GAJSHIELD
Data Security Firewall

ABOUT US

GajShield lnfotech (I) Pvt. Ltd. head-quartered in Mumbai, India. Since its inception in 2002, focuses on providing Security Solution to Corporates and Government agencies.

With our mission to deliver best of technology to deal with "Zero-Day" threat for a "carefree network and internet experience", We in our 19 years of our experience in the Firewall space, have deployed over 20,000+ firewalls spread across geographic regions in India, Europe, United States, Middle East, Africa, Australia, New Zealand and South East Asian countries. GajShield stands as one of the key players in leading the firewall space. GajShield is also the only Indian vendor amongst the highest rated vendors in multiple rating and experience sharing Portal in Firewall Category.

At GajShield, we understand data, its value as an asset to organizations and the important of protecting it without disrupting primary business activity. Our approach of looking beyond traditional security solutions and focusing on Data First security strategy is a leap forward in the security solution industry that is helping enterprises to secure cloud and Saas applications by implementing a Data Security Firewall solution.

We address major security challenges and deliver solutions for client's current and future needs that includes remote & roaming user's security, Data Leak Prevention, seamless branch connectivity and more has helped in constant product innovation, creating advanced real security solutions of today's and tomorrow's enterprise.

Team Gajshield

GajShield Infotech (India} Pvt. Ltd

Address: 4, Peninsula Center, Dr. S.S. Rao Road, Parel, Mumbai, India - 400012
Phone: +91 (22) 66607450 I Email: info@gajshield.com I www.gajshield.com

RECOGNITIONS AND CERTIFICATIONS

Recognized in Gartner's 2019 & 18 Asia/Pacific Context: 'Magic Quadrant for Enterprise Network Firewalls'.

GajShield is a leading Cyber Security Company with the distinction of being one of the few companies worldwide and the 1st Indian Firewall Product Company to have earned ICSA Labs Firewall Certification criteria 4.1. GajShield's Next Generation firewall products have now been certified by ICSA Labs for Corporate Firewall Certification for more than 14 years. We are also been honored with EIST Award by ICSA Labs.

GajShield has always believed in serving its customers with greatest of firewall security solutions, this reflects in our Gartner's Peer Insight Rating of 4.9* out of 5, being one of the highest rated vendors in the industry.

"GajShield clearly understands the importance of ICSA Labs testing and has demonstrated through their ongoing involvement with the Firewall Certification testing program that they are dedicated to maintaining the highest security standards" - Brian Monkman, Technology Programs Manager- lCSA Labs.

Other Certifications:
GajShield is also a global group ISO 9001 certified company (ISO 27001:2013 and ISO 9001:2015) to have met all the ISO standards required for the certification.

- Awards & Certificates -

GAJSHIELD
Data Security Firewall

KEY CAPABILITIES OF GAJSHIELD

Data Understanding Product & Solutions

GajShield Products and Solution understands contextual Data for better security. Looking at the current cyberattack trends towards data breaches, it addresses the major concern of data visibility and uses it as an aid for data security.

Preventing Data Leaks

GajShield uses a Context Based Network Data Leak Prevention to prevent business critical data from being leaked out through various gateways like Email, Saas application like Gmail, Google Drive, etc. and other popular social media platforms.

Protection against Email Borne Threats

Email being the go to means of business communication, attracts threats through it. GajShield uses Advanced Email Security Solution to protect from Email Borne malware, virus, business email compromise attacks and more.

Protection from Threat

At GajShield, we understand various threat vectors and help organizations to protect from the commonly ignored intentional and unintentional threats using intelligent security solutions.

Security for Roaming Users

Roaming users are the most accessible and easy targets for a lot of a hackers. GajShield enforces roaming users to route all network traffic through the firewall at HO, bringing them under a secured network.

Unified Platform for Security

GajShield's constant research and development has led to the creating of a uniformed platform for both network and data security.

Contextual Security

GajShield leverages its capability to provide visibility of data context, deeper than the traditional Layer 7 application visibility and performs proactive scanning to identify exactly which application, threat vector and user makes the network vulnerable and increases visibility, data security and performance.

GAJSHIELD
Data Security Firewall

DATA SECURITY FIREWALL

A Firewall That Understands Your Data

The increasingly relying of businesses on data and data-driven technologies, their business-critical data is being generated from a variety of different sources and being shared with a wide range of different enterprise stakeholders. Data being critical, experts agree that data security should be the top priority for enterprises. The traditional next-generation firewall solutions just aren't able to keep up with the task of monitoring and understanding each and every bit of data transactions.

The Data Security Firewall is a leap ahead of the traditional Next Generation firewall with Data First Approach for security. It understands organizations data and takes appropriate security measures to prevent data exploitation. The Data security firewall is self-learning, smart security solution that learns various data patterns and user behavior to identify anomalies and internal threats. It gives a better understanding of the data threat surface and allows enterpises to control them while improving overall data security health.

The Data Security Firewall is a powerful and robust platform that accommodates various security solutions to help secure data and organization's network. The Data Security Firewall is powered by GajOS Bulwark and backed by Contextual Intelligence Engine for a deeper data level visibility. Deployable On-premise and both public and private cloud infrastructure, Data Security Firewall caters to all sizes of companies across various business industries.

