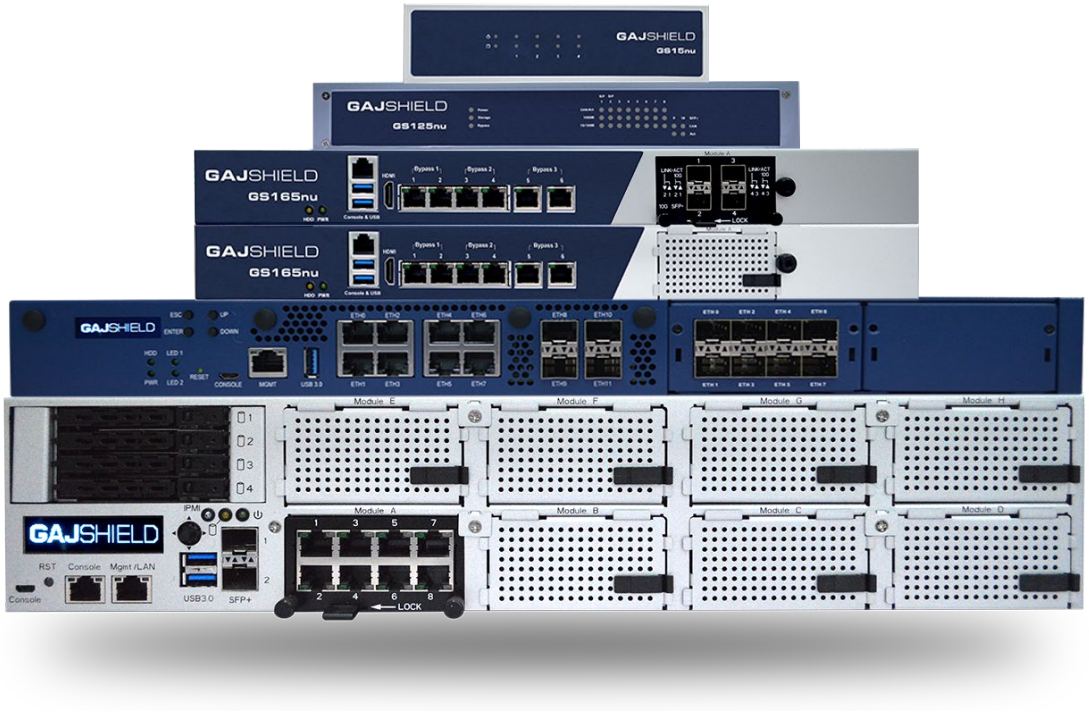
SD WAN



CONTEXTUAL INTELLIGENCE ENGINE

GajOS 4.0 BULWARK

GAJSHIELD
Data Security Firewall

Next Generation Firewall & more!

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 to 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

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 Centralized 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 of Setup and Operation

With the help of Centralized 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 to 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.

Highly Available

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) 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 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 (IPS), 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 High scalability & throughput overlay VPN tunnels to ensure that confidential traffic is always encrypted.

GAJSHIELD

Data Security Firewall

- Awards & Certificates -

GajShield Infotech (I) Pvt Ltd
Peninsula Centre, 4, Dr SS Rao Marg, Parel, Mumbai, Maharashtra 400012