# Contents

Foreword ....................................................................................................................................................................5  
Letter from the Co-Chairs...........................................................................................................................................6  
Acknowledgments ......................................................................................................................................................7  
1.0 Introduction ..........................................................................................................................................................8  
   1.1 Intended Audience ...........................................................................................................................................8  
   1.2 Scope ................................................................................................................................................................9  
2.0 Requirements Addressed ..................................................................................................................................10  
   2.1 Technical Evaluation and Assessment ...........................................................................................................10  
   2.2 Project Scope and Management ...................................................................................................................11  
   2.3 Existing Infrastructure ...................................................................................................................................11  
   2.4 Pilot and Deployment Phases........................................................................................................................11  
3.0 Implementation Considerations and Concerns .................................................................................................12  
   3.1 Considerations ...............................................................................................................................................12  
      3.1.1 Proxy Configuration ................................................................................................................................12  
      3.1.2 Capacity for Broad or Granular Policy Management ..............................................................................12  
   3.2 Concerns ........................................................................................................................................................13  
      3.2.1 Data Privacy ............................................................................................................................................13  
      3.2.2 Data Protection .......................................................................................................................................13  
      3.2.3 Regulation Compliance ...........................................................................................................................13  
4.0 Implementation .................................................................................................................................................14  
   4.1 Architecture Overview ...................................................................................................................................14  
      4.1.1 Direct Web Security as a Service ............................................................................................................15  
      4.1.2 Web Security as a Service through a Gateway .......................................................................................15  
      4.1.3 Web Security as a Service Using Agents .................................................................................................16  
      4.1.4 Web Security as a Service: A Combination Architecture ........................................................................16  
   4.2 Guidance and Implementation Steps ............................................................................................................17  
      4.2.1 Technical Evaluation and Assessment ....................................................................................................17  
      4.2.2 Security ...................................................................................................................................................17  
      4.2.3 Compliance .............................................................................................................................................19
4.2.4 Management/Administration.................................................................................................................. 20
5.0 References and Useful Links................................................................................................................... 22
   5.1 References.............................................................................................................................................. 22
   5.2 Useful Links......................................................................................................................................... 22
Foreword

Cloud Computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. We are reaching the point where computing functions as a utility, promising innovations yet unimagined. The major roadblock to full adoption of Cloud Computing has been concern regarding the security and privacy of information.

Much work has been done regarding the security of the cloud and data within it, but until now, there have been no best practices to follow when developing or assessing security services in an elastic cloud model—a model that scales as client requirements change.

One mission of the Cloud Security Alliance is to provide education on the uses of Cloud Computing to help secure all other forms of computing. To aid both cloud customers and cloud providers, the CSA SecaaS Working Group is providing Implementation Guidance for each category of Security as a Service, as delineated in the CSA’s SecaaS Defined Categories of Service. Security as a Service was added, as Domain 14, to version 3 of the CSA Guidance.

Cloud Security Alliance SecaaS Implementation Guidance documents are available at https://cloudsecurityalliance.org/research/working-groups/security-as-a-service/.

We encourage you to download and review all of our flagship research at http://www.cloudsecurityalliance.org.

Best regards,

Jerry Archer          Alan Boehme           Dave Cullinane
Nils Puhlmann         Paul Kurtz           Jim Reavis

The Cloud Security Alliance Board of Directors
Letter from the Co-Chairs

Security as a Service is a specialized area categorized two years ago as growing rapidly and in unbound patterns. Vendors were struggling. Consumers were struggling. Each offering had its own path. We felt it was urgent to address the needs and concerns common to the implementation of Security as a Service in its many forms.

The Defined Categories of Service helped clarify the functionalities expected from each Category. In this series, we hope to better define best practices in the design, development, assessment and implementation of today’s offerings.

We want to thank all of the many contributors worldwide who have worked so hard to produce these papers providing guidance for best practices in Cloud Computing Security. Many have been with the Security as a Service Working Group since the beginning; many others joined in this effort. Each has spent countless hours considering, clarifying, writing and/or editing these papers. We hope they help move forward toward those unimagined innovations.

