Clearswift and F5® mitigate web application information breaches

The need to protect critical and sensitive information is a priority for all organizations. At the same time, increased numbers of industry and state regulations are being implemented to protect all forms of information to minimize the growth of data breaches, with substantial financial penalties, reputational damage and loss of business differentiation for those who do not increase their awareness and implementation of appropriate information protection. The majority of coverage in the industry centres on information leaks that happen through the Internet gateways, hidden as common data types or standard browsing traffic. But Clearswift and F5 customers have acknowledged that a larger exposure exists in the protection and control of the communication channels used by the information their webservers provide to external stakeholders as part of their information value chain. This exposure goes well beyond not only having their homepage defaced, which in itself damages the reputational and business efficiency of the organization, but more damaging, what information may have been leaked through via the exposed webserver. Unfortunately, many organizations take the approach of relying on standalone security architectures that do not meet the increased complexity of today's advanced threat environment and the growth of insider threats from employees, contractors and business partners. Information protection can no longer be treated as an afterthought there is a necessity to take control and act in real-time to remediate the exposure that applications web servers can contribute to critical information losses. Clearswift and F5 have partnered together to provide a highly scalable secure application delivery platform that takes full advantage of Clearswifts unique Adaptive Redaction technology and F5 high performance and optimized application delivery architecture, with the ability to detect information security issues and transparently resolve them in a pro-active manner before the loss, alerting organizations to the potential breach immediately.

Why every organization is a potential victim of 'Team Attacker'!

Ask the majority of organizations if they have been attacked via a cyber-activity and the response would systematically repeat 'no', 'not us', 'they could get through our security', 'probably, but it hasn't hurt us', 'no, we don't have anything of value', 'definitely not, I'd know if we had been breached'. Consider this, the average date of intrusion of breach discovery is approximately 300 days[1], so the immediacy of breach awareness, is about as rare as a finding a 'mint perfect' Honus Wagner baseball card[2] or realizing your copy of 'A Midsummer Night's Dream' was signed by Shakespeare[3]. In a targeted attack, your organization is singled out because the attacker has a specific interest in your business, or has been paid to target you. The groundwork for the attack could take months so that they can find the best route to deliver their exploit directly to your systems (or users). A targeted attack is often more damaging than an un-targeted one because it has been specifically tailored to attack your web servers, applications, processes or personnel, in the office and sometimes at home.
The independent attacker or 'Lone-Wolf' still exists, primarily to gain a reputation or make a statement, but the attackers who spend weeks and months surveying your organization as a potential honey pot of valued information will come from the 'Premier League' of black hatters. Under a matrix operational model, actors sign up and transfer from one cause or objective to another under the simplicity of anonymization, credentials and belief. Who might 'Team Attacker' comprise? Cyber criminals interested in making money through fraud or from the sale of valuable information stored on your web servers or executed within your applications; Industrial competitors and foreign intelligence services, interested in gaining an economic advantage for their companies or countries; Hackers who breach your organizations [apparently secure] collaboration channels as an enjoyable challenge; Hacktivists who wish to attack companies to gain insights of their political or ideological preferences; Employees, or those who have legitimate access, either by accidental or deliberate misuse and finally Script Kiddies (a derogative term, by the more sophisticated crackers), the apprentices and interns of the 'Team' who have yet to earn their stripes, but unfortunately often just as dangerous for exploiting back door and patch flaw security lapses on applications web servers.

1 Don Ulsch, Managing Director, Price Waterhouse Coopers, 2014

2 aT206 Honus Wagner, made by the American Tobacco Company, 1909. Sold for $2.8 million in 2012. It has been called the "Mona Lisa of baseball cards."

3 William Shakespeare' s signature is one of the rarest of all, with only 6 of them in existence and valued somewhere around $3 million dollars

Clearswift and F5 integration

Addressing the need to widen a pro-active advanced threat protection strategy, whilst also accurately identifying and protecting critical information assets, F5 and Clearswift have worked together to provide a solution that provides the unique opportunity to address unauthorized information collaboration and removal of potential embedded advanced persistent threats

The resulting platform takes advantage of the perfect match between both technologies to provide some unique key features:

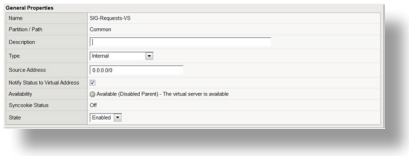
- Adaptive Redaction to modify requests and responses to prevent data loss and targeted attacks from infecting the organization
- Adaptive Redaction to recognise, inspect and mitigate unauthorized data streams leaving a host web server
- Adaptive Redaction to identify and block or remediate web page loads with inappropriate content
- Deep content inspection to identify data fingerprints and hidden meta data
- Complete protection and control, including SSL connections for decryption and inspection
- Layered defences for complete web server protection

The deployment is greatly simplified by using the industry standard protocol ICAP, which allows decisions to be made, based upon policy rules, identifying which content, from/to which user and to/from which site, needs to be inspected.