GAJSHIELD
Data Security Firewall

DSF ARCHITECTURE

Data Visibility

Data Control

Data Protection

Web

- Browsing
- Download
- Uploads

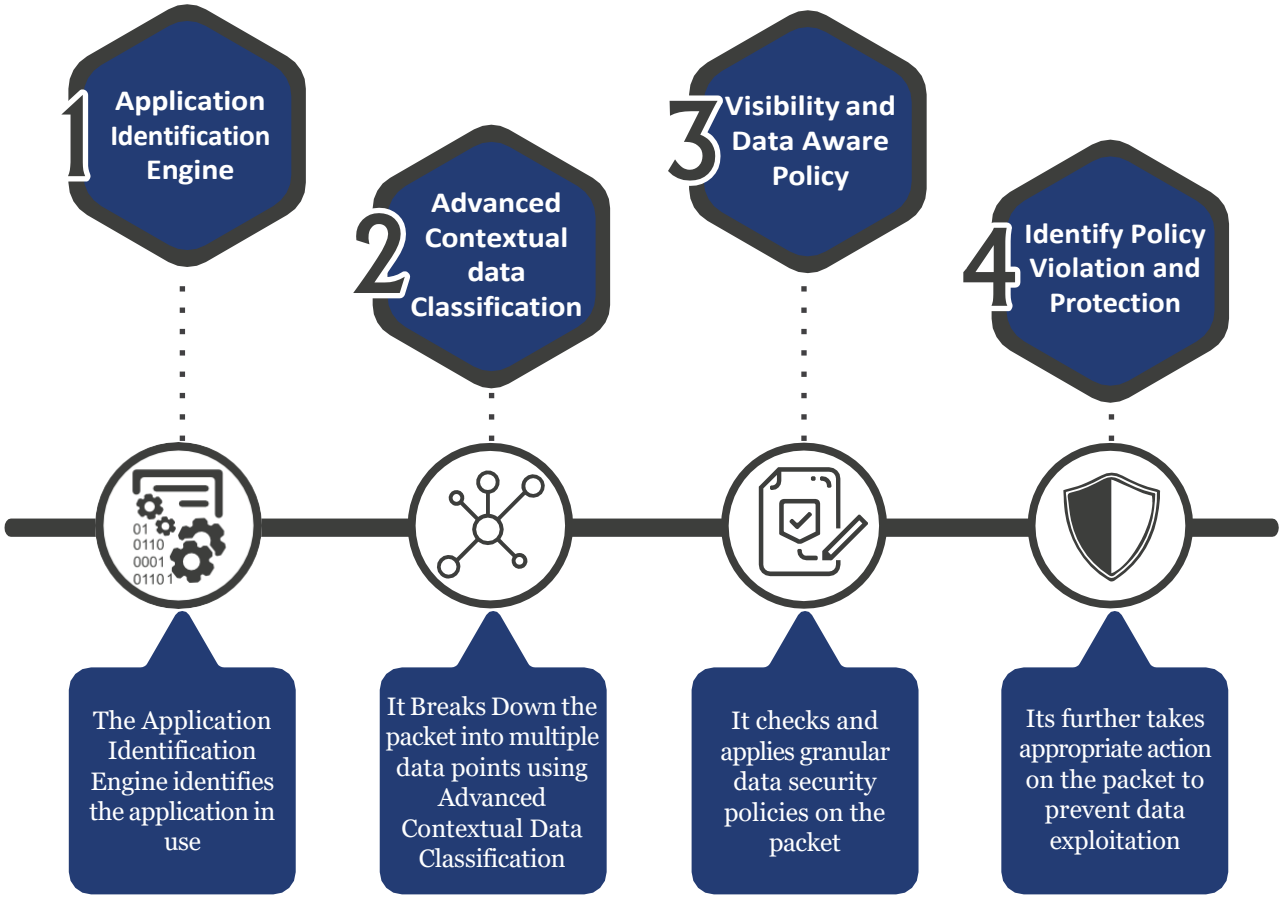
SaaS Application

- E-Mail
- Cloud Storage
- File Share
- Social Media

Network

- Vendor
- Branches
- Roaming User

APPROACH



GAJSHIELD
Data Security Firewall

BENEFITS

Advanced Contextual Data Classification

The Advanced Contextual Data Classification identifies the application and uses Deep Data Inspection to dive into the data context of the application. It identifies various data contexts within the application and breaks it into multiple data points for analysing them for possible data security policy violation and prevent data exploitation.

Cloud based data security model for roaming users

The Data Security Firewall with the help of an agent application Enterprise Cloud, routes all the traffic through the firewall at the HO and provides visibility on data transaction of the roaming user. e.g. in an instance where a roaming user with laptop connects to a public wifi, the Data Security Firewall Agent routes the traffic through the Head Office firewall and brings the roaming user under its protection.

Context sensitive data leak prevention

Using contextual intelligence, now you can define data leak prevention policies based on textual content inside the text-based file. The DLP can block data including files based on textual content it carries. For example, if in an organization, keywords like “tenders”, “Quotation” etc. are blocked, the users will be restricted to send mails or documents and attachments consisting of these keywords. The Deep Packet Inspection inspects the file content attached to a mail, being uploaded to a popular file sharing application, file sharing application, social media etc.

Threat Surface Management

Manage overall Data Threat surface with a 2 stage threat categorization for effective threat identification and management. The Data Security Firewall give deeper understaning of various sources of threats and their nature for organizations to understand them and take necessary action to gain control on these threat surface.

