GAJSHIELD

Security Simplified

Risks and Threats due to Web 2.0, Data Leak and internal threats

GajShield offers enterprises a unique approach DATA LEAK PREVENTION

Data leak prevention (DLP) technology has captured the attention of many IT organizations, with a promise to help organizations manage their confidential data. Project scope, for these technology providers, however, is a problem. Questions of access control, reporting, data classification, data at-rest vs. data in-transit, data ownership, desktop agents, server agents, and encryption have slowed DLP projects to a crawl in many organizations. Venture capitalists funded many data leakage prevention vendors, many of which have been acquired by larger security companies, who have further expanded the scope of an already unwieldy offering.

Some of these vendors are now marketing data loss prevention, which incorporates practically the entire information security function (and even includes elements of storage management!). Needless to say, this broadened scope is beneficial, but adds complexity, time, and expense – both in hard costs and in staff time. Oddly enough, many of the recent breaches caused by unauthorized and misconfigured peer-to-peer file sharing applications wouldn't have been prevented by the typical implementation of DLP technologies on the market today – because control of applications isn't addressed.

For 90% of Enterprises, knowing what is uploaded and controls to block it, keeping Social Security and Credit Card Numbers From Leaking Would Be Enough For a few highly intellectual property dependent organizations, implementing a long-term, comprehensive DLP project – which should ultimately include data discovery, classification, and cataloging – is appropriate. But for the remaining 90% of enterprises out there, stopping a couple classes of confidential data (e.g., uploaded files, social security numbers and credit card numbers) at the trust boundary would be a great start. This would avoid the expensive and embarrassing public exposure of employee and/or customer personal data.

• Data Leak Prevention

Applications like orkut, bit-torrent, facebook, youtube, 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.

- HTTP (42.57%)
- Email (15.84%)
- Malicious Web Pages (11.88%)
- Hiding in SSL (10.89%)
- Peer-to-peer (9.9%)
- Web Logs / Wikis (4.95%)
- Webmail (2.97%)
- IM (0.99%)

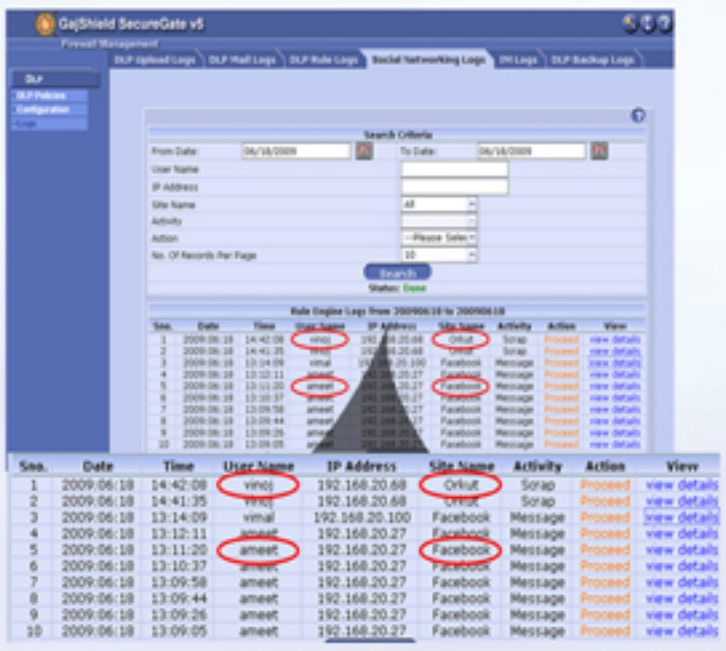
GajShield's Data Leak Prevention enables to control and mitigate leak of information by:

Visibility	Monitor	Detection	Precaution
• Giving visibility on the applications used and not just the ports or protocols. • Giving Visibility of information going out through Corporate mails & Web mails. • Giving visiblity of information going through Orkut scraps and facebook scraps.	• Monitor the content sent through applications used including HTTP, SMTP, SSL. • Monitor unwanted applications like P2P, Open proxies – to reduce the chance of information leak. • Monitor attachment going out of your organisation through webmails, corporate mails.	• Identifies Who is accessing, Which application and What content is being sent out. • Know who is sending information using yahoo, msn, webmail. • Know what content is being sent through Instant Messengers and Web chats.	• Define policies based on users rather than IP address. • Add rules for Popular mail sites to match mails on Subject, From, To, CC, BCC, Msg Body, Attachment Size, Attachment Type with a wide range of matching option. • Set runtime Mail Alerts based on DLP rules match.