Sincerely,

Kevin Fielder and Cameron Smith
SecaaS Working Group Co-Chairs
Acknowledgments

Co-Chairs
Aradhna Chetal, The Boeing Company
Kapil Raina, Zscaler

Contributors
Aaron Bryson, Foundstone
James Duff, Symantec

Peer Reviewers
Phil Cox, RightScale
Sandeep Mittal
Jean Pawluk
Jim Brigham, EMC/RSA
John Linn, EMC/RSA
Robert Polansky, EMC/RSA
Said Tabet, EMC/RSA

CSA Global Staff
Aaron Alva, Research Intern
Vicki Hahn, Technical Writer/Editor
Luciano JR Santos, Research Director
Kendall Scoboria, Graphic Designer
Evan Scoboria, Webmaster
John Yeoh, Research Analyst
1.0 Introduction

Business today has changed to become more mobile and user-centric, embracing trends such as BYOD and mobile devices. Users now are demanding specific capabilities and dictating to IT staff the platforms and applications they want to use. Location and device platform are no longer constant.

At the same time, cyber-attacks have become increasingly sophisticated and more targeted with threats from formidable opponents such as nation-state attackers. Attacks such as botnets and advanced persistent threats (APTs) have become harder to detect and stop, in part because they are increasingly focused on the weakest link – the user.

Furthermore, underlying these business trends and a morphing security threat landscape is a macroeconomic picture that demands higher productivity with fewer resources. Most CISO/CIOs have fewer budget dollars to allocate to security solutions than ever before.

To meet these requirements, the vendor and academic community have come together to form a set of solutions called Security as a Service. This document specifically addresses one element focused on Web Security as a Service (Web SecaaS).

Broadly defined, Web SecaaS provides cloud-based, dynamic services to protect end-users and end-user devices without requiring hardware or static approaches to security. Generally, characteristics of Web SecaaS models include (but are not limited to):

- Cloud or SaaS delivery model for the security and management of the service
- Minimal, if any, touch point on the server or user’s devices
- Platform independence i.e. support for mobile, desktop and laptop environments
- Mobility support to accommodate a user that will travel from location to location
- Capability of updates and security resolutions through a “backend” or cloud push without requiring any work or effort on the end-user’s part

1.1 Intended Audience

This introduction provides any senior technologist a broad overview of this document and problem space. Section 2 provides information for decision makers and evaluators for both technical and business/process segments. Some material may be suitable for CXO’s that would require a broad understanding of Web SecaaS project depth and scope. Section 3 offers insight, at some technical depth, into those considerations and concerns that should become part of the decision making discussion, whether by a technical design team or within the context of a purchasing decision. Section 4 offers the most technical depth of all the sections and provides guidance as to the proper implementation of Web Security as a Service. Section 5 provides general references and links to additional resources suitable for all audiences.
1.2 Scope

This document focuses on several key concepts:

- Web Security topics including:
  - Web 2.0/Social Media controls
  - Malware and Anti-Virus controls
  - Data Loss Prevention controls (over Web-based services like Gmail or Box.net)
  - XSS, JavaScript and other web specific attack controls
  - Web URL Filtering
- Policy control and administrative management
- Bandwidth management and quality of service (QoS) capability
- Monitoring of SSL enabled traffic

Given that this document is focused on SaaS models, on premise solutions such as appliance and other hardware-based approaches are not addressed in this document.

Additionally, while Web SecaaS must include additional elements and some of those points will be incorporated in this document, separate documents (under the Cloud Security Alliance SecaaS Defined Categories of Service framework) will detail in more depth the following controls:

- Identity and Access Management
- Data Loss Prevention
- Email Security
- Security Assessments
- Intrusion Management
- Security Information and Event Management (SEIM)
- Encryption
- Business Continuity and Disaster Recovery
- Network Security

Cross references to these other documents will help the reader of this Web SecaaS guide drill down further.
2.0 Requirements Addressed

A customer’s ability to manage Web Security depends largely on the following features and functions:

- **Administrative tools.** This includes integrated Active Directory and LDAP synchronization, fine-grained user authorization policy definitions, and the ability to adjust spam-scoring criteria manually if required.
- **Accessibility and integration.** The Security as a service solution should offer a Web-based management interface with single-console access to all of the Web, email, and content security services that an organization uses.
- **Reporting features.** Administrators should have access to the information they need to make accurate decisions and to evaluate the effectiveness of a Security as a service solution. The solution must include comprehensive reports on vulnerabilities including severity levels, time to fix estimates and impact on business, plus trend analysis on security issues. By continuously and proactively monitoring all network access points, such a service dramatically reduces security managers’ time researching, scanning and mitigating network exposures and enables companies to minimize the impact of network vulnerabilities before they can be exploited.
- **Ease of use.** End-users should have easy-to-use administrative features, such as security dashboards; policy controls; granular search capabilities, the ability to perform tasks appropriate to their organizational role and level of access, the ability to delegate administration and be able to capture audit trail of administrative actions.