Limit Social Media/Collaborative Apps to Business Use only

The Data Security Firewall allows to set policies to restrict the use of popular personal email and social media ID and allow only corporate logins. E.g. one can allow only corporate logins for Social Media platform including LinkedIn, Facebook, Twitter, Instagram, etc. this allows marketing and the Human Resource team to access social media with restrictive/business usage.

Data Security Health

Monitor and Understand the overall Data Security Health of your organization based on various criticality parameters. Displayed in 3 stages of security, the health indicator is a real-time monitor that reacts based on various data security policy violations. it allows allocation of criticality to each policies e.g. High Medium and Low, helping organizations to take actions to improve data security health.

Data Visibility and control

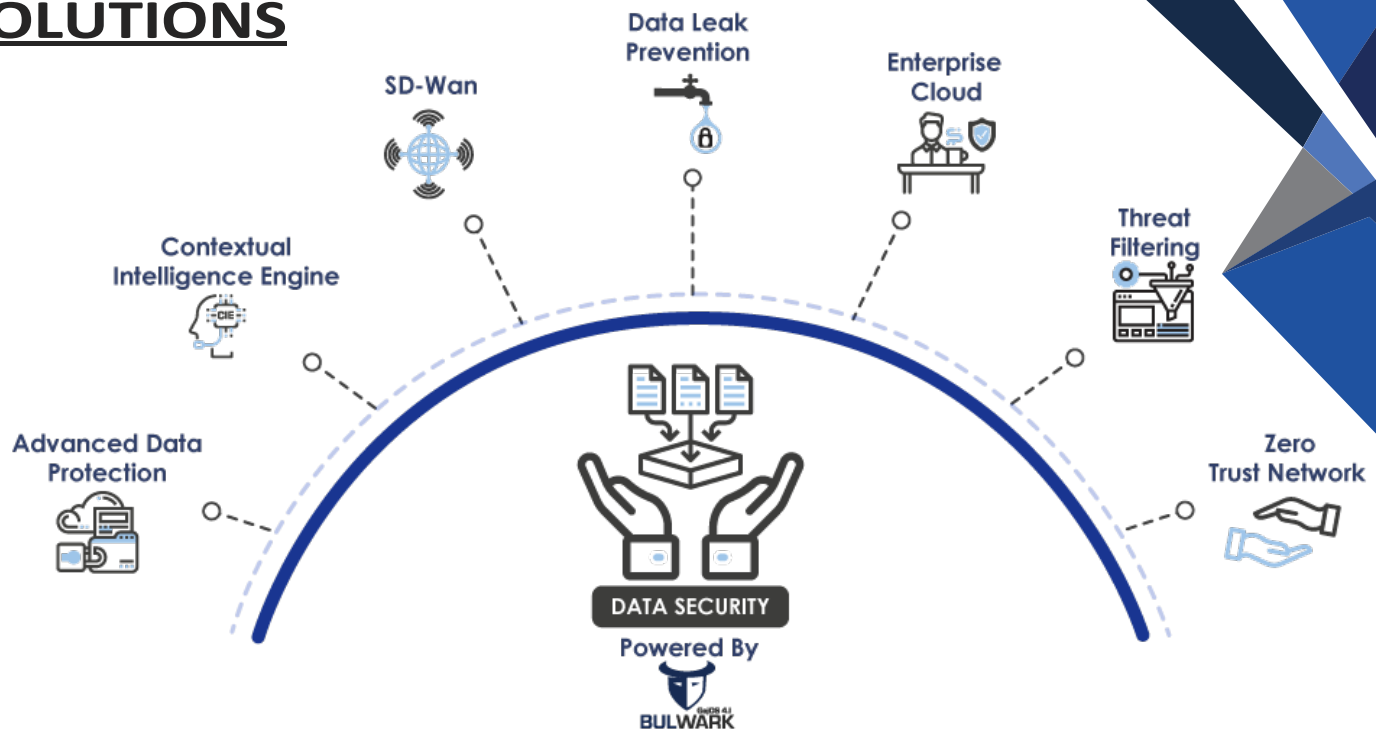
Backed by Contextual Intelligence Engine, the Data Security Firewall generates deeper data visibility by identfying the context of applications that helps in sending up policies to Control data transaction based on contextual parameter at both application and data level. E.g. restricting ‘From’, ‘To’, ‘Subject’, ‘Email body content, ‘Attachments’ etc. in an email applications and other parameters for various other popular platforms like Saas Applications, File Sharing Applications, Social Media, Cloud Storage, Network, web browsing and more.

SaaS data Control

GajShield’s CASB (Cloud Access Security Broker) works on a proactive detection model to ensures that all the communication between the on-premise device and cloud application provider complies with organization’s security policies. It uses information from the Contextual Intelligence Engine, check for compliance with Data Leak Prevention Policies to detect and take necessary action against an unsanctioned use.