• Web 2.0 Protection

GajShield DLP enables enterprises to benefit from the latest Web 2.0 technologies and applications in a secure corporate environment. Employees can use Web 2.0 without compromising corporate security or productivity. Organizations can secure and control the way their employees use Web 2.0 applications such as Facebook, MySpace or others, without the need for IT to completely block them. Collaborative applications such as IM, Skype, and P2P can also be controlled for better productive use.

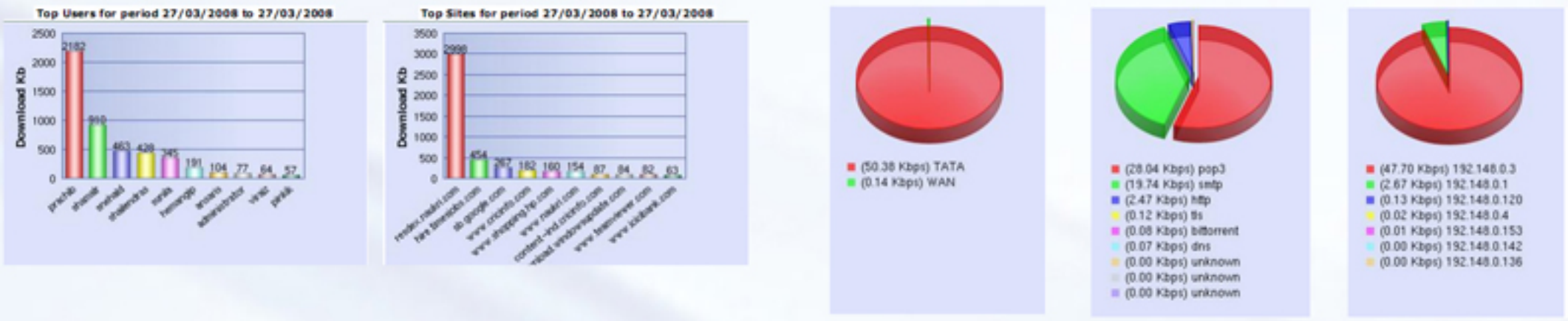
Using GajShield DLP, IT can apply specific policies that suit their organizational needs, such as allowing employees to access Facebook, while preventing them from posting comments or attachments to eliminate the risk of sensitive or confidential data leaking out.



GajShield DLP is uniquely capable of protecting organizations and companies - regardless of their size, location or business activities - against crimeware and malware posted on Web 2.0 sites. Since all Web content is analyzed, malicious content embedded in Web 2.0 pages is detected and blocked, while allowing legitimate content on the same webpage to be accessed. GajShield allows enterprises and their employees to fully embrace Web 2.0 in a secure and productive environment

• Productivity Control

Productivity control was one of the first issues that organizations had to deal with after their employees started to use the Internet. Employees access websites for business reasons, but also for personal use. They visited undesirable sites that contained adult content, gambling, gaming, trading, shopping or entertainment. This widespread non-work related use resulted in reduced productivity, waste of bandwidth, and liability issues.



GajShield DLP enables productivity, liability and bandwidth control combined with superior virus, spyware, malware filtering. As a result, this unified solution gives organizations control, security and compliance for all their web productivity, liability and security needs. With GajShield DLP, organizations can set policies for dozens of web categories, including Web 2.0, business related sites, Web email, streaming media, personals/ dating, society/lifestyle and dozens others.

• URL Filtering

Traditional URL filtering solutions are stretching beyond their limit, attempting to deal with today's increasingly complex web environment. The explosion in highly dynamic sites, user-initiated content, and growing web threats like drive-by downloads make it nearly impossible for these client-centric solutions to filter URLs meaningfully any longer.

GajShield's URL Filtering solution leverages its unique "in the cloud" infrastructure to provide unprecedented breadth of web coverage. The solution localizes responses specifically to the needs of end customers, avoiding the "one size fits all" approach of traditional solutions. With nearly two decades in the email security industry, GajShield provides matchless insight into threats, blocking harmful sites at the zero hour, often long before users are exposed to them.