White paper

CLEAR SWIFT

Look both ways

Protecting your data with content inspection

If you build it, they will come

In the early 1980's, Ethernet inventor Robert Metcalfe postulated that the value of any communications network increases in direct proportion to the number of connected users. Metcalfe's Law, as it became known, may have been developed in an era when the fax machine was at the cutting edge of communications technology, but as the success of everything from Facebook to company intranets illustrates, it's still relevant.

The more networks we build and the more information and ideas we share, the more opportunities to innovate and do business we create. The problem, of course, is that Metcalfe's Law applies equally to 'good' communications as it does to 'bad': As the number of users of any network increases, so too does the attack surface. And the more valuable the communications being created, the more attractive they become to criminals, who have adapted their methods in keeping with constantly evolving technology.

Five years ago, all the focus was on a relatively fixed landscape of Trojans, viruses and spam. Today, criminals are increasingly seeking to exploit vulnerabilities associated with individual users to gain access to their wider networks. Targeted attacks using familiar techniques are gaining traction in a cyber crime world where high value intellectual property, trade secrets, sensitive competitive information and other market-related data are becoming the currency of choice for criminals; with lists of credit card numbers fetching as little as $6 a pop on the black market, those with an eye for the bigger prize are looking to corporate data assets. Corporate spying has also become a key motivation for network breaches, with hackers gaining a toehold on company systems with a view to launching subtle data gathering software, often sending large volumes of sensitive data out of the organisation before they're noticed.

Research undertaken in the UK revealed 23 incidents in which NHS workers posted patient information on social networking sites such as Facebook. In one case, a medical employee at Nottingham University Hospital Trust posted a picture of a patient on Facebook, leading to their dismissal; the NHS has sacked 120 employees following a variety of data breaches.

Between July 2008 and July 2011, there were at least 806 separate incidents where patient records were compromised; that's five breaches every week.

Source: Big Brother Watch, UK.

Inside out

With much of the focus on cyber security emphasising in-bound threats, many organisation overlook the threat from within company walls: As Deloitte's 2011 *Global Security Survey* has pointed out, 'external attacks get most of the headlines, but internal security risks are just as onerous.' While many of the high profile attacks making the headlines are sophisticated, the reality is that the key 'in' for many cyber criminals is human error: Whether it's executable programs buried in harmless-looking spreadsheets, malware embedded in Word documents or dodgy links hidden in online games or services, the weakest link in the IT security chain is the tendency of people to click without thinking.

Factor in malicious intent, such as the Goldman Sachs programmer who stole code used for proprietary trading in 2009, or failure to grasp the seriousness of a situation, such as the UK National Health Service workers who shared sensitive data on Facebook, and it's easy to understand Ernst and Young security expert Jose Grando's statement that, in today's business IT environment, "The human being is now the perimeter, not the systems."

Get the balance right

Finding the right balance between ensuring the safety of sensitive data, enabling the free flow of information and using new web-based technologies is increasingly difficult in today's evolving regulatory and threat environment. Faced with reputational damage, loss of competitive edge and increasingly hefty fines for data breaches, many business leaders are adopting a stop-and-block approach to web-based services, despite widespread acknowledgement that these are crucial to the future success of their company.[1]

If businesses are looking to clamp down on social media usage, it's fair to say that any security ground gained there is likely to be undermined by what's best described as a cavalier attitude to email security. Research undertaken in 2011 found that large companies routinely risk losing highly sensitive data because board members access and exchange confidential information via web-based email accounts and mobile devices, sometimes over unsecured connections.[2] Forrester research has found that up to 75 per cent of intellectual property is sitting on email data stores and one in five outgoing mails contains data that poses a legal, financial or regulatory risk. The Brookings Institute estimates that 80 per cent of intellectual property is no longer tangible; companies today hold significant volumes of digital assets like market research, R&D strategies or product design data.

1 Clearswift – *WorkLifeWeb* report 2011
2 Thomson Reuters: *2011 Board Governance Survey*

Sensitive data is no longer controlled under lock and key in data centres or filing cabinets. It's everywhere. Locking down communications in today's business environment isn't a realistic solution to information security challenges. Dynamic business environments call for flexibility. Context is everything when it comes to deciding what information needs to be blocked or controlled. And when.