With a Web Security as a Service solution, organizations can reduce significantly the total cost of ownership (TCO), as organizations can reduce costs by eliminating the distribution, deployment, and ongoing upgrade of on-premise hardware. In addition, no electricity or cooling is required. For service providers with a large number of regional access points, bandwidth costs can be lower than having to backhaul traffic back to a single, fixed data center. Labor costs are also reduced, because instead of paying for training, installation, management, and ongoing maintenance, the labor costs associated with a SaaS solution are focused on minimal staff training and administrative functions.

2.1 Technical Evaluation and Assessment

The overall technical aspects for consideration of a potential vendor of Web SecaaS fall into three key areas:

- **Security** – focuses on the protection of the user.
- **Compliance** – covers data loss prevention and focuses on protection of the organization’s data.
- **Optimized availability** – involves the control of the organization’s bandwidth (as a result of large data consuming Web 2.0 and streaming services) to ensure critical services always have network bandwidth.

In addition to ensuring complete technical coverage, it is critical that organizations understand how a vendor can respond to updates in the security landscape, as well as scale out to meet organizational needs. Updates could include security fixes, new models of security analysis, specific security controls or, potentially, updates in
the vendor’s own software stack. Scaling could encompass not just being able to handle more users, but also capacity the provider offers across all geographies.

2.2 Project Scope and Management

By definition, a SaaS model should be easier and faster to deploy than an on-premise option. However, to ensure success, several key elements must go into the formation of an appropriate project scope and project management plan, including:

- Selecting personnel to manage specific aspects of the service (e.g., Security, DLP, and Optimizations),
- Determining how standard policies are created and by which departments,
- Determining how exceptions are created, and
- Determining audit procedures.

2.3 Existing Infrastructure

In all likelihood, most organizations looking at a Web SecaaS will have some web security infrastructure or appliances on premise in operation. Planning the phase-in of a new Web SecaaS service and then eventual replacement has to be coordinated among several areas:

- Determining the rollout phase and planning so specific appliances can be removed from the critical path,
- Negotiating the end of licensing/contracts with appliance vendors,
- Ensuring the Web SecaaS provides overlapping licensing for a smooth migration to the cloud service while hardware remains on premise,
- Migration of policies from existing infrastructure to Web SecaaS provider,
- Reconfiguration of end user devices as required and end user education, and
- Ensuring the appropriate destruction of data of the on-premise solution before being sold or returned to vendor.

2.4 Pilot and Deployment Phases

As with any IT project, identifying success criteria and planning for success is critical. General deployment models include:

- Pilots based on geography (to make it easier for support initially),
- Pilots based on job function (to test out a particular set of use cases), and/or
- Pilots based on need/urgency (to get the most critical users protected immediately).

Equally as important as developing a pilot testing model, organizations need to have success criteria developed for their organizations. In general, terms these criteria would include:

- Testing viability over specific use cases (for example current weak points and measuring how the new SaaS vendor works), and/or
- Testing based on common IT / Industry standards.
3.0 Implementation Considerations and Concerns

3.1 Considerations

3.1.1 Proxy Configuration

The majority of Web SecaaS services today are based on proxy servers that reside in the cloud. If there is an existing proxy-based solution that resides within the corporate network, the migration to a SaaS-based solution will be relatively straightforward as much of the configuring of proxy settings on devices will have been done, and there were will an existing level of user knowledge of the process.

If proxy-based technologies are new within the environment then research and evaluation will need to be conducted as to the best way to configure the proxy settings on devices. For Windows centric environments, deploying and enforcing proxy settings on devices is a well-known and understood task. For Mac OS X, Linux or heterogeneous environments with a variety of platforms in use, companies may need to look at automatic proxy discovery processes. There are several mechanisms to enforce proxy use; the most direct is to block outbound port 80/443 (HTTP/HTTPS) traffic at the firewall for desktop segments.

