White paper

CLEARSWIFT

Yes. We. Can.

Flexible Policy 2.0

Yes.We.Can.

Mark Twain wasn't talking about social media use in the workplace when he said "To a man with a hammer, everything looks like a nail" but he might as well have been. In the face of high-profile data breaches and perceptions that the social web is little more than a productivity vampire, an increasing number of organisations are simply locking it all down and preventing employees from using it.

It's not that people can't see the benefits: With more than a billion users worldwide, half of whom connect with an average of 12 brands[1], business leaders understand the value proposition of the social web. The problem is, they also understand the risks: While 58 per cent of respondents in Clearswift's 2011 WorkLifeWeb survey said they viewed web collaboration services as crucial to their future success, 87 per cent said security concerns were the main issue holding them back.

It doesn't have to be that way.

Clearswift's Flexible Policy engines mean you can have your social media cake and eat it too. Flexible policy means you don't have to sacrifice security for agility and collaborative innovation. Traditional stop-and-block technologies are neither flexible nor intelligent enough to understand the nature of the content being exchanged and, crucially, how and where it can legitimately be used.

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

"Clearswift's WorkLifeWeb research for 2011 shows that 19 per cent of companies worldwide now completely block social media use, rising to 56 per cent when it comes to specific sites."

Social media may have changed the way we do business, but the rules of engagement are still the same. Dynamic business environments call for flexibility. Context is everything when it comes to deciding what information needs to be blocked or controlled, and when.

Trick or Tweet?

Social networking is useless without the sharing element. But you don't want employees sharing sensitive product release data or making the kind of comments that anyone with the brains to read between the lines will be able to extract information from. And you definitely don't want anyone uploading sensitive files or downloading potentially dangerous content.

Clearswift's technology secures your social media experience, enabling the productive use of web applications without exposing your organisation to data loss, intellectual property theft or malware attacks – because it knows the difference between an innocent Tweet and potentially damaging data sharing. Context-aware scanning and policies mean that users can be prevented from up/downloading sensitive data while continuing to exchange day-to-day data. Data uploads can be restricted according to the nature of the application: For example, you might want safe data sharing on Salesforce.com but need to be able to block it on Facebook. No problem.

This granularity can be extended right down to individual user level, where different users with different access requirements are given the tools they need to get the job done. Clearswift's technology now offers pre-defined, out-of-the-box policies for the most popular social media sites (Facebook, LinkedIn, Twitter and YouTube), while making it easy for you to configure further policies according to your needs. Authentication, policy and a content-aware gateway combine to enable social networking services while minimising the risks. Here's how...

[1] InSights Consulting: Social Media Around the World, 2011.

"From a security perspective , dealing with pornography is easy: It's a binary decision, you block it or you don't, it's a one-policy-fits-all situation.

Web 2.0 and social media sites are different because the purpose, capabilities and access control for specific functionality can all be factored in when you're building a policy using Clearswift's technology. This allows users to access the business, productivity or even just staff relations benefits of the social web without endangering company data and security."

- Mark Maciw, Global Product Manager, Clearswift.

