GAJSHIELD EMAIL SECURITY

Email being the primary means of official communication, has become a gateway for threats for a lot of companies. Companies of all sizes face this daunting challenge. While email threats move fast, and malicious files look more like normal files that are often used for communication.

GajShield Email Security enables enterprise users to communicate securely and protects them for latest email borne threat vectors like ransomware, advance malware, spam, phishing and data leak using its unique Contextual Intelligence engine with multi layered approach to security.

Approach

Gajshield Threat Lab

Proactive virus detection, Robust and inherent immune system that integrates Zero-Hour (Zero-Day) Virus Outbreak Protection to shield enterprises in the earliest moments of malware outbreaks, and right through as new variants emerge. By proactively scanning the Internet and identifying massive virus outbreaks as soon as they emerge, proactive virus blocking is effective and signature-independent.

At the Threat Lab a database of real-time spam outbreaks is Collected, compiled and maintained, through consultation with global Internet Service Providers. Patterns are analyzed, categorized, and cross-matched using algorithms, run to optimize the detection of repeating patterns and their sources. This database, containing approximately over six million signatures, is continuously updated with more than 30,000 new unique signatures added hourly.

Contextual Intelligence Engine

All new contextual intelligence engine for ultimate visibility and better security. The Contextual Intelligence Engine helpsin creating context of the mail application beyond just the traditional context. It analyses the usage of the application and creates context by deep diving into granular details like:Address of Sender, Address of Recipient, Subject, Mail Content, Attachments, Signature, etc. for better and informed security with advanced visibility of mail services.

Highlights

- Global threat intelligence processing over 25 billion transactions daily.
- Block ransomware, spam, phishing and malware attacks before it reaches your infrastructure.
- Advance malware protection using machine learning techniques to model trusted email behavior.
- Advance threat protection using Contextual Intelligence, Recurring Pattern Detection, reputation scoring and file sandboxing.
- URL-related protection and control using scanning of URLs in emails based on their category and reputation.
- Combines rapid Domain Message Authentication Reporting and Conformance and forged email detection using DKIM and SPF to protect against BEC attacks.
- Protect sensitive data with integrated Data Leak Prevention solution.
- Seamless integration with GajShield Archiving solution.
- Simple to manage and configure using a Web based Administration.
- In depth reporting offers single view for comprehensive insight across your organization.

Recurrent pattern Detection

At the heart of the GajShield's Mail Security is its powerful, Recurrent Pattern Detection, spam engine that identifies spam patterns regardless of content, format, or language. By immediately detecting newattack patterns, and maintaining a database of spam outbreaks, the RPD engine identifies the quantityand the speed of the distribution of spam.

Network Sandbox

An Intelligent Network Sandbox solution that has anti-evasion capability for protection against malwarethat understands and detects a virtual environment. With the ability to sandbox various file types and embedded URLs, our intelligent sandbox inspects content that a traditional signature-based antivirus cannot identify as malicious and categorise accordingly.

Features

Advanced Threat Protection

- Scrutinises IP, domain of mails
- Reputations check and validation
- Bounce history, address authentication
- DMARC and DKIM checks
- Analyse message and content structure
- Analyse Image, Digital signature, keywords in context
- Scan embedded URIs
- Categorizing
- Advanced Intelligent Sandboxing.
- Complete Mail Analysis

Gateway Anti-Malware

- Powerful and Real-Time protection from Virus outbreaks
- Scans HTTP, HTTPS, FTP, POP3, SMTP & SMTPS traffic
- Detects and removes viruses, worms and all kinds of malware
- Instant identification of virus infected users
- ZERO Hour Virus protection
- Spyware, Malware, Phishing protection
- Automatic real-time Virus update
- Complete protection of traffic over all protocols
- Last virus update definition
- Complete report

Data Leak Prevention

- Deep packet analysis
- Restrict Content sharing
- Easy Policy implementation
- Unique group mailing policies
- Protect Critical Data
- Supports major mail services

Gateway Anti-Spam

- Scans SMTP, POP3 traffic for spam
- Detects, tags or quarantines spam mail
- Content-agnostic spam protection includingImage-spam
- Preemptively stops sophisticated threats likephishing, pharming & zombie attacks
- RBL lists
- Enforces black and white lists
- Real-Time protection from emerging threats
- Language, content, format & signature independent spam prevention
- Detects phishing URL in emails
- Quarantine Spam Mails
- Mail Archiving