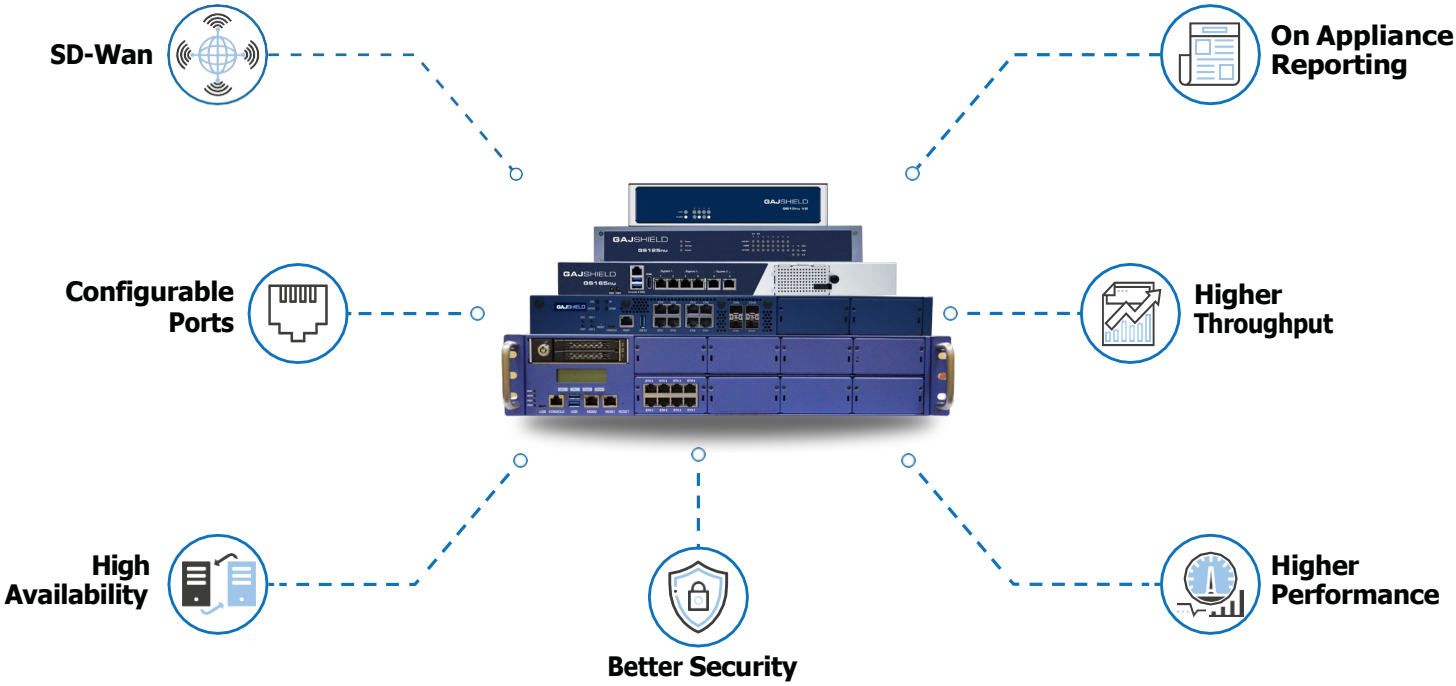
GAJSHIELD
Data Security Firewall

SOLUTIONS



APPLIANCE FEATURE

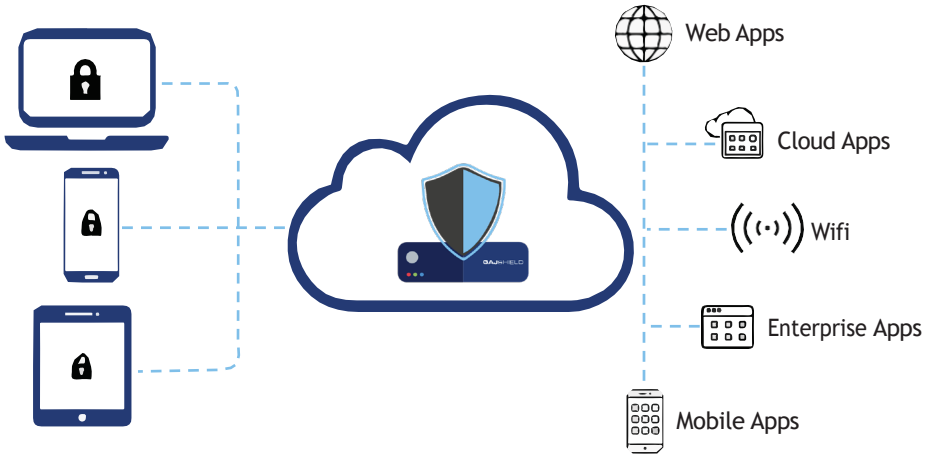
Brings Roaming users under your Firewall



GAJSHIELD
Data Security Firewall

ENTERPRISE CLOUD

An integrated, best-in-class and comprehensive cloud functionality by GajShield



Organizations these days have a number of different distributions which are stationary as well as mobile. These organizations need to cater to the security of both the types of users. Most organizations have multiple Internet gateways, and each gateway is a potential entry point for an attacker and thus, it is imperative that the security solution for an organization requires multiple point products to secure it. GajShield's integrated and comprehensive functionality provides security and control to any user, any device, at any location thus eliminating the need for multiple point products. As a result, the traffic from each firewall or device is simply redirected to the GajShield cloud.