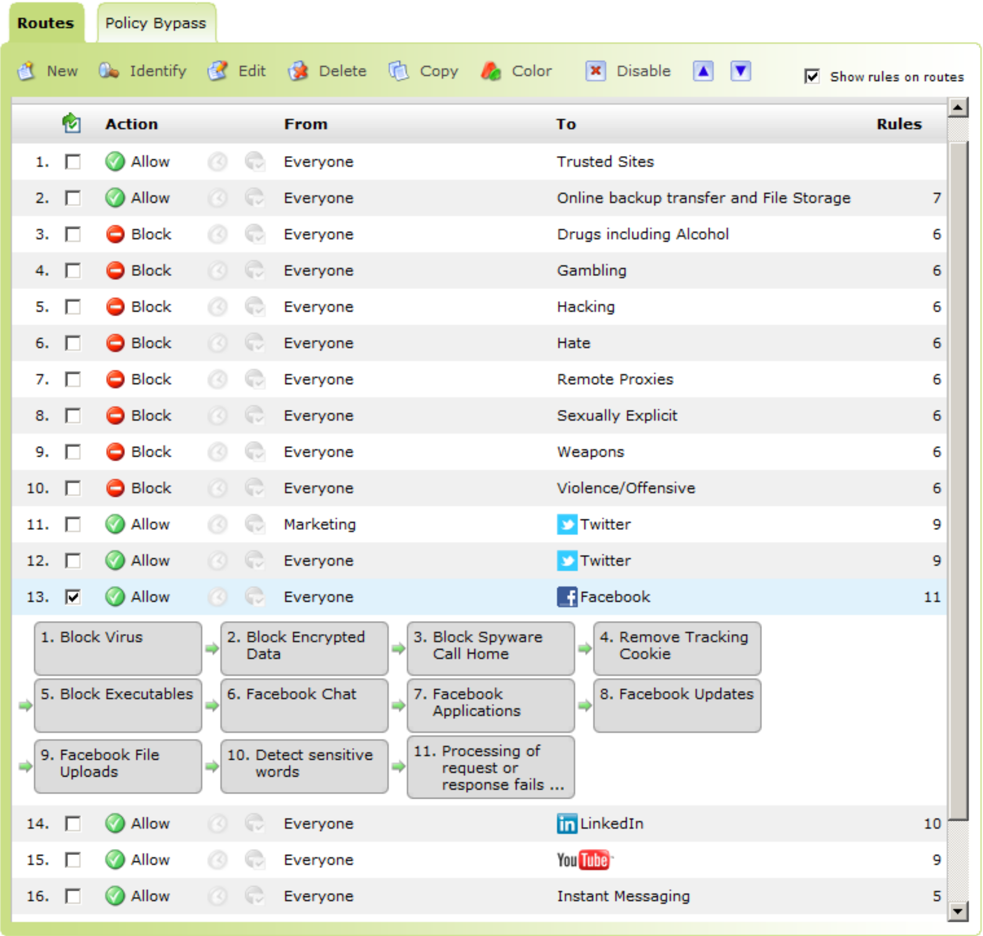
Keep the good stuff, block the bad

The social web is dynamic, so it shouldn't come as any shock to find that so too are the attacks that hackers launch through it. Javascript, Flash and other script-based malware can lie buried inside harmless-looking applications, just waiting for an innocent click through to open the backdoor to your business.

Clearswift's technology moves beyond simple URL filtering with real-time scanning to monitor sites like Facebook for threats that might ordinarily slip through the cracks. Multi-layer malware control keeps viruses and malicious code at bay, while filters ensure anything you deem inappropriate is kept out – e.g. adult content, games, gambling, phishing sites.

Granular, content-aware Web 2.0 policies enable collaboration

All acceptable use policies need the flexibility to adapt to different job functions and departments. For example, you might want to allow your marketing department to be able to access functionality on Facebook that you don't want extended to other users. Or maybe you want staff to be able to access YouTube for specific content such as training materials but not for videos of cats on skateboards...Clearswift enables you to set specific policies that allow control over any given site's capabilities.