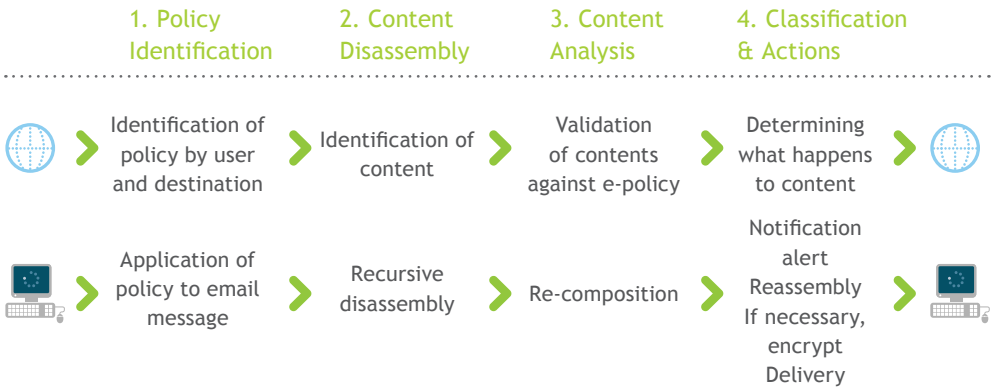
Look before you load: Deep Content Inspection

In a dynamic threat environment, web-based tools introduce an extra layer of vulnerability, creating threats that can't always be anticipated. At the same time, data entering and leaving the organisation needs to be strictly controlled. Content needs to be reviewed dynamically, in real time. Which is where deep content inspection comes in.

Clearswift's SECURE Web and Email Gateways allow your IT staff to work with end users to set flexible, secure parameters within which communications technologies can be used, whether it's placing limits on personal browsing, applying policy-based deep content inspection to automate the decision to encrypt sensitive content sent via company email or exchanged via online storage services such as Drop Box.

Clearswift's Gateways are built on the MIMEsweeper engine, which is responsible for data recognition, deconstruction and checking. The technology uses a process called recursive disassembly to examine complex data formats and analyse content for potential threats. During this process, the Gateway breaks down email or web content and messages, drilling down up to 50 layers of compressed or embedded body content, ensuring complete analysis of data.

The Web and Email Gateways use true binary-type file identification with full recursive decomposition analysis to ensure that no malware or inappropriate content is hidden within files. Message and file content can be identified by byte signature, deconstructing nested or compressed files and extracting all the useful parts of any piece of data before inspecting them.



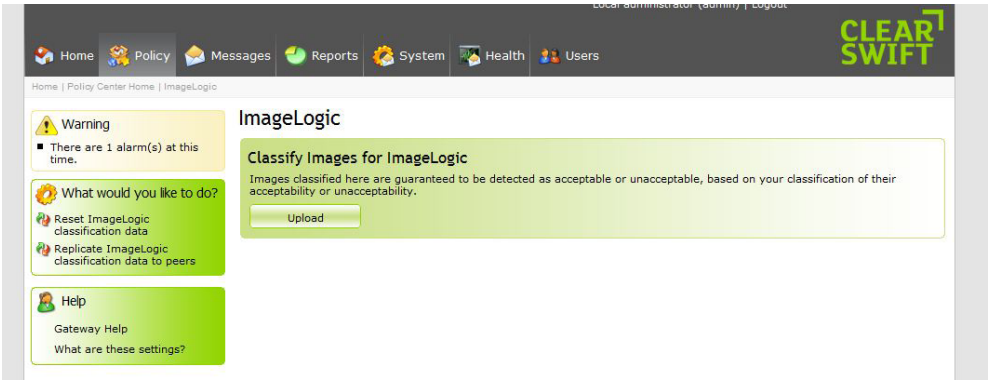
Bi-directional content inspection examines all data entering and leaving the organisation.

Going with the grain

The Clearswift engine recognises files using strict file type checking to ensure files aren't being re-named in an attempt to bypass filters. This includes strict inspection of the structural nature of the data, ensuring that files haven't been manipulated or hijacked to insert dangerous or sensitive data.

The data decomposition is highly granular, allowing document types such as Microsoft Office, archiving, streaming media and hundreds of other common file types to be analysed by source, type and bandwidth consumption. Documents can be deconstructed into their individual parts, meaning that keywords like 'Confidential' in the footer of a document is more important than finding it in the main body. File blocking using 'true type' recognition and keyword analysis using customer and supplied dictionaries is also permitted. The Clearswift content inspection engines will detect executables embedded within documents or other file formats, preventing users from unwittingly unleashing spyware or other malware onto organisational networks.

Clearswift's ImageLogic technology adds an additional layer of security for inappropriate or sensitive enterprise images being sent or received via email. Companies can use this image inspection technology to protect intellectual property by registering an image, such as a new product design, which can then be blocked from leaving the organisation. This gives users an additional layer of data loss protection.



