DATA LEAK PREVENTION

Better visibility, control, and protection of your business

Security Challenges of Businesses - Data Leak a major concern

Hundreds of Web Applications traverse a network every day. Some of these applications, like social media provide a strong marketing tool but expose enterprise to risks. As perimeter of business boundaries is evaporating, it is leading to higher risk to business data and Intellectual Property. Intentional or unintentional data leak of information is a major concern for enterprises due to the exposure of users to increasing number of personal and business applications. The challenge that an enterprise face is that these applications use evasion techniques like dynamic or random port numbers or application emulation. Applications like Bit-torrent, Facebook, Gmail, Webchats, 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. This is because Firewalls don't understand content, don't understand applications, can't see inside SSL-encrypted traffic, and have no understanding of users. Enterprises are unable to match the Application risks and rewards, as Firewalls/UTM's are unable to provide visibility and control beyond, port and protocols.

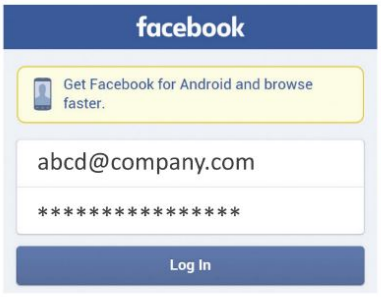
GajShield Firewall's Data Leak Prevention features

- 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.

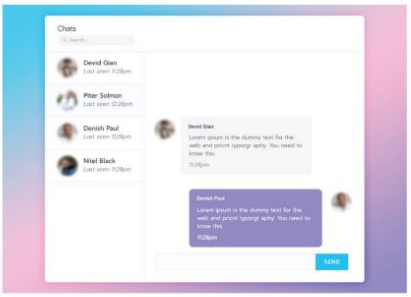
Web Leak Prevention

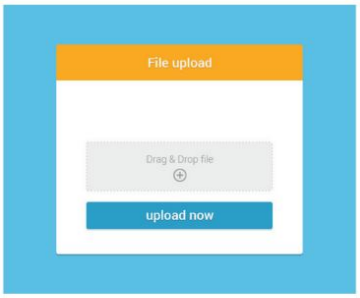
The most recent and profound development in cyberspace is the global migration of social media. As of March 2018; Facebook have 1.94 billion monthly active users, in a single second of the day, 7,615 tweets are posted to Twitter and 782 photos are posted on Instagram. Social media has become the new cyber battleground, presenting one of the largest, most dynamic risks to organizational data security in decades. With the help of GajShield Data Leak Prevention feature you can now setup policies to limit the access of these applications based on authorised users of these application who have been given access by your organization. With GajShield Data Leak Prevention you can also monitor and block files being uploaded on the internet with details of the application used and the user who used to upload this file. Even you can view the content of uploaded file. Many company allow employees to use instant message program to communicate, however, employees may send instant messages which are not related to their work, or even leak out a business secret, such communication can also be traced & blocked using GajShield DLP.

For example: You can allow your corporate Facebook id (abcd@company.com) to login to Facebook. All other login to Facebook using personal ids will be blocked. Even if the user is allowed to access Facebook then also he/she will be blocked, which means only corporate ids are allowed to login on Facebook. Similar policies can be setup even on Yahoo mail, Hotmail, Gmail & other social media can also be restricted.



Login only with you corporate email id


Trace live chat of disgruntled employee



Monitor & block files upload on the internet

SMTP Leak Prevention

Email continues to be dynamic to business communications and operations. An intrusion in which organization's disgruntled employee uses his/her own email to leak company's confidential data like clientele, pricing, financial data etc... this can cause financial losses to the company. With GajShield Data Leak Prevention System, policies can be configured at the organizational level, to block / trace email content and attachments sent by disgruntled employee and necessary action can be taken. Email can be tracked with entire email body content.You can create policies based on the 'From', To', 'Subject', 'Cc', 'Bcc', 'Email Body', 'Email size', 'Attachment name', 'Attachment size' of email applications.