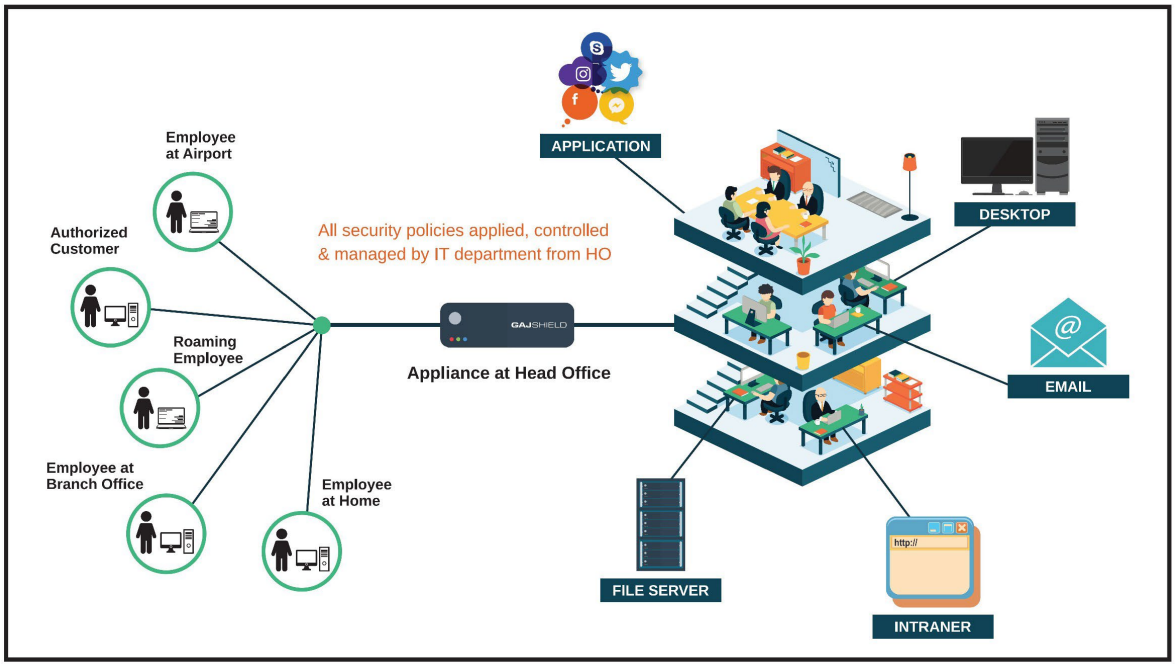
An organization may have roaming users with their own devices- mobile phones or laptops along with data cards provided to them for professional usage. It is important to keep a track on this usage, to monitor that the data card isn't utilized for personal purposes, to set policies pertaining to their use and more. In addition to this, antivirus to block malicious sites, malware, virus and more should also be incorporated to keep a track on the mobile users.

GajShield provides an integrated, best-of-breed, and comprehensive cloud functionality which allows the organizations to create common granular policies for various areas. It has an intuitive user interface so that use of the service literally requires no training. There are three key areas of functionality, namely- secure, manage, and comply. GajShield inspects all the inbound-outbound web traffic to protect enterprises from these threats. Various features have been incorporated like roaming users comply with company policies even when they are not in network which helps us keep track of them regardless of them being in the office or mobile.

Enterprise Cloud Key Features:

Roaming users comply to company policies even when they are not in the network

- Cloud Client enforces and routes all traffic securely through the Cloud Firewall (Public or Private).
- Secures roaming users even when they use insecure networks (public wifi etc).
- Central policies with ease of management for Roaming Users.
- No end point security product required, improves performance.
- Mobile users comply to company policies even when they are not in the network.
- All processing done in cloud & hence no performance impact on endpoint.
- Connect/disconnect status report.



GajShield Cloud Functionality:

- Viruses & Spyware: The Known Threats.
- GajShield inspects and protects against known viruses and worms using signature and heuristic technologies.
- GajShield's architecture provides inspection at many times the speed of most competitive products, ensuring full protection without introducing latency. In addition, spyware is a pervasive and significant security risk. GajShield antispyware detects and stops a range of spyware, including malicious Trojans, system monitors, keyloggers, and adware.
- Web traffic is increasingly being encrypted using the SSL protocol. If an organization selects SSL decryption policy, GajShield allows that organization to decrypt SSL traffic to detect and block hidden malicious content or outgoing sensitive information.
- As the traditional perimeter is vanishing, with enterprises connecting to their customers and partners, data leakage is becoming an expensive, burdensome problem. Employees, whether their intent is innocent or malicious, can easily send a Webmail or IM with confidential information. Information can be posted on social networks and biogs instantaneously. Private information, such as consumers' Social Security and credit card numbers, is protected by government regulations and leakage creates legal liabilities and harms brand reputation. Further, leaks of sensitive company information risk financial loss.
- Several companies have emerged to offer specialized solutions to prevent data leakage. These solutions often require extensive implementation and consulting services. They are also just another point solution to be added to an already-crowded perimeter gateway. Not surprisingly, less than 5% enterprises have deployed data loss prevention (DLP) solutions today.
- GajShield DLP solution provide in-depth visibility to the data which is sent out of your corporate asset.