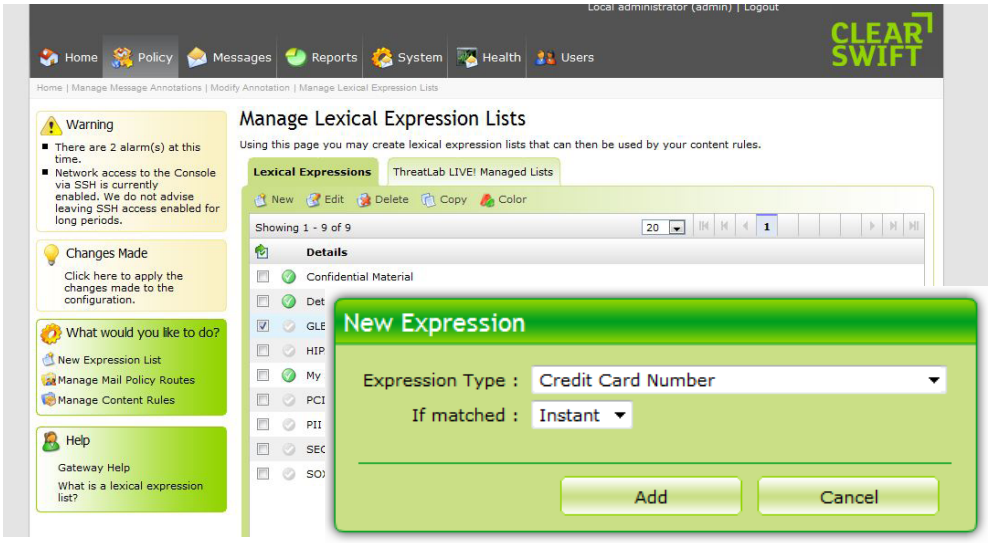
Images classified using ImageLogic are guaranteed to be detected as acceptable/unacceptable

Keyword search lowers insider risk

Keyword search is a very powerful mechanism capable of detecting information leakage, abuse, insider trading activity or inadvertent sensitive data leakage. Using single and complex expressions, regular expressions and operators, users can look for these and block them accordingly. Powerful expression lists allow users to build up search patterns for detecting content leaks; the regular expression engine combined by Boolean and positional operators allows constructs such as:

- Reference number FOLLOWEDBY=1 Part Number
- Credit Card numbers NEAR expiry dates
- Employee ID AND postal code

Content checking is extremely thorough; keywords can be extracted out of deeply nested files and Clearswift's technology can separate content in message bodies, word document headers or even the document author, extracted from document properties. Built-in rules will find commonly used data structures such as credit card, social security and IBAN numbers, which are checked for correct syntax to reduce the chances of false positives.



Deep inspection and intuitive scanning options are at the heart of the policy engine.

Users can define their own lexicons or use the supplied dictionaries, including PCI DSS, PII, SEC, SOX, HIPAA or GLBA. These capabilities makes finding a credit card number in a cell in an Excel spreadsheet embedded in a Word document that has been zipped easy.

Users can easily define the policies that will be applied to the data, choosing to execute specific security rules for sender and recipient, all based on the extracted data. Unrecognised file types can be blocked by default, quarantined and/or deleted.

High granularity capabilities mean the Clearswift policy management engines can configure rules and thresholds by department, location, user, group, sender, recipient, file type, file size, time of day or individual user. Once set, the content-aware policies will automatically invoke the prescribed response to any threat or potential breach, including block/delete/quarantine – and alerting relevant managers and generating tailored reports.

Inspecting web too

Clearswift's context-aware, deep content inspection capabilities mean that organisations don't have to sacrifice security for agility and collaborative innovation. The Web Gateway secures the social media experience, enabling productive use of web applications without exposing the organisation to data loss, intellectual property theft or malware attacks. This is because the content inspection engine is able to discern the difference between an innocent Tweet and potentially damaging data sharing.

Context-aware scanning allows you to prevent users from up/downloading sensitive data while continuing to exchange day-to-day data. Content inspection means that a user could be prevented from uploading restricted images or information to public sites such as Facebook; granularity means that authorised users, such as the marketing department, would have a different policy applied following the inspection of the content they wanted to share.

