GajShield Virtual Firewall GS nuv
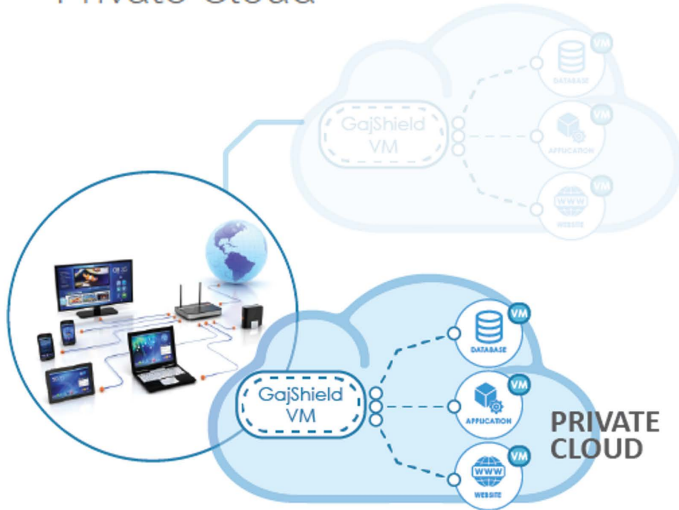

DATA SECURITY FIREWALL APPROACH

Application Identification Engine

The Application Identification Engine identifies the application in use
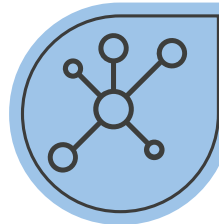
Advanced Contextual data Classification

It Breaks Down the packet into multiple data points using Advanced Contextual Data Classification Engine

Visibility and Data Aware Policy

It checks and applies granular data security policies on the packet

Identify Policy Violation and Protection

Its further takes appropriate action on the packet to prevent data exploitation

DATA SECURITY FIREWALL

The Data Security Firewall is a leap ahead of the Last Generation firewall with its Data First Approach for security. It understands data, provides deeper visibility on data transactions, and allows control over threat surface. It takes appropriate security measures to prevent data exploitation. The Data security firewall is selflearning, smart security solution that learns various data patterns and user behaviour to identify anomalies and threats, both intentional and unintentional.

The Data Security Firewall is a powerful and robust platform with various security solutions to help secure data and organization's network and is powered by GajOS Bulwark and backed by Contextual Intelligence Engine for a deeper data level visibility.

GajShield Virtual Firewall GS nuv

Organizations of all sizes are turning to virtualization to reduce costs and increase the efficiency, availability, and flexibility of their IT resources. At GajShield we continue to innovate and provide multi-dimensional security using our Data Security Firewall appliances, virtual firewall and cloud-based firewalls on platforms like. Azure, Amazon-AWS, VMWARE, Microsoft Hyper-V, Google cloud platform, etc.

Having virtual environment can lead to added complexity in managing them which could lead to additional security threats for whole of the organisation. Having a single, unified view and management system to manage physical and virtual firewalls can lead to improved security and visibility. GajShield brings its unique next generation data security platform with contextual intelligence engine to the world of virtualisation. Powered by GajOS: 4.0 Bulwark, GajShield firewall brings to you an advanced and granular reporting for deeper network visibility, adding to ease of management of your virtual environments to secure as your physical one.

GajShield's virtualized security appliances offers unmatched performance and deployment flexibility with no service degradation, bottlenecks or degrading of security. You can choose to deploy a mix of hardware and virtual appliances, operating together and managed from a common centralised management platform.

Multi-Tenant Management

GajShield's unique contextual security can be deployed easily to protect your customer data even in a cloud environment. It could be implemented for a per customer, region or department, managed through a single management portal. GajShield's multitenant management provides security services to multiple client organisation from a single shared deployment with user roles with distinct responsibility. You can deploy multiple instances of GajShield virtualised firewall on servers at the perimeter of their data centres isolating them from each other and yet managing them through an intuitive console which helps in guaranteeing service level agreements.

Increased visibility and security using 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, Contextual Intelligence Engine understands the application and its data context. It allows to create context of SaaS applications and understand its usage. Combined with Machine Learning, contextual intelligent engine helps in finding anomalies for and advanced network security.

	CPU CORES	RAM (GB)
MODEL		
GS 12VFnu	1	2
GS 24VFnu	2	4
GS 36VFnu	3	6
GS 48VFnu	4	8
GS 816VFnu	8	16
GS 1632VFnu	16	32

DATA SECURITY FIREWALL
- Application Identification Engine
- Advance Contextual Data Classification Engine
- Apply Visibility and Data Aware Policy
- Identify policy violation and protect against data exploitation

DATA LEAK PREVENTION
- Network based data leak prevention
- Prevent data leak on G Suit, Office 365, Popular Social Media, Web etc.
- Protect business critical data
- Scan for Data Leak on all outbound communication
- Alert on Data Security Policy violation
- Block Password Protected zip and PDF file uploads
- Block file uploads based on File Content, file type and size
- Time scheduling for DLP policies
- Visibility on Information sent as attachments on popular Webmail, Blogs, web uploads, SaaS, etc.