GAJSHIELD
Data Security Firewall

DATA LEAK PREVENTION

Better visibility, control, and protection of your business

Security Challenges of Businesses - Data Leak a major concern

Hundreds of Web Applications traverse a network every day. Some of these applications, like social media provide a strong marketing tool but expose enterprise to risks. As perimeter of business boundaries is evaporating, it is leading to higher risk to business data and Intellectual Property. Intentional or unintentional data leak of information is a major concern for enterprises due to the exposure of users to increasing number of personal and business applications. The challenge that an enterprise face is that these applications use evasion techniques like dynamic or random port numbers or application emulation. Applications like Bit-torrent, Facebook, Gmail, Webchats, Skype, Instant Messaging which are popular with users constitute risk to enterprises as they are unable to affectively monitor and control these applications and content sent through these applications. This is because Firewalls don't understand content, don't understand applications, can't see inside SSL-encrypted traffic, and have no understanding of users. Enterprises are unable to match the Application risks and rewards, as Firewalls/UTM's are unable to provide visibility and control beyond, port and protocols.

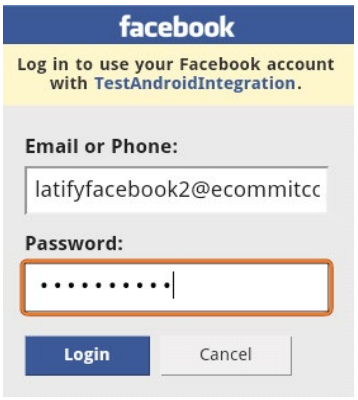
GajShield Firewall's Data Leak Prevention features

- Detection and Prevention of data leaks.
- Set policies to monitor/block data leaks via Email, File upload and Chats.
- Set policies to allow read only access to corporate email/social networking.
- In-depth reporting of data moving out of network.
- DLP & UTM on a single appliance, which makes it cost effective.
- Monitor IM & Web chats and block content, if data leak is suspected.
- Policies can be set based on users, groups. Also based on the application context.
- Easy to configure and integrated into single firewall policy window.
- Powerful DLP Engine sense data on filters set in DLP polices for a granular analysis.

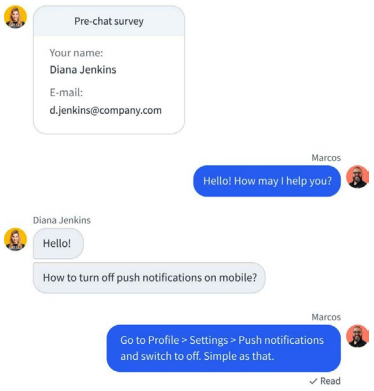
Web Leak Prevention

The most recent and profound development in cyberspace is the global migration of social media. Facebook have 2.89 billion monthly active users, in a single second of the day, 7,615 tweets are posted to Twitter and 1074 photos are posted on Instagram. Social media has become the new cyber battleground, presenting one of the largest, most dynamic risks to organizational data security in decades. With the help of GajShield Data Leak Prevention feature you can now setup policies to limit the access of these applications based on authorised users of these application who have been given access by your organization. With GajShield Data Leak Prevention you can also monitor and block files being uploaded on the internet with details of the application used and the user who used to upload this file. Even you can view the content of uploaded file. Many company allow employees to use instant message program to communicate, however, employees may send instant messages which are not related to their work, or even leak out a business secret, such communication can also be traced & blocked using GajShield **DLP.**

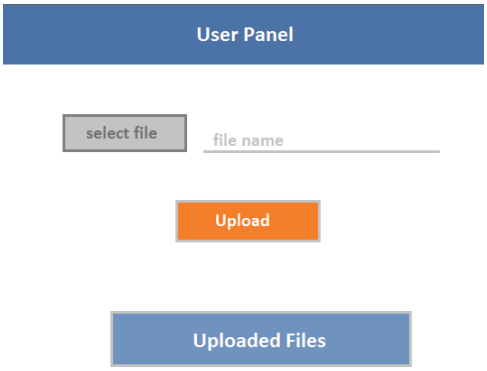
For example: You can allow your corporate Facebook id (abcd@company.com) to login to Facebook. All other login to Facebook using personal ids will be blocked. Even if the user is allowed to access Facebook then also he/she will be blocked, which means only corporate ids are allowed to login on Facebook. Similar policies can be setup even on Yahoo mail, Hotmail, Gmail & other social media can also be restricted.