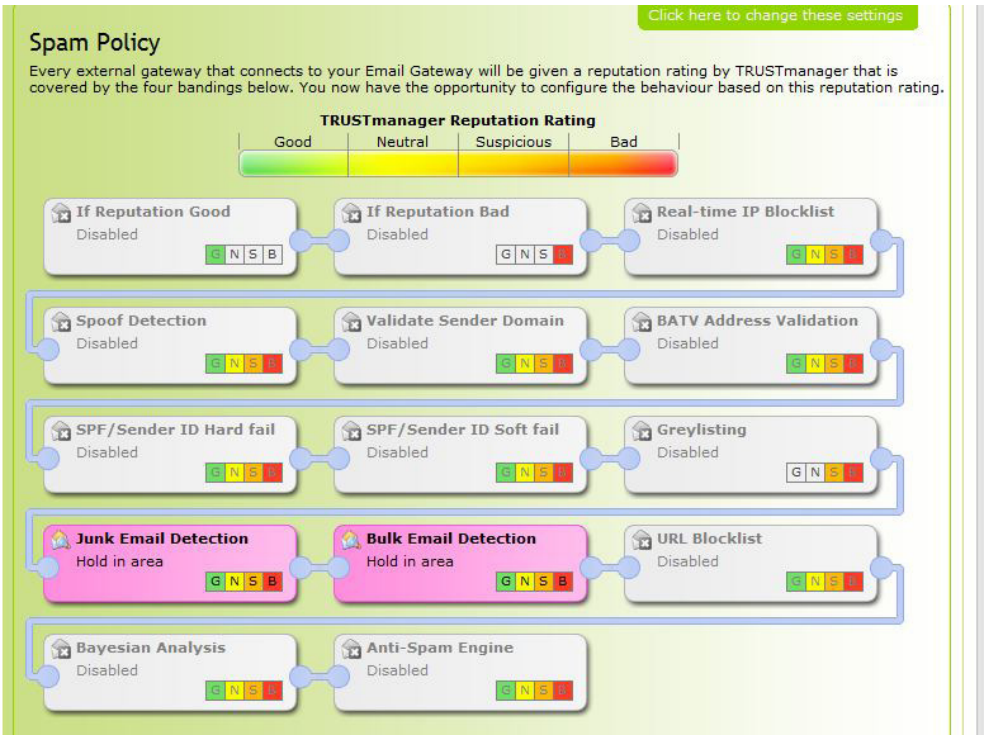
The social web is dynamic and so too are the threats that come with it. Javascript, Flash and other script-based malware can be launched through harmless-looking applications. The Web Gateway analyses all the traffic coming into the network, breaking it down and inspecting the content to ensure that nothing malicious can enter the network, even if it's buried within an application or hidden within an ostensibly secure site. Deep content inspection also guards against accidental uploads of files to inappropriate locations or recipients using web services such as Drop Box.

Look both ways

Content inspection and filtering capabilities aren't just about preventing sensitive data from leaving your organisation. Clearswift's Unified Information Security (UIS) approach adds further robustness to network defences in the form of high-quality, zero-day malware, anti-virus and anti-spam capabilities. These work alongside the content inspection engines to prevent suspicious content and spyware from entering the network, while continuing to inspect data that's flowing out.

Zero hour anti-malware filters offer early detection, allowing proactive defence against new, undiscovered malware based on 'honey pot' activity. This works in tandem with the deep content inspection engines, examining message attachments and web-based content, among other things, to ensure that no data enters the network unchallenged. Once flagged, the content is analysed against relevant policy and automatically dealt with accordingly.

Spam is dealt with via a global reputation network that detects and rejects 80-90 per cent of all spam traffic before it reaches the gateway, saving time, bandwidth and administration costs. Spam is detected and dealt with on a 99.6 per cent accuracy basis, while Clearswift's TRUSTmanager contains over 50 million IP addresses. A dynamic feedback mechanism constantly monitors behaviour and adjusts settings accordingly.



Configure spam response based on TRUSTmanager ratings

Seeing the wood for the trees

Today's threat environment is as dynamic as the business world in which we operate. As the communications channels we use continue to proliferate and evolve, so too have the vulnerabilities.

Finding the right balance between ensuring the security of sensitive data, enabling the free flow of information and making full use of the latest web-based technologies can be a challenge. Context-aware content inspection allows you to automate the inspection of all traffic entering and leaving the network, eliminating the clutter to give a clear picture of where the real threats lie.

Deep content inspection is a vital layer in any unified information security strategy, helping organisations to take control over their information assets while proactively protecting against malware and data leakage.

If you block everything, you see nothing. Managing traffic based on content inspection allows organisations to apply highly-granular policies to all communications and users, allowing everyone to make the most of the tools they need, while mitigating the security risks that come with information exchange.

Get in Touch

CLEAR SWIFT

Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale
Reading
Berkshire
RG7 4SA

Tel : +44 (0) 118 903 8903
Fax : +44 (0) 118 903 9000
Sales: +44 (0) 118 903 8700
Technical Support: +44 (0) 118 903 8200
Email: info@clearswift.com