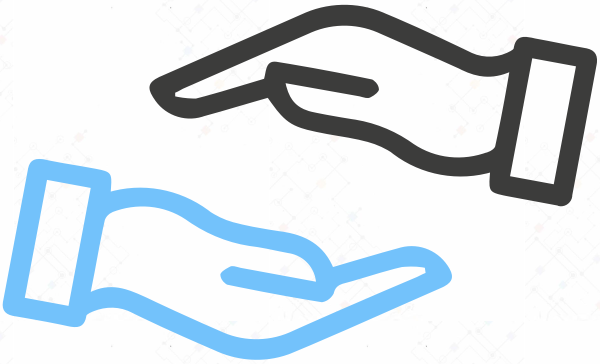
Zero Trust Network

GajShield Zero Trust Network



The zero-trust network eliminates possible data breach by creating a layer of protection that trusts none. It a data security strategy that is based on a "Trust None, Always Verify Concept".

Features of Zero Trust Network:

- Prevent unauthorized Movement of Data
- Prevent Data Exploitation
- Multiple Authentication Mechanism
- Prevent access to unauthorized Users

What Is Zero Trust?

Zero trust is a framework for securing organizations so that no user or application should be trusted by default. Following a key zero trust principle, least-privileged access, trust is established based on context (e.g., user identity and IP address, the app or service being requested) with policy checks at each step.

Zero Trust Definition

Zero trust is a cybersecurity strategy wherein security policy is applied based on context established through least-privileged access controls and strict user authentication—not assumed trust. A well-tuned zero trust architecture leads to simpler network infrastructure, a better user experience, and improved cyberthreat defense.

Zero Trust Architecture Explained

A zero-trust architecture follows the "never trust, always verify. A zero-trust architecture enforces access policies based on context—including the user's role and the data they are requesting—to block inappropriate access and lateral movement throughout an environment. Establishing a zero-trust architecture requires visibility and control over the environment's users and traffic, including that which is encrypted; monitoring and verification of traffic between parts of the environment; and strong multifactor authentication (MFA) methods beyond passwords, such as QR code or OTP via Email.

Critically, in a zero-trust architecture, a resource's network location isn't the biggest factor in its security posture anymore. Instead of rigid network segmentation, your data, workflows, services, and such are protected by software-defined micro segmentation, enabling you to keep them secure anywhere, whether in your data center or in distributed hybrid and multicloud environments.

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

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

ATP Features:

- Ransomware Protection
- Malware Protection
- Real-time protection from unknown threats
- Deploy signatures to the firewall when a file is identified as malware
- Analyses many different malicious files (executables, office documents, pdf files etc.) as well as malicious websites under various operating systems like Windows and Android.
- Trace API calls and general behaviour of the file and distil this into high-level information and signatures.
- Analyse network traffic, even when encrypted with SSL/TLS.
- Perform advanced memory analysis of the infected virtualized system
- Recurrent Pattern Detection of unknown malware through emailing protocols
- Multiple spam classification
- Independent of Content, Format, Language
- Real-time Blacklist (RBL), MIME header checks
- Filter based on message header, size, sender, recipient, subject line tagging
- Zero-hour Virus Outbreak
- Anti-botnet security

STATEFUL INSPECTION FIREWALL – ICSA CERTIFIED

- User Sense 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

***