With the move to a SaaS-based solution, companies will also need to remember to inform other service providers that they utilize that their external public IP address used for client web traffic will change to the public IP address of the SaaS service provider as all web traffic will now appear to originate from the SaaS provider.

One of the great benefits of the Web SecaaS service being provisioned from within the cloud is that it will be possible to utilize the Web SecaaS service from any location, not just from within the corporate network. This will mean that users on the road and at home can utilize the service. It is important to inform users that all traffic is potentially being monitored regardless of location. Notices should be included within acceptable usage policies to inform users that monitoring is extended to any location where the device is used. The implications for environments that utilize a BYOD policy need careful consideration.

With all web traffic now being transferred to an external entity, the Web SecaaS provider, companies should pay close attention to how payment card data and personally identifiable information (PII) could be observed and stored by the Web SecaaS provider. There could be significant privacy ramifications if PII data is stored in another country or the scope of a PCI assessment needs to be adjusted to include the Web SecaaS provider.

3.1.2 Capacity for Broad or Granular Policy Management

Given the dynamic nature of today’s global business environment, policy management must be flexible to accommodate a range of needs. Consider the following range of scenarios:

- **Mobility**: A user works in multiple offices, across different regions (road warrior)
- **Platform**: A user works on a tablet, then moves to his laptop
• **Cloud Apps**: A user accesses one cloud-based application, then goes to another

Tied to organizational roles, the above scenarios (and numerous other variations) must be accounted for and capable via the service provider policy management system.

### 3.2 Concerns

#### 3.2.1 Data Privacy

Given the mobility of users and the general volume of web traffic, it is critical for a SecaaS provider to have data center points of presence in as many geographical locations as possible. The more geographic coverage a vendor has, the more likely the end-user experience will be smoother (less time to a SaaS node for policy and security processing). Overall latency should be considered as a factor of the number of data centers available.

#### 3.2.2 Data Protection

Each SaaS vendor must establish both policy and technical capability to handle data privacy of traffic being monitored on behalf of a customer. Specifically, a SaaS vendor should provide data obfuscation. This ensures that data (such as web logs) are captured and then stored in an obfuscated manner. Thus, log storage and its movement from server to server over a cloud can be safe from bad actors, as its interception will have no meaning without the ability to de-obfuscate it. One common technique is to leverage tokenization as a method of data obfuscation. Tokenization in the web context could take web log information such as IP and URL and store them in an abstract manner. (The abstract token then is used in referencing the original content, which makes it more secure than storing the data in plain text.) Another common technique is to encrypt log traffic data.

#### 3.2.3 Regulation Compliance

In certain countries, specific regulations dictate data privacy including (in some cases) the fact that certain types of data (such as the web audit logs) cannot leave the borders of a country. In those cases, the SaaS provider must be able to keep a data center location that can store restricted data locally – including bringing all audit data back to the nodes in the geographically defined regions. However, the provider needs to be able to monitor and protect users even as they cross the border, but route the data and logging in the country as required.
4.0 Implementation

4.1 Architecture Overview

Web security provided as a service from a cloud platform may have many different architectures. There are, however, common components which are shared across various models.

The architecture stack has layered services, with the key component including web malware scanning, web (URL) filtering, instant messaging (peer-to-peer) controls, vulnerability intelligence (for zero hour detection), and central policy control. A global web security policy can be created and enforced across the organization, at the group or user level. Within the administration console component, reporting provides an overview data to review ongoing trends and forensic data. All of this is deployed in a cloud environment to provide Internet service architecture, which utilizes the scalability & elasticity of the cloud as well as ease of use through a web-based interface to the consumer organizations.

From the consumer organization’s perspective, Web SecaaS is seen as SaaS. However, companies providing these services can have a variety of different architectural models, including both SaaS and hybrid deployment models.

Service providers can host their services in a private cloud, which means the infrastructure comprising Security as a Service is fully owned and managed by the provider of the service. In this model, while the service itself may be a public, multi-tenant cloud SaaS offering, the underlying infrastructure is a private cloud.

