Top Reasons to choose GajShield Unified Performance & Threat Management Appliances

Top Reasons why Customers get, complete and Proactive security with GajShield Unified Performance and Threat Management. In today's organization, application, employees, vendors, clients, and security threats fight for the same network resources. It has become difficult for small to medium enterprises to manage their infrastructure as they are unable to distinguish between good traffic v/s bad traffic. Threats or various productive applications have become smarter as they camouflage data transfer using standard internet ports. Current day security products have failed to distinguish and manage such malicious traffic.

1) **Proactive Security**
   Security problems become known when they start impacting the network and performance. Most of the time organizations do not find out security issues till they start impacting performance on the network and internet. Spyware is the best example of this. Organizations should look for solution that monitor the internet connection performance along with security breaches which can enable them to take proactive and informed decisions.

2) **Integrated Policy Management**
   Security, access and policies for application can vary by department , group, job function hence a solution should allow to deploy policy based on application bandwidth, content, scheduling, Natting, failover and access policy into an integrated interface

3) **Policy based Failover & Load balancing**
   Importance of applications can vary from one organization to the other so a solution should allow a per service ISP failover and load balancing. In the traditional security solutions all the services whether critical of non-critical have to be in failover or load balancing mode. This is very important in a country like india where ISP's are not yet stable and bandwidth provided in very low and not consistent.

4) **Policy based Protection**
   Policy based Protection for Firewall, IPS, Content filtering, P2P control, IM control, Adware, Spyware and set policies based on user identity or IP address. This provides more control over security.

5) **Corelation of isolated Internet and Network events**
   Today users, applications and threat all are fighting for the same network resources. Once you come to know that there is a problem, how can you identify and trouble shoot it? The current day solutions ask network administrators to look at various logs like Firewall, traffic logs, proxy logs or set up sniffers to identify problems. The normal administrator does not have time or the expertise to do these hence is left in lurch. GajShield correlates isolated events to provide tools for administrator to decisions in proactive and informed manner.

6) **Users, Applications and Threats will always demand more resources**
   There are three major source who will always demand for more Bandwidth
   a) Users will always want to download or upload larger and larger files
   b) Applications whether business-critical or non-business-critical applications will fight for the bandwidth as it is served on a first-in-first-out basis.
   c) Threat from newer breed of threats like spyware/adware/malware/viruses/P2P will demand and consume more and more of bandwidth which should have been available for business-critical applications.

7) **Policy based Performance Management** - what is happening on Internet and WAN resources, both by application and by user. GajShield provides both real time visibility and historical reporting - providing your company with the secure, intelligent data flow it needs.

8) **Gateway Antivirus Scanning :**
   GajShield UPTM provides inline and Real-time Gateway Virus scanning stopping the viruses at the network perimeter. The virus signature updates are continually made available on the GajShield UPTM appliance ensuring round the clock security from viruses.

9) **Spyware/Adware/P2P and URL Blocking**
   Spyware & P2P increases the bandwidth cost as well as making systems and business-critical applications slow . GajShield Spyware scanning provides a provides a powerful antis-spyware protection to organizations by identifying and stopping spyware infections. P2P control relieves the administrator from identifying the impact of P2P on the ISP bandwidth and give the ability to prioritize, limit, or stop them completely. GajShield UPTM is the only solution that correlates events show how different kinds of attacks impact your network.