CONTEXTUAL VISIBILITY
- View Content of mail for Gmail, Outlook, Office 365, Rediff, Yahoo etc.
- Visibility of data transaction over HTTP, HTTPS, SMTP, SMTPS-SSL & Web Chats
- Data Transaction on SMTP mail, popular Web Mail and browser-based SaaS application
- View attachments attached with the mail
- View webmail draft attachments information
- visibility of evasive applications like P2P and Skype application accessed by users
- Identifies Who is accessing, which application,
- Visibility of application usage and data transaction on application
- Data transfer reporting (By Host, Group & IP Address)

DATA TRANSACTION LOG:
- Log of Data sent through
  - Web
  - Browser based SaaS
  - SMTP mails
  - Network
- Data Transaction logs from HTTP, HTTPS, SMTP, SMTPS-SSL & Web Chats
- Log Data context of the Popular webmail sites such as Gmail, Office 365, Yahoo and Rediff mail including To, CC, BCC, subject, body of the mail and attachment.
- Archive all types of file uploads on popular websites
- Mail archiving on SMTP & SMTP-SSL

REPORTING
- Identify the most bandwidth consuming users
- Identify application misuse and bandwidth abuse
- Identify work or non-work-related browsing
- Intrusion events reports
- Policy violations reports
- Virus reporting by User and IP Address
- Separate reporting for BYOD devices.
- Email alerts for Admin activity
- Application Traffic, Total Traffic, Application set and application detail

DATA CONTROL
- Control on Critical Data outflow
- Monitor/block & alert for data transactions on popular web-based emails like Gmail, Office 365, Yahoo, Rediff and Corporate web mails hosted on Gmail, Office 365, Yahoo, Rediff and social media platforms
- Accessing web mails in read only mode
- Entire internet in read only mode
- Block Context based application usage based on:
  - emails sender
  - recipient
  - subject & content
  - File attachments type
  - File attachment size
- User wise allow/block file transfer

POLICY CONTROL PLANE
- Firewall Policy License
- Quick action based on data security dashboard learnings
- Data Security Policies for user and user group
- Data Security Policies for IP address and IP group.
- Flexible Generic rules matching for Http header and Http Content
- Context based Data Security policy
- Content keyword-based data leak prevention policy
- user wise policies for accessing web mails like Gmail, Office 365, Yahoo and Rediff, web chats for Gmail hangout chat and Facebook webchat, social networking site Facebook & SMTP mail
- user wise policies to block content in body, subject of the popular web-based emails like Gmail, Office 365, Yahoo and Rediff
- Mail rules for Popular webmail sites like Gmail, Office 365, Yahoo and Rediff to match mails on Subject, From, To, CC, BCC, Msg Body, Msg Body Size, Attachment Text, Attachment Name, Attachment Size, Total Attachment Size, Attachment Type with a wide range of matching option. (is, is not, contains, does not contain, begins with, ends with)

POPULAR WEB CHAT SECURITY
- User wise allow/block web chat
- Live Chat Monitoring
- User wise allow/block file transfer
- User based web chat Archiving

VPN CLIENT
- IPsec compliant
- Inter-operability with major IPsec VPN Gateways
- Supported platforms: Windows 98, Me, NT4, 2000, XP, Vista, windows 7 & 10

INTRUSION PREVENTION SYSTEM
- Signatures: Default (25000+), Custom signatures
- Policy Based IPS, Anomaly Detection
- Automatic real-time updates & e-mail notification
- P2P applications signatures

ENTERPRISE CLOUD
- Visibility & Control over internet as well as secure access to corporate network
- Enforcing of security policies on roaming users

GAJSHIELD

NETWORKING
- Transparent Mode, Route Mode, Layer3, Layer 4 Bridge mode
- Static IP Address, PPPoE, DHCP support
- DHCP server support on multiple interfaces
- Policy based Multiple Link Auto Failover
- Policy based Load balancing
- Policy based routing based on Application and User
- DDNS/PPPoE Client
- Policy based NAT, Port Address Translation
- NTP,SNMP,SNMP v2, SNMP v3
- HTTP Proxy Mode, Parent proxy support
- Traffic Handled - TCP, UDP, HTTP/TCP, TCP/UDP
- IPv6 Ready
- Packet Size (kb) 64, 128, 1024
- Dynamic Routing: RIP v1& v2, OSPF
- Multicast Forwarding