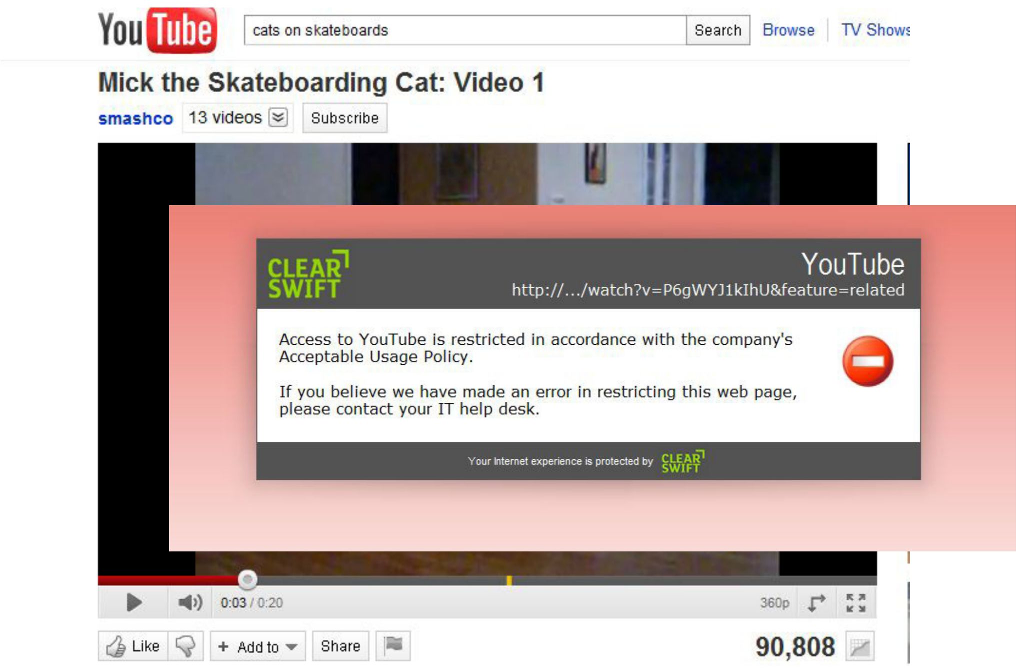
		Action	From	To	Rules
1.	□	Allow	Everyone	Trusted Sites	
2.	□	Allow	Everyone	Online backup transfer and File Storage	7
3.	□	Block	Everyone	Drugs including Alcohol	6
4.	□	Block	Everyone	Gambling	6
5.	□	Block	Everyone	Hacking	6
6.	□	Block	Everyone	Hate	6
7.	□	Block	Everyone	Remote Proxies	6
8.	□	Block	Everyone	Sexually Explicit	6
9.	□	Block	Everyone	Weapons	6
10.	□	Block	Everyone	Violence/Offensive	6
11.	□	Allow	Marketing	Twitter	9
12.	□	Allow	Everyone	Twitter	9
13.	☑	Allow	Everyone	Facebook	11
14.	□	Allow	Everyone	LinkedIn	10
15.	□	Allow	Everyone	YouTube	9
16.	□	Allow	Everyone	Instant Messaging	5

Rules for route 13:

1. Block Virus
2. Block Encrypted Data
3. Block Spyware Call Home
4. Remove Tracking Cookie
5. Block Executables
6. Facebook Chat
7. Facebook Applications
8. Facebook Updates
9. Facebook File Uploads
10. Detect sensitive words
11. Processing of request or response fails ...

Allow or deny access to things like Facebook Chat, applications, status updates, file uploads/downloads.

The pre-defined routes for sites like Facebook work in addition to the standard, generic web routes that come with the Web Gateway. Each of these defined routes comes pre-populated with content rules allowing policies to be defined based on a site's capabilities. As mentioned above, different departments with different policy requirements can be catered for through the addition of multiple routes.



Mick the Skateboarding Cat: Video 1

CLEAR SWIFT

YouTube

http://.../watch?v=P6gWYJ1kIhU&feature=related

Access to YouTube is restricted in accordance with the company's Acceptable Usage Policy.

If you believe we have made an error in restricting this web page, please contact your IT help desk.