Login only with you corporate email id



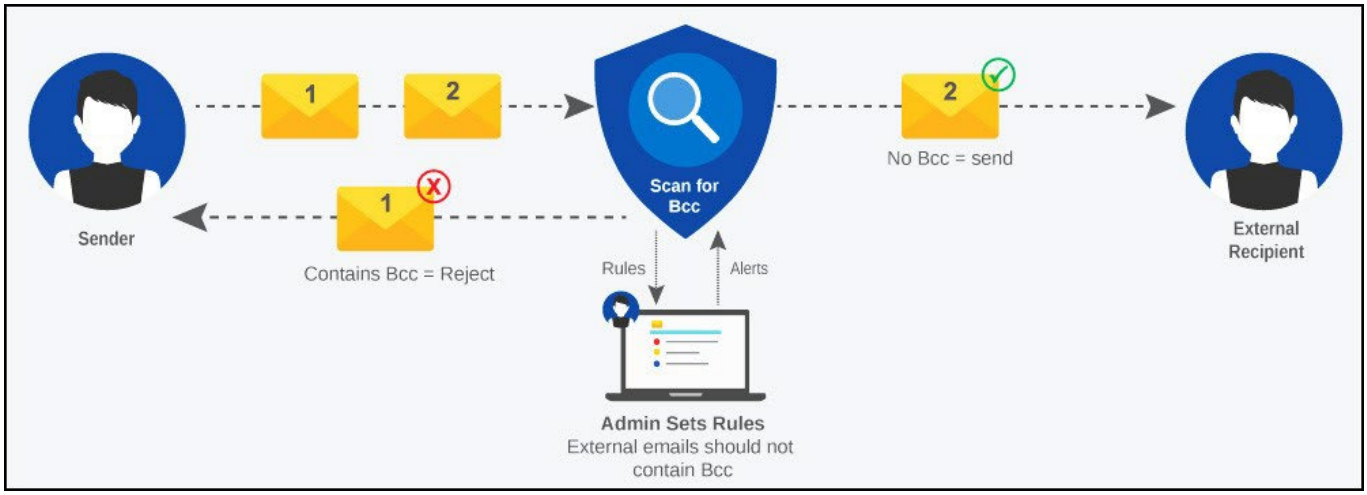
Trace live chat of disgruntled employee



Monitor & block files upload on the internet

SMTP Leak Prevention

Email continues to be dynamic to business communications and operations. An intrusion in which organization's disgruntled employee uses his/her own email to leak company's confidential data like clientele, pricing, financial data etc... this can cause financial losses to the company. With GajShield Data Leak Prevention System, policies can be configured at the organizational level, to block / trace email content and attachments sent by disgruntled employee and necessary action can be taken. Email can be tracked with entire email body content. You can create policies based on the 'From', To', 'Subject', 'Cc', 'Bcc', 'Email Body', 'Email size', 'Attachment name', 'Attachment size' of email applications.



GAJSHIELD
Data Security Firewall

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 helps in 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.

GAJSHIELD
Data Security Firewall

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 new attack patterns, and maintaining a database of spam outbreaks, the RPD engine identifies the quantity and the speed of the distribution of spam.

Network Sandbox

An Intelligent Network Sandbox solution that has anti-evasion capability for protection against malware that 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
- Deep Mail Inspection

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

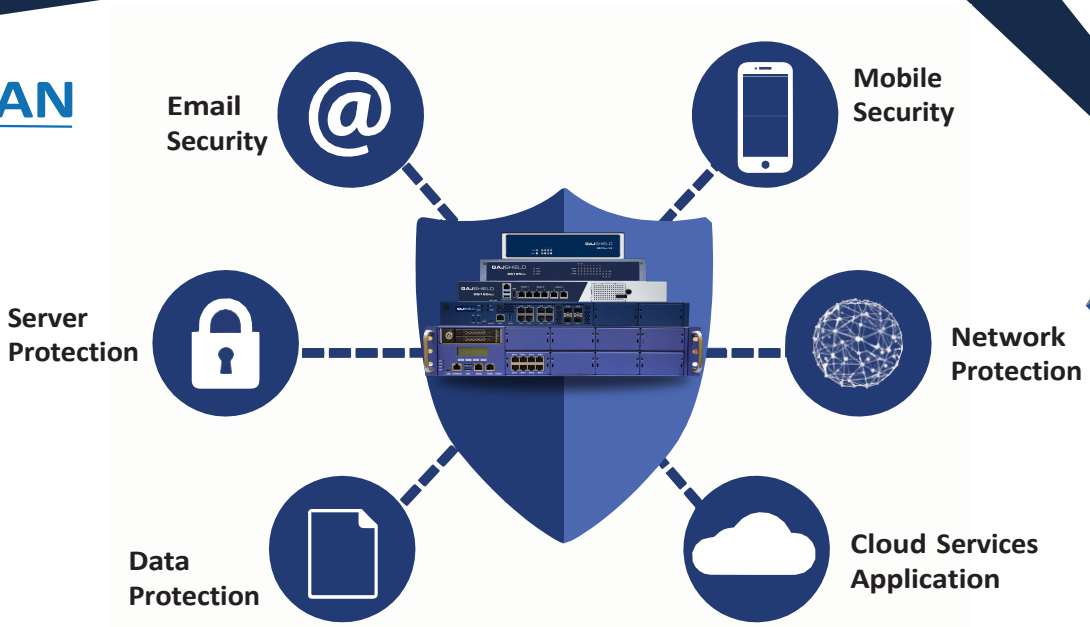
- Deep packet analysis
- Restrict Content sharing
- Easy Policy implementation
- Unique group mailing policies
- Protect Critical Data
- Supports major mail services

Gateway Anti-Spam

- Scans SMTP, POP3 traffic for spam
- Detects, tags or quarantines spam mail
- Content-agnostic spam protection including Image-spam
- Preemptively stops sophisticated threats like phishing, 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

GAJSHIELD
Data Security Firewall

SD-WAN



The speed of business continues to accelerate. Competition is fiercer than ever; customer expectations are higher than ever. Today's businesses run on applications and rely on connectivity, and when you're opening up new sites or branches, time is money.

Geographically distributed organizations often have hundreds or even thousands of branch offices connected to hub or headquarters' sites. For security reasons, cloud-based application traffic is often backhauled from the branch across expensive WAN/MPLS Links to a hub site before being handed off to the Internet. Not only is this expensive, but performance is often compromised due to WAN bandwidth constraints at the branch and added Latency from backhauling connections.