Service providers can also deliver their services from a public cloud in which the infrastructure of the SecaaS platform relies upon a public cloud using an IaaS or PaaS. Some SecaaS service providers build their service and architecture from the ground up to be a cloud-based model (rather than an appliance hosted on behalf of customers).

Regardless of the delivery model, these architectures provide consumer organizations with Web Security capabilities without having to invest in additional hardware and appliances, and may reduce costs significantly.

The traffic types which can be supported include the traffic coming from branch offices, retail sites, or even home users through GRE, IPSEC or VPN traffic protocols. It can be routed through multiple proxies (proxy chaining), different desktop connectors and other explicit proxies/gateways.

The basic principle of deployment should be “easy and flexible” deployment for a Web Security as a service solution. It should be recognized that networks are all different; it is painful and expensive to modify an existing network topology to accommodate a security solution. A service should be designed to fit any deployment scenario for any size of an organization with different topologies. The easiest deployment option would be to simply point end users’ browsers to the cloud-based service, but other alternatives can be to have onsite appliances that are deeply integrated into enterprise directory services and software agents to filter laptops. Either way, management and monitoring should be provided through a simple cloud-based interface for all the deployment choices.
4.1.1 Direct Web Security as a Service

The simplest way to use Web SecaaS is to directly proxy Web traffic to the cloud-based content filtering and malware protection services. This can be done with browser proxy settings or by transparently forwarding traffic from any network firewall or proxy that supports forwarding to an upstream proxy.

4.1.2 Web Security as a Service through a Gateway

The Web Security Gateway can be deployed on-premises by consuming organizations, which will integrate with enterprise directory services for group-based policies, and the gateway can cache static Web content locally to save bandwidth. The gateway can be configured to forward traffic to the cloud-based Web filtering service. Gateway appliances are managed and configured through the cloud-based central management and reporting interface. There are a number of Gateways available as a hardware appliance or as a virtual appliance.
4.1.3 Web Security as a Service Using Agents

Securing remote, roaming users can be a challenge, and an approach that works for mobile clients are web security agents. These agents protect remote users by enforcing the routing of all Web traffic from the end-point through the cloud-based content filtering and malware protection service.

Agents are usually lightweight, tamper-proof clients available for various platforms like Windows, Mac OS, iOS, etc. While agents are not required (for example if a mobile using a corporate WiFi routes through a an office router, which in turn, uses GRE tunneling to forward all traffic, including the mobile device traffic to the SecaaS provider) they can enhance the functionality for some companies.

4.1.4 Web Security as a Service: A Combination Architecture

There is always flexibility to combine multiple deployment options to suit the specific need of each location. The cloud-based central administration interface should allow the administrator to specify a uniform Web usage policy and monitor Web access across all the user segments and deployment components.
4.2 Guidance and Implementation Steps

4.2.1 Technical Evaluation and Assessment

While there can be a range and varied set of requirements on an organization by organization level, there are some general sets of requirements for a Web SecaaS model. This section describes the most critical categories that a Web SecaaS provider should offer, including:

- Security,
- Compliance, and
- Management/Administration.

4.2.2 Security

Web SecaaS providers should offer, at a minimum, the capabilities described below in order to provide a baseline of reasonable security.

4.2.2.1 Web (URL) Filtering

URL Filtering is the broad capability of looking at a uniform resource locator (URL) and its content, and allowing or disallowing access based on defined policies or known threats.

The Web SecaaS provider should have:

- Known black list blocking with the ability to update without customer intervention. These lists are compiled by industry or vendor sources to prevent access to known bad locations.
- User configurable additions to system level black listing. Each organization may have specific destinations they may wish to block or allow.
- Categorization of websites to help classify types of content and destinations that may or may not be allowed (e.g., adult, gambling, social networking, etc.).
- Background updates (does not require user involvement) to ensure that, as new information is made available (vendor security updates, signature updates, heuristic algorithm updates, etc.), they will be reflected by the SaaS provider seamlessly and not require action on the user’s part.
- Comprehensive and accurate categorization. Previous generation technology filtering products created “catch-all” categories that were essentially uncategorized or unrated, making policy enforcement less useful. The ability to accurately identify web sites and place them into enforceable policy categories is important.
- User defined bypass of security services for specific URLs to ensure internal testing or other use cases can be accommodated.
- Ratings by domain name rather than URL/IP address alone where appropriate.
- Multi-language support (to cover non-English content/domains) to ensure global organizations can function and be protected adequately.
• The ability to look at embedded sites when performing dynamic categorization. Dynamic categorization does not rely on pre-determined user classification, but rather looks at the content as well as the destination. This helps detect sites that have copied legitimate content from another site but still push out malware.