BANDWIDTH MANAGEMENT
- Application and User based Bandwidth allocation
- Prioritize, shape or Limit bandwidth
- Priority based bandwidth allocation
- Multi WAN bandwidth reporting

VIRTUAL PRIVATE NETWORK – VPN
- IPsec, SSL, L2TP, PPTP
- Encryption - 3DES, DES, AES
- Hash Algorithms - MD5, SHA-1, SHA-2
- Authentication – Pre-shared key, Digital certificates, Xauth
- IPsec NAT Traversal
- Site to Site VPN Supported
- Client to Site VPN Supported
- SSL VPN Peers Supported
- Dead peer detection and PFS support
- Diffie Hellman Groups - 1,2,5,14,15,16
- External Certificate Authority support
- Export Road Warrior connection configuration
- Domain name support for tunnel end points
- Hardware Token: RSA, Vasco
- VPN connection failover

GATEWAY ANTI-SPAM
- Multiple spam classification
- Image-based spam Filtering
- Recurrent Pattern Detection on POP3, SMTP & SMTPS-SSL
- Independent of Content, Format, Language
- Real-time Blacklist (RBL), MIME header check
- Filter based on message From, To, Subject
- Subject line tagging
- Zero-hour Virus Outbreak
- Quarantine folder for Spam

GATEWAY ANTI-VIRUS
- Zero-hour Virus protection
- Advanced Persistent Threat
- Inline HTTP, HTTPS, FTP, SMTPS-SSL, SMTP, POP3, IMAP scan
- Virus, Worm, Trojan Detection & Removal
- Spyware, Malware, Phishing protection
- Automatic Real Time virus signature database update
- Scan by file size

AUTHENTICATION
- Support for multiple authentication schemes simultaneously
- Local database, Windows Domain Control & Active Directory Integration
- External LDAP/RADIUS/TACAS+ database Integration
- RSA, VASCO secure tokens

ADMINISTRATION
- Two-factor Authentication support
- Web-based configuration wizard
- Role-based administration
- Upgrades & changes via Web UI
- On Appliance Analytics
- Graphical real- time and historical monitoring
- Email notification of reports, viruses and attacks
- Syslog support
- Web GUI (HTTPS)
- Command Line Interface (Console, SSH)

HIGH AVAILABILITY
- Active/Active & Active/Passive with state synchronization
- Stateful Failover
- E-mail Alert on Appliance Status change

STATEFUL INSPECTION FIREWALL – ICSA CERTIFIED
- UserSense UTM - Policy combination of User, Source,
- IP, URL, Domain and Service
- Policy based single window control for Firewall, DLP, BYOD,
- URL Filtering& Application Control.
- Anti-virus, Anti-spam, DLP and Bandwidth Management
- Access Scheduling
- Policy based Source & Destination NAT(DNAT,SNAT & PNAT),loop-back NAT & Dynamic NAT.
- H.323 NAT Traversal, 802.1q VLAN Support
- DoS, DDoS, Syn Flood Attack prevention
- Policy creation based on BYOD

APPLICATION FILTERING
- Control and Visibility of Layer 7 Applications
- Protects your Corporate users as well as BYOD devices
- Inbuilt Application Categories
- 5000+ Applications Signatures
- Schedule-based access control
- QoS Control over Layer 7 Applications

URL FILTERING
- Inbuilt Web Category Database
- Millions of sites arranged in 85+ categories
- URL, Domain, Keyword, File type block
- Mime type blocking
- Protocols Supported – HTTP, HTTPS
- Block Malware, Phishing, Pharming URLs
- Block Java Applets, Cookies, Active X
- URL Exempt/White List
- Schedule-based access control

ADVANCED THREAT PROTECTION

- Ransomware Protection
- Malware Protection
- Multiple spam classification
- Image-based spam Filtering
- Recurrent Pattern Detection on POP3, SMTP & SMTPS-SSL
- Independent of Content, Format, Language
- Real-time Blacklist (RBL), MIME header check
- Filter based on message header, size, sender, recipient, subject line tagging etc.
- Zero-hour Virus Outbreak
- Anti-botnet security

24x7 Supports

GajShield is committed to delivering a high-quality customer experience. That means, you have a variety of award-winning support options to meet your needs, including.

- **Multi Language Support**
- **On Call Complete Assistance**
- **24*7 Availability**
- **Highly Trained Support Expert**
- **Turn Around Time - < 5mins**
- **1800-2200-32 –Toll Free**

- **24*7 Mail Support**
- **Descriptive Step by Step Assistance**
- **Quick response**
- **Support@gajshield.com**

- **Live Chat Support**
- **Instant access to Support Experts**
- **24*7 Chat assistance**
- **Human Assistance for unscripted support.**
- **www.gajshield.com**

GajShield Infotech (India) Pvt. Ltd.

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

@gajshield | @gajshield-infotech | @GAJSHIELD | @gajshield