A solution is to use direct Internet connectivity that provides simpler and consistent performance to cloud-based applications. With GajShield Data Security Firewalls, Internet connections become secure and reliable, it helps in augmenting or even replacing the traditional MPLS connections and Lower WAN costs.

GajShield GS-Branch

Distributed enterprise branches transitioning to a digital business model have a significant impact on their network. With enterprise users both remote and Local directly accessing the internet for cloud and Security-as-a-Service (Saas) applications, the WAN and access edges are getting more complicated than ever and introduce new vulnerabilities for attackers to exploit.

GajShield Firewalls enables customers to converge their security and network access, extending the benefits their distributed branches. GajShield security device is comprised of GajShield Next-Generation Firewall. Secure Access using VPN, Anti Malware with Advance Threat Protection to deliver consolidation of branch services for network edge and device edge protection.

Benefits

- Centralised policy management
- Easy operations with minimum learning curve
- Flexible deployment
- Consolidated Network and threat visibility
- Allows grouping of security appliances
- Reduced operational cost
- Create policy templates, which can be re-used

GAJSHIELD
Data Security Firewall

Centralized Management System

Quick Deployment

GajShield's simplified and easy deployment Capabilities allow enterprises to ship unconfigured GajShield NGFW appliances to each remote site. When plugged in, the appliance automatically connects to the service in Centralized Management Service Server. Within seconds, the server authenticates the remote device and connects it to a Central Management System.

The GajShield Centralised Management System is a dedicated network security management appliance, that enables network admin to manage distributed network of GajShield Firewalls, Like managing all aspects of device configuration, push global policies, view all firewall traffic, and generate reports - all from one central Location using a single console.
Multi-path technology can automatically fail over to the best available Link when the primary WAN path degrades. This automation is built into the GajShield's Multi WAN management, which reduces complexity for end-users while improving their experience and productivity.

Benefits

Lower Cost or Setup and Operation

With the help of Centralised GajShield Security Management Architecture, enterprises can deploy and manage multiple Internet Links, you can now augment or even replace MPLS connections with broadband internet services to connect users to applications and Lower WAN costs by up to 90%.
The ROI is dramatic and immediate.

Better Performance

GajShield Security Architecture is powered by multi core architecture which provides faster application steering and unrivaled application identification performance. This includes deep secure sockets Layer (SSL) / Transport Layer Security (TLS) inspection with the Lowest possible performance degradation.

GajShield's MultiWAN management helps in routing applications and users over the most efficient WAN connection at any point of time. To ensure optimal application performance, it identifies a broad range of applications and applies routing policies at a very granular Level for better end-user productivity.
GajShield's application engine uses an application control database with the signatures of identify various applications (plus regular updates from GajShield threat Lab). GajShield identifies and classifies applications, even encrypted cloud application traffic, from the very first packet. This can be set to recognize applications by business criticality. Unique policies can be applied at a deeper Level for sub-applications. This deep and broad application-Level visibility into traffic patterns and utilization offers a better position to allocate WAN resources according to business needs.

High Availability

One of the goals of high availability is to eliminate single points of failure in your infrastructure. A single point of failure is a component of your technology stack that would cause a service interruption if it became unavailable. As such, any component that is a requisite for the proper functionality of your application that does not have redundancy is considered to be a single point of failure.

High availability is an important subset of reliability engineering, focused towards assuring that a system or component has a high Level of operational performance in a given period of time. At a first glance, its implementation might seem quite complex however, with GajShield it becomes much simpler and it can bring tremendous benefits for systems that require increased reliability.

Better Security

Contextual Intelligence Engine

Contextual Intelligence Engine is a technology that allows to gain advanced visibility of data transaction over applications that uses network. Context based security approach is a step ahead from traditional firewall capabilities. Using deep inspection at Different Levels for advanced security, Contextual Intelligence Engine understands the application and its data context. It allows to create context of Saas applications and understand its usage, much deeper than just the application. Combined with Machine Learning, contextual intelligent engine helps in finding anomalies.

Data Leak Prevention

DLP identifies, monitors and protects the data in motion on your network through deep content inspection and a contextual security analysis of transactions, DLP systems act as enforcers of data security policies. They provide a centralized management framework designed to detect and prevent the unauthorized use and transmission of your confidential information. DLP protects against mistakes that Lead to data Leaks and intentional misuse by insiders, as well as external attacks on your information infrastructure.

Intelligent Sandboxing

An Intelligent Network Sandbox solution that has anti-evasion capability for protection against malware that 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 categories accordingly.

GajShield Threat Lab

Proactive virus detection, Robust and inherent immune system that integrates Zero-Hour (Zero-Day) blocking is effective and signature independent.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, At the Threat Lab a database of real-time spam outbreaks is collected and 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.

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

Security-Driven Networking

GajShield enables best-of-breed software driven networking that is both high-performance and protected. GajShield NGFWs featuring multi core architecture to deliver a faster network management with extreme security performance. GajShield has robust threat protection, including Layer 3 through Layer 7 security controls. Featuring Complete threat protection, including firewall, antivirus, intrusion prevention system OPS), and application control High-throughput SSL inspection with minimal performance degradation, ensuring that organizations do not sacrifice throughput for complete threat protection against zero-day threat. Web filtering to enforce internet security and Highly scalable & throughput overlay VPN tunnels to ensure that confidential traffic is always encrypted.