### 4.2.2.2 Anti-Virus/Spyware Category Features

The Web SecaaS provider must provide protection, at a minimum, in the following areas:

<table>
<thead>
<tr>
<th>Anti-Virus</th>
<th>Anti-Spyware</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viruses</td>
<td>Dialers</td>
<td>Archive Bomb</td>
</tr>
<tr>
<td>Unwanted Applications</td>
<td>Backdoor Trojans</td>
<td>Exploits</td>
</tr>
<tr>
<td>Boot Sector Viruses</td>
<td>Adware</td>
<td>Malware Tools</td>
</tr>
<tr>
<td>Trojans</td>
<td>Backdoor Proxy</td>
<td></td>
</tr>
<tr>
<td>Worms</td>
<td>Password Stealer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Downloader</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other Spyware</td>
<td></td>
</tr>
</tbody>
</table>

In addition, the provider should be able to:

• Ensure that all antivirus offerings are capable of detecting and protecting against all known types of malicious or unauthorized software with antivirus signature updates at least every 12 hours.
• Support multiple malware scanning engines (for anti-virus signature-based approaches).
• Protect users independent of whether they have local software protection or not (cloud provider should not assume any local capability).
• Remove executables in attempted downloads that may be considered malicious.
• Detect spoofed file extensions (e.g., a PDF that is really an EXE).
• Block previously installed malware communication and prevent Command and Control functions (such as Botnet call homes).

### 4.2.2.3 Other

Additional threats and protections should include:

• Enforced patching levels of browser and related plug-ins (to user defined levels). This ensures the user does not have outdated software that could be open to vulnerabilities.
• Block or warn users of invalid SSL certificates (expired, untrusted roots, etc.).
• Blocking malicious, active content including:
  o Known malware sites (a blacklist model).
  o Vulnerable ActiveX controls (since ActiveX can execute commands on the local browser/computer, this can be a risk).
Browser exploitation attack vectors.
- File format vulnerability (e.g., an EXE disguised as a PDF).

- Fraud detection, including:
  - Known phishing sites (a blacklist model)
  - Suspected phishing sites (heuristic detection of fraudulent content). This can prevent the avoidance of relying on black lists only as the many fraudsters will create new URLs constantly to avoid black lists.
  - Suspected adware/spyware Sites (heuristic detection of pages copied from legitimate sites).
  - Web spam

- Restriction of unauthorized traffic, including:
  - IRC tunneling. IRC can provide a mechanism to channel botnet or malware traffic to the host or an attacker.
  - Anonymizer. Many anonymizers are created to bypass traditional proxy controls but can also hide malicious destinations (as in the case of a malware/Trojan talking to the command and control center).

- XSS Attack Protection, including:
  - Cookie stealing. Cookie stealing allows attackers to impersonate another user and possibly take over an existing session (in combination with other attacks).
  - Potentially malicious requests (e.g., XSS patterns in web requests).

- Blocking of suspicious destinations (user configurable)

- P2P controls, including:
  - File sharing
  - VOIP

- SSL traffic inspection:
  - For DLP policy enforcement
  - For detection of Botnet callback traffic

4.2.3 Compliance

Note that there is a separate document describing the Data Loss Prevention elements a Security as a Service provider should have. Some overlapping components are noted here as they pertain specifically to web transactions.

Web SecaaS providers should have the following specific security controls as it pertains to DLP for the Web domain:

- A DLP engine that can leverage updateable or user defined data dictionaries including credit card leakage, social security number leakage, financial statements leakage, medical information leakage, source code leakage, social insurance number leakage, salesforce.com data leakage, UK National Insurance number leakage, among others.