This is an industry recognized integration method for F5 BIG-IP® administrators and requires just three simple steps:

- Configure the ICAP virtual services in the F5®BIG-IP® Local Traffic Manager™ (LTM®)
- Set the policy to redirect specific traffic to the Clearswift SECURE ICAP Gateway for inspection
- Configure the Clearswift SECURE ICAP Gateway to accept connections from F5®BIG-IP® Local Traffic Manager™(LTM)

1 | SECURE ICAP Gateway Virtual Servers definition in F5 BIG-IP LTM



2 | Adaptation configuration in the target Virtual Server in F5 BIG-IP LTM

Clearswift technology overview

Clearswift's deep content inspection technology can recursively decompose the communication flows to granularly apply information security policies.

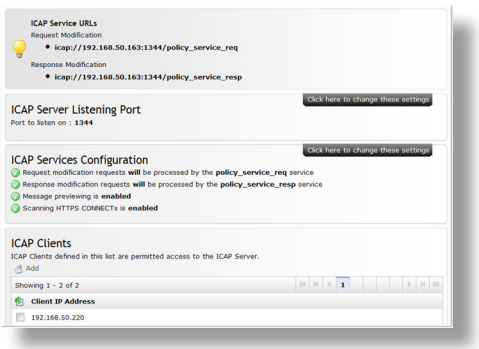
The Clearswift SECURE ICAP Gateway can perform true data type detection even with embedded objects. Once identified, the information is then extracted and analyzed to detect potential data breaches.

In order to simplify the definition of the content security policy, predefined templates with common dictionaries are provided. The ability to detect tokens, like credit card numbers, and to obtain content from structured data sources – such as databases – makes it even simpler to determine the nature of the information and to drastically reduce the number of false positives.

Blocking violations is the first approach that companies tend to think of when talking about data losses. Even though this might be valid in some cases, Clearswift introduces technology to modify the content to remove the offending content while allowing the rest of the communication to happen. Even hidden meta-data which might contain revision history or quick save data is stripped out. Business processes are not hindered and the critical information asset is protected.

The ability to make immediate changes is applicable for bi-directional (forward and reverse proxy) content and is not limited to removing data. Advanced persistent threats (APTs) can also be removed from their common infection vectors with the active content removal feature.

3 | Clearswift SECURE ICAP Gateway configuration to accept F5 BIG-IP LTM as an ICAP Client



Once the integration is done, the inspection policy can be configured in the Clearswift SECURE ICAP Gateway.

F5 technology overview

BIG-IP products have been recognised as leaders for Application Delivery Controllers by Gartner for over a decade. BIG-IP products offer the application intelligence that network managers need to ensure applications are fast, secure, and available. All BIG-IP products share a common underlying architecture, F5 TMOS®, which provides unified intelligence, flexibility, and programmability. Together, BIG-IP platforms, advanced modules, and centralized management system make up the most comprehensive set of application delivery tools in the industry.

About F5

F5 (NASDAQ: FFIV) provides solutions for an application world. F5 helps organizations seamlessly scale cloud, data center, telecommunications, and software defined networking (SDN) deployments to successfully deliver applications and services to anyone, anywhere, at any time. F5 solutions broaden the reach of IT through an open, extensible framework and a rich partner ecosystem of leading technology and orchestration vendors. This approach lets customers pursue the infrastructure model that best fits their needs over time. The world's largest businesses, service providers, government entities, and consumer brands rely on F5 to stay ahead of cloud, security, and mobility trends. For more information, go to f5.com.

clearswift | SCC We make IT work

Clearswift and SCC

Clearswift is trusted by organizations globally to protect their critical information, giving them the freedom to securely collaborate and drive business growth. Their unique technology supports a straightforward and 'adaptive' data loss prevention approach, avoiding the risk of business interruption and enabling organizations to have 100% visibility of their critical information 100% of the time

The partnership between Clearswift and F5 is a significant development that will help SCC customers to maintain visibility of, and control access to, their web application critical information. It will provide a tangible benefit that SCC can pass on directly to customers as we work with them as they transition to a phase of consuming more web services and applications.

SCC's relationship and Gold Partner status with both Clearswift and F5, combined with our deep technical skills, experience and capabilities across a broad range of sectors, vendors and partners, ensures we can provide customers with a complete end-to-end solution. We have the ability to design, supply, install, support and maintain integrated Clearswift and F5 solutions and also have a wealth of experience working with government and defence organisations to whom we supply products and services through a number of purchasing frameworks, including: Technology Products; Technology Services; and G-Cloud.

United Kingdom
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale
Reading, RG7 4SA
UK

Germany
Clearswift GmbH
Landsberger Straße 302
D-80 687 Munich
GERMANY

United States
Clearswift Corporation
309 Fellowship Road
Suite 200
Mount Laurel, NJ 08054
UNITED STATES

Japan
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
JAPAN

Australia
Clearswift (Asia/Pacific) Pty Ltd
Level 17
40 Mount Street
North Sydney
New South Wales, 2060
AUSTRALIA