Your Internet experience is protected by CLEAR SWIFT

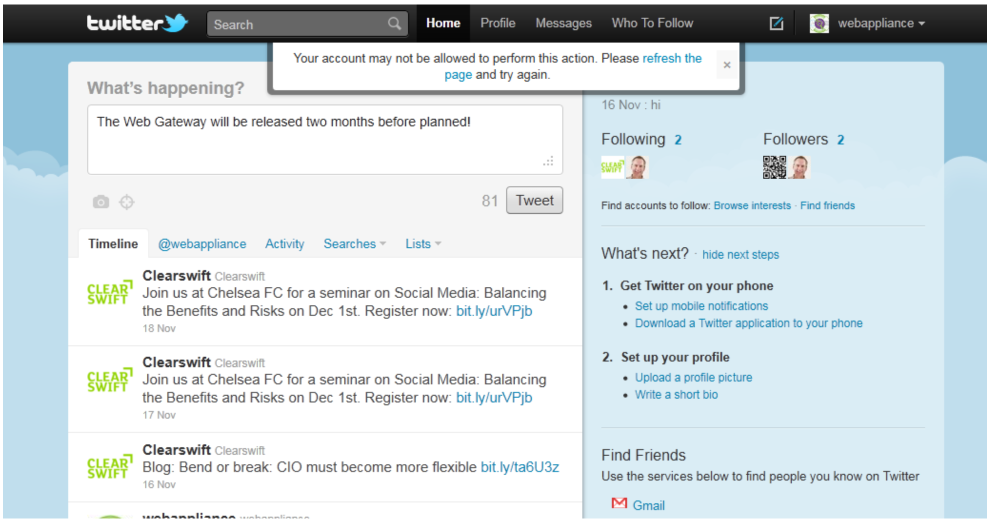
The YouTube site can be accessed and searched but only authorised videos can be viewed.

Don’t be the next headline: Data Loss Prevention

Respondents to Clearswift’s annual *WorkLifeWeb* research said security concerns were the main obstacle to their organisation fully embracing the social web. As we mentioned before, social networking is useless without the sharing element, which is where deep content inspection comes in. To really protect your organisation’s IP and other information assets, monitoring the data leaving the network is just as important as keeping an eye on what’s coming in.

Clearswift’s Web Gateway technology uses deep content inspection to search for and identify keywords and phrases within attached/up/downloaded documents. Think credit card numbers, IBANs, phrases like ‘confidential’ in the footer of a document... depending on company policies, responses include completely blocking (and reporting) the attempted exchange or issuing an alert asking the user if they’re sure about what they’re doing.

For Twitter, where a key concern is employees discussing sensitive business information, you can set the Gateway to block the key phrases most likely to indicate risk in your specific industry. For example, a financial services organisation may wish to flag words like ‘buy’, ‘sell’ or ‘share’ while a software company may wish to block any references to product names or release dates.



Your account may not be allowed to perform this action. Please refresh the page and try again.

What’s happening?

The Web Gateway will be released two months before planned!

Clearswift Clearswift
Join us at Chelsea FC for a seminar on Social Media: Balancing the Benefits and Risks on Dec 1st. Register now: bit.ly/urVPjb
18 Nov

Clearswift Clearswift
Join us at Chelsea FC for a seminar on Social Media: Balancing the Benefits and Risks on Dec 1st. Register now: bit.ly/urVPjb
17 Nov

Clearswift Clearswift
Blog: Bend or break: CIO must become more flexible bit.ly/ta6U3z
16 Nov

16 Nov : hi

Following 2 Followers 2

Find accounts to follow: Browse interests · Find friends

What’s next? · hide next steps

1. **Get Twitter on your phone**
   - Set up mobile notifications
   - Download a Twitter application to your phone
2. **Set up your profile**
   - Upload a profile picture
   - Write a short bio

Find Friends

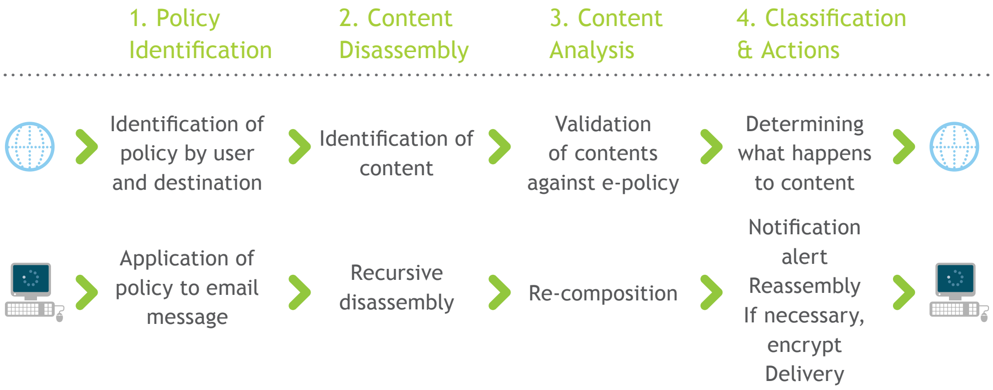
Use the services below to find people you know on Twitter