- Ensure literal text matching alone is not used (to reduce false positives). For example, to detect HIPAA violations, the fuzzy page would note the use of a Social Security Number in addition to a medical record term or diagnosis on the same page.
• Auditor notification for real-time alerts around compliance violations

4.2.3.1 Web 2.0 Control

Given the content aggregation (like links to photos, videos, etc.) and liability around Web 2.0 destinations and applications, it is critical that a Web SecaaS provider have Web 2.0 controls. At a minimum, a provider should have:

• The ability to control access to webmail services.
• The ability to allow or block attachments.
• Instant messaging access controls, including access to chat and file transfer capability.
• Social network/blog access for reading, posting, or both, with defined access to specific services.
• Streaming/media access controls, including:
  o Definition of access to which sites (by category or by specific site),
  o Bandwidth quota by application, user or group, and
  o Timeframe (of day) access is allowed.

4.2.4 Management/Administration

4.2.4.1 SaaS Administration Capability

To effectively manage a SaaS capability, administration needs to be accessible from multiple locations. Coupled with Role-Based Access Control, this forms the basis of an effective administration capability.

4.2.4.2 Real-Time Analytics and Query Capability

There are three important capabilities which must be part of the Web Security as a service solution:

• A scalable threat assessment infrastructure. The ability to recognize a zero-hour threat depends mainly upon a provider’s ability to collect, classify, and correlate large quantities of security intelligence data. This includes data gathered from current customers, automated Web scanning tools, honey pots and security researchers. Given very large statistical samples and advanced analysis tools, a provider can detect under-the-radar threats and deploy suitable countermeasures.
• A centralized, comprehensive management interface. A single interface will result in greater efficiencies, visibility, control, and management over combined Web, data, and email security technologies and will deliver unified content analysis and management. This should also allow custom queries/ad hoc reports for specific vulnerabilities or trends.

4.2.4.3 Monitor and Enforce Policy Modes

It is very important to be able to reliably predict the consequences of adding or modifying existing Web SecaaS policies. To facilitate the outcome of certain changes, a Web SecaaS provider should provide facilities whereby a customer can evaluate or test the policy changes they want to enforce. A Web SecaaS should have a combination of the following features:
• An option to enable a policy rule in monitor mode. In this mode, the rule would be evaluated as normal, however the outcome of the rule is only logged; the resulting block, quarantine or allow is not enforced and no rule specific action is taken on the traffic, and processing moves on to the next rule in the list or any other processing that is required. For example, if there is a rule that denies traffic where the SSL certificate is invalid in monitor mode and a user accesses a site with an expired certificate, then the traffic would be allowed to flow but the hit count on the rule would be incremented and an administrator would be able to review how the rule was evaluated.
• An option to mark a rule as enforced. In this mode, the rule is enforced as defined, and set responses are triggered.
• An option to simulate traffic flow. In this mode, an administrator can provide content and source and destination IP addresses/domain names, and the Web SecaaS software will simulate how the information would be processed and what the resulting actions taken would be.

4.2.4.4 Event and Alert Alarms and Configuration

The key to maintaining a high level of security and operational uptime is for systems to generate meaningful alerts that can be acted upon. To ensure proper operator responses to events and alarms:

• Alarms should be sent through multiple channels such as email, pager and SMS.
• Alarms can be escalated if they are not acknowledged in a set amount of time.
• Alarms can be throttled or suppressed to avoid a large influx of duplicate alarms that overwhelm operators and cause confusion.
• Alarms should have an option to mark rules as enforced. In this mode, the rule is enforced as defined, and set responses are triggered.
• Events and alarms should be correlated to identify root causes of security events.

4.2.4.5 Role-Based Access Control

Role-based access control (RBAC), with administrative controls for the SaaS management, is critical. Given that administrators will be distributed geographically and will have to service various roles, RBAC capability should be provided for policy management, reporting, auditing, and user administration.

4.2.4.6 Administrator Audit Trail

All good systems must keep an unalterable trail of administrator activities. This ensures that an outside auditor can audit, with confidence, changes in the system and attribute each modification or action to an individual.

4.2.4.7 SIEM Integration

In larger organizations that already have Security Information Event Management (SIEM) systems, the SecaaS provider should be able to provide a data feed or integration directly with the SIEM. This avoids creating silos of data which can lead to missing out on critical data patterns.
5.0 References and Useful Links

5.1 References


5.2 Useful Links


http://www.flexos.com/

https://www.barracudanetworks.com/

https://www.websense.com