61 2 9416 0416

SOFTGEN AUSTRALIA