Gmail

The Tweet contained a product name and was stopped.

The Web Gateway includes pre-configured dictionaries for compliance with PCI, PII, SEC, SOX and HIPAA as well as templates for IBAN, credit card, national insurance and social security numbers.

Clearswift uses a process called recursive disassembly to examine complex data formats and analyse the content for potential threats. This breaks down email messages and web traffic, drilling down up to 50 layers to completely analyse all data. Apart from preventing malicious exchange of IP or other valuable business information, the content aware engine prevents those ‘Oops’ moments, where you accidentally upload the wrong file or try to share it with the wrong person.



1. Policy Identification	2. Content Disassembly	3. Content Analysis	4. Classification & Actions
Identification of policy by user and destination	Identification of content	Validation of contents against e-policy	Determining what happens to content
Application of policy to email message	Recursive disassembly	Re-composition	Notification alert Reassembly If necessary, encrypt Delivery

Auditing and reporting

Effective policy is a living thing that should be as dynamic and flexible as the social web you’re working to secure. Easy-to-use auditing and reporting functionality will allow you to gain a strong handle on how your organisation uses web services, making it easy for you to refine and hone your policies around usage.

Clearswift’s Web Gateway allows you to investigate and analyse individual user activity, such as sites accessed and files uploaded/downloaded. Any policy violations or threats will be detected, allowing you to act accordingly by blocking certain kinds of applications or placing time limits on the use of certain kinds of site, such as online shopping.

The human factor

Now’s probably a good time to point out that no matter how good the policies applied at your Gateway are, employees increasingly have smart devices and home networks from where they can break the rules.

There’s only so much you can do about this, but it’s not all bad news: Strong, well-communicated policies can be further enhanced through ongoing employee education regarding responsible usage. Keep your staff well informed regarding the risks associated with social networking sites, not only from a malware and file exchange perspective, but also from the point of view of making it clear what sort of work-related information can be discussed in public and, more importantly, what can’t. When it comes to effective policy, always factor-in the ‘Three E’s’: Establish, Educate and Enforce. Policy can only ever be as good as your organisation’s capacity to communicate and enforce it.

Clearswift’s Web Gateway will also protect your organisation from those momentary lapses in concentration, when users accidentally click a malicious link or browse to a site that might be in breach of regulations. Apart from simple blocking, the issuing of timely alerts reminding users of company policy before allowing them to choose whether or not they continue can also serve to drive increased awareness and responsible usage.

Social with security

The social web's popularity is also its biggest risk. The more people use it in both work and personal contexts, the more the lines of acceptability are blurred. Similarly, the more familiar users become with social media, the less switched-on to risk they can become, leaving them vulnerable to exploitation by hackers who know only too well where the weakspots are. From scouring the social web for the sort of information that can facilitate social engineering exploits to using popular services to disseminate malware, the threats are obvious.

With traditional software and services, organisations simply made one of two choices: block it or don't block it. Web 2.0 and social media services are different because the business benefits are many: From building brand awareness to enhancing communications, increasing productivity and having a motivated, happy workforce, most organisations don't want to pull a good thing down.

Fortunately, you don't have to. It's time to adopt more flexible policies that deal with the twin realities of social media and smart device proliferation. Unified, flexible policies drawing on a shared set of rules mean you can apply the same security standards and limits to all communications channels. Policy, not policing creates the confidence to tackle the negative side effects of evolving communications without spoiling the party.

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