clearswift

Critical Information Protection for Application Availability with F5 & Clearswift.

Protecting sensitive web application information from inside and external threats.

What is the solution?

Available with the integration of unique Adaptive Redaction technology via the Clearswift SECURE ICAP Gateway (SIG) with F5® BIG-IP® Local Traffic Manager™ (LTM®).

As a member of the F5 Technology Alliance Program (TAP), together Clearswift and F5 provide a highly scalable secure application delivery platform that takes full advantage of Clearswift's unique Adaptive Redaction technology, enabling the ability to detect information loss risks alongside the facility to resolve them in a pro-active manner, alerting organizations to potential internal or external data breaches; immediately.

What is the SECURE ICAP Gateway?

The Clearswift SECURE ICAP Gateway (SIG) provides organizations with the ability to apply deep content inspection, adaptive redaction and data loss prevention technologies to existing web architectures, with no disruption to the current infrastructure, thereby having the ability to align the flow of information to the organization's information governance policies, mitigating risk and underpinning compliance requirements.

What is BIG-IP LTM?

BIG-IP LTM resides within the BIG-IP family of products that offer the application intelligence that network managers need to ensure applications are fast, secure and available. BIG-IP LTM increases your operational efficiency and ensures peak network performance by providing a flexible, high-performance application delivery system. With its application-centric perspective, BIG-IP LTM optimizes your network infrastructure to deliver availability, security and performance for critical business applications.
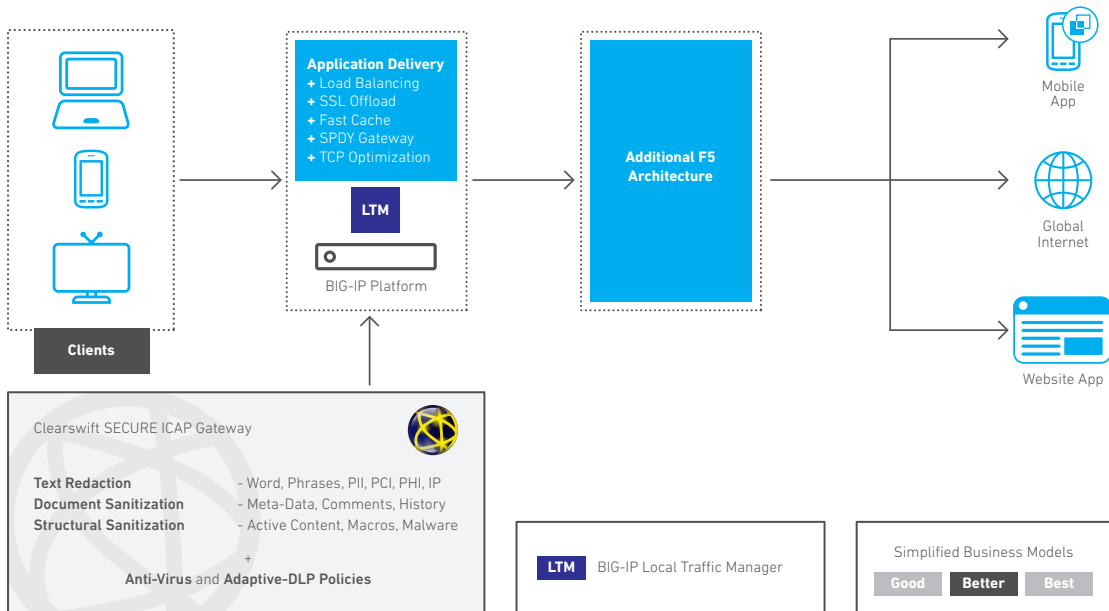
What is Adaptive Redaction?

Adaptive Redaction is the removal or transformation of data according to policy (rules), to ensure that information complies with corporate information security policies before it is sent to or received by the recipient (person, application or system). Traditional Data Loss Prevention (DLP) solutions are a simple 'yes' or 'no' to sending information, as they lack the architectural design to inspect, disassemble and apply recursive assembly to the content 'in its original format'. Adaptive Redaction removes this barrier by modifying the information according to policy to ensure only acceptable levels of information are shared and received in a bi-directional manner, and that critical and sensitive information utilized by application web services remain secure at all times.

How do the products integrate?

The introduction of the SECURE ICAP Gateway and BIG-IP LTM solution can be installed as a new client implementation or should a client already have BIG-IP LTM already installed the SECURE ICAP Gateway integrates via a connection that utilizes the ICAP protocol architected within BIG-IP LTM.

Adaptive Redaction options can be implemented on data flowing through BIG-IP LTM in 'monitor mode' initially, so clients can see the results of their policies without impacting the operational environment. When satisfied with the outcome of the policies, they can be switched (turned on) into operational mode.

Application Delivery
+ Load Balancing
+ SSL Offload
+ Fast Cache
+ SPDY Gateway
+ TCP Optimization

LTM

BIG-IP Platform

Additional F5 Architecture

Clients

Mobile App

Global Internet

Website App

Clearswift SECURE ICAP Gateway

Text Redaction	– Word, Phrases, PII, PCI, PHI, IP
Document Sanitization	– Meta-Data, Comments, History
Structural Sanitization	– Active Content, Macros, Malware

+

Anti-Virus and **Adaptive-DLP Policies**

LTM BIG-IP Local Traffic Manager

Simplified Business Models
Good Better Best

What are the benefits?

Cloud Connectivity

- As organizations adopt a public, private, or hybrid cloud approach, Clearswift and F5 simplifies the optimization, authorized information collaboration and accessibility of business applications, ensuring that they're fast, secure, and available — wherever they are.

- Migrate appropriate data to the 'Cloud' using automated content inspection and redaction of data, meta-data and active content that breach defined policies for content passing across BIG-IP LTM into or out of the 'Cloud'

A Simplified SECURE Application Acceleration Architecture

- The combination of acceleration techniques, which reduces page-load times, and increased security with Adaptive Redaction will ensure that in times of stress and pressure, only authorized content will be loaded, removing the risk of, for example, financial results and hidden meta-data being posted to the production web server prior to official disclosure.

- Without the ability to cache objects for an extended time, you may open the door for a hacker to transfer invalid data from the server in order to compromise your web application. Adaptive Redaction will ensure that only active content and/or data that is acceptable going to or coming from the application is from an authorized source and is therefore permissible.

Application Vulnerabilities

- Heighten business and IT awareness of potential data exfiltration from databases, ERP, CRM, etc. used to populate responses to web enquiries, regardless of whether it is caused by a poorly implemented application, a vulnerability being exploited or inappropriate access to a system gained.

- Maintain application uptime due to the removal of targeted malware intent on damaging the web experience of users

Web Services Delivery

- Ensure sensitive data is always protected, even when the stress to deliver web services quickly can cause organizations to move services from development to production environments without following the appropriate security procedures. This creates a list of security problems, such as having components installed by default or data used for development available in the production environment.

- Ensure critical information is always protected, when vulnerabilities in services are uncovered related with deficient or inexistent application lifecycle management. This problem can get even bigger in organizations following a poorly implemented Continuous Delivery methodology.