IMPERVA®

IAAS Reference Architectures: For AWS

WHITE PAPER

1. Overview

This document provides guidance on architecting security for cloud-based web applications using the leading WAF solution[1] in the market today, Imperva SecureSphere, along with other Imperva security solutions for Amazon Web Services (AWS). Leveraging this document and the Imperva family of products, data center, IT and Operations Architects can now secure their web applications whether those are on-premise, in a virtual environment or in the most popular public cloud, AWS.

Validated reference architectures are presented which have been implemented at many customer sites. These "blueprints" and the associated use cases represent a small, but typical, subset of those in the AWS Cloud today.

Imperva solutions have been built to run natively in AWS, taking full advantage of AWS services such as Elastic Load Balancing, Availability Zones, CloudFormation and CloudWatch. So, the architectures and examples in this document serve as examples of how to get the most out of your investment in AWS.

2. What Is IaaS?

Simply put, Infrastructure as a Service (IaaS) offers traditional data center resources in a cloud-based environment, with a layer of automation, standardization and scalability that is effectively unattainable on-premise.

Enterprises of all sizes are moving applications to the cloud. From CRM to email to web application in banking, retail, e-retail, and government, organizations are migrating their web applications to the Cloud to save dollars and leverage all the other benefits the Cloud offers. These applications and the infrastructure that supports them, including—storage, load balancers, security and application servers, are adapting and evolving to address this trend.

In a recent CIO survey on cloud adoption published by PiperJaffray,[2] it was reported that 30% of all workloads will be run out of public clouds within five years, up from today's 9.7%.

The business drivers that influence organizations to consider migrating to the cloud are:

- **Cost Effectiveness**
  Cost is a key consideration, and organizations are constantly looking for ways to spend less, and get more. For IT organizations, in particular, infrastructure requirements are constantly on the rise with the need to support and enable the latest capabilities. By using high levels of automation, cloud deployment becomes cheaper, more accurate, and faster.
- **Scalability & Flexibility**
  Scale-up and scale-down infrastructure offerings are required for a business that sees varying or seasonal workload requirements. Dynamic scalability in the cloud helps organization better prepare for those periods of high demand.

[1] Gartner, Inc. has released the 2014 Magic Quadrant for Web Application Firewalls and named Imperva as the only vendor in the "Leader" quadrant.

[2] PiperJaffray Industry Note: "Enterprise Software, CIO Survey Pinpoints Public Cloud Trajectory, Impact to Legacy Infrastructure"; Oct 17, 2013

- **Always-On**
  Few, if any, organizations can compete with the capabilities of an IaaS platform in terms of availability and accessibility.
- **Lower Maintenance**
  By leveraging services offered in cloud deployments, organizations do not need to burden themselves with the task of ongoing servicing of their hardware and software updates. Besides the cost savings, this translates into fewer deployment errors and higher resource availability.
- **Simplicity**
  Transitioning the underlying infrastructure to the Cloud results in an environment that is much simpler to understand, design, deploy, and sustain.

Why AWS?

Gartner[3] estimated that the IaaS market size in 2014 was $13 billion, and growing fast. By 2018, it will be $42B (CAGR 35.6%). While there are many vendors offering IaaS today, AWS is the clear leader in this space and accounts for the majority of the business. Per Gartner, "AWS is the overwhelming market share leader, with 5x the Cloud IaaS compute capacity than the aggregate total of the [next] 14 vendors".

Imperva offers a comprehensive suite of products that secure applications, users and resources on AWS. By leveraging these technologies, you can move to the Cloud with the same level of availability and security as in the on-premise world.

The blueprints and use cases that follow below describe a set of validated reference architectures, which have been implemented at dozens of customer sites.

[3] Gartner's "Magic Quadrant for Cloud Infrastructure as a Service", 28 May 2014 ID: G00261698.

3. Blueprints

The IT architecture patterns discussed in this section describe an Imperva security layer in AWS, which has been tested and validated. We call these patterns "blueprints," and they represent the most common design approaches used by our customers. These blueprints include the technologies that underlie each type of cloud-computing implementation. Specific use cases for each of these will be discussed in Section 5.

3.1 Components

3.1.1 AWS

The following diagram represents a typical AWS environment, including just the components which are applicable to the Imperva offerings. Intentionally excluded are additional components (such as NAT devices, subnets, security groups, etc.), which are likely to be present, but not applicable to this document.

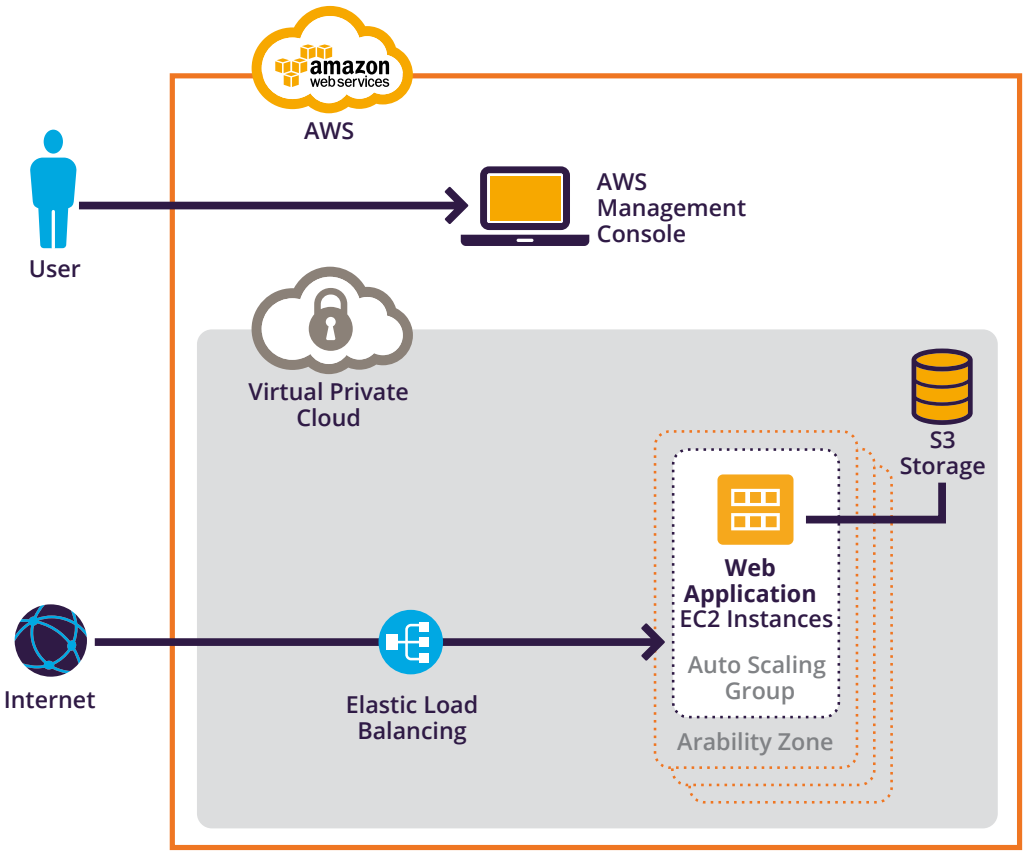

Diagram 1: Typical AWS Architecture, including those components which are applicable to the Imperva offerings

3.1.2 SecureSphere WAF for AWS

Diagram 2 illustrates a scenario whereby SecureSphere Web Application Firewall (WAF) for AWS is protecting data and applications in a data center in the AWS Cloud.

Benefits:

- **Block attacks, accurately**
  Stopping attacks on AWS applications is a high priority. But blocking legitimate user activity is not an option. The Imperva Dynamic Profiling technology automatically builds a profile, or "white list," of acceptable user behavior. Correlated Attack Validation correlates anomalous behavior, known as "profile violations," with other suspicious activity to correctly identify attacks, without blocking legitimate user activity.

- **Shut down malicious sources and bots**
  Distinguishing between real customers, known attackers, and bots is a complicated task. For example, cloaking identities is easily done using anonymous proxies. Imperva ThreatRadar Reputation Services detects these users with IP reputation feeds of malicious sources, anonymizing services, phishing URLs, and IP geolocation data. ThreatRadar delivers an upto- date and automated defense against automated attacks and attack sources, to help maximize uptime and protect sensitive data.

- **Stop application DDoS and business logic attacks**
  Business Logic Attacks are used to exploit the normal logic of applications, enabling attackers to post comment spam in forums and message boards; scrape web content; or disable access to websites. SecureSphere mitigates these concerns by identifying and shutting down communications from malicious bots and known attack sources. Additionally, by understanding the behavior of legitimate clients, attackers can be stopped in their tracks, based on their misbehavior.

- **Leverage world-class application security research**
  The Application Defense Center (ADC) research yields the most up-to-date threat intelligence and the most complete set of application signatures and policies in the industry. As a result, SecureSphere customers receive timely security content updates that includes signatures, reports, and policies, that often protect customers before exploits are publicly known.

- **Instantly patch website vulnerabilities**
  SecureSphere integrates with web application scanners to provide virtual patching capabilities. After importing the vulnerability scanner's results, SecureSphere can automatically create custom security policies to remediate the vulnerabilities that were found. Compared to manually fixing website vulnerabilities, virtual patching reduces the window of exposure and associated costs.

- **Gain forensic insight with customizable reports**
  Graphical reports provide the ability to analyze security threats and meet complex compliance reporting requirements. SecureSphere provides several pre-defined reports that meet the needs of many customers. Additionally, the reporting engine allows for creating fully customizable reports. All of the reports can be viewed on demand or emailed on a daily, weekly or monthly basis. Furthermore, a real-time dashboard provides a high-level view of system status, health, throughput and recent security events.

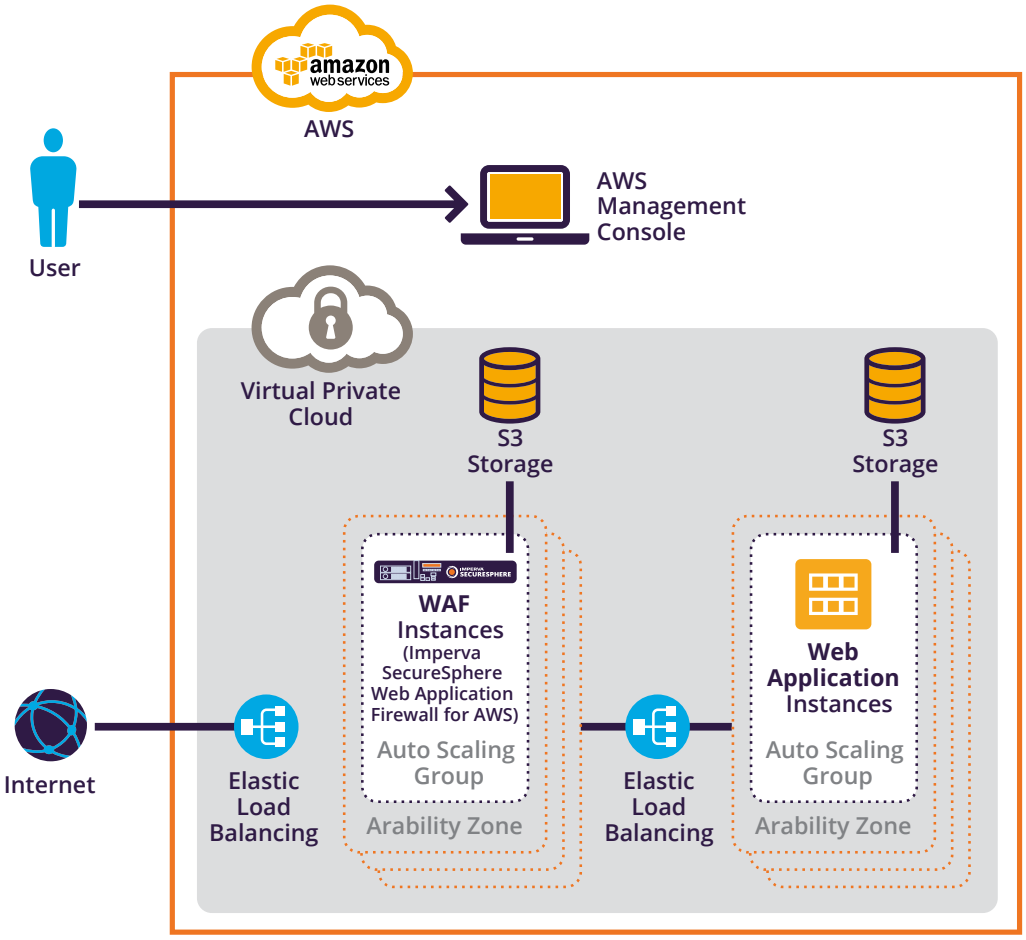

Diagram 2: An AWS data center deployment protected by Imperva SecureSphere Web Application Firewall

3.1.3 Imperva Incapsula Application Delivery Cloud

Incapsula provides an enterprise-grade, cloud-based Application Delivery Network for organizations hosting their applications on AWS. While Incapsula is offered as a standalone component for AWS, used in conjunction with SecureSphere WAF for AWS, it delivers a security solution which more efficiently deals with large scale DDoS attacks, and provides additional levels of security for bot protection, access control, two-factor authentication, backdoor, and malware protection. Imperva customers who purchase SecureSphere WAF for AWS as an annual BYOL subscription receive, as part of the package, Incapsula's "Business Plus" offering for the entire duration of the service, at no additional cost.

Incapsula complements AWS by providing advanced DDoS protection, utilizing traffic inspection and user profiling. These are offered alongside other advanced application acceleration capabilities which enable enterprises to maximize the performance and availability of their web applications. Incapsula supports Amazon's ELB and is fully compatible with Amazon's route 53 DNS. The Incapsula dynamic CDN offering also complements Amazon's Cloudfront Static CDN offering.

The Incapsula Application Delivery Cloud provides the following benefits:

- **DDoS Protection**
  Incapsula's large network capacity and dedicated 24x7 NOC protect websites from network and application level DDoS attacks at layer 3, 4, and 7, complementing AWS' inherent infrastructure capacity.
- **Application Acceleration**
  Built on a global content delivery network (CDN) of data centers, distributed worldwide, that boosts website performance and maximizes cacheable content.
- **Load Balancing & Failover**
  Supporting local multi-server load balancing, global traffic management with global server load balancing (GSLB) for site failover, geo load balancing, and real-time monitoring.
- **WAF-as-a-Service (WaaS)**
  For those customers who are interested in a WaaS product (as compared to the Imperva SecureSphere WAF, which is managed directly by the customer), the Incapsula solution features a PCI-certified Web Application Firewall, bot protection, two-factor authentication and granular access control. This offering can be used instead of the SecureSphere WAF, for those customers who are interested in a WAF service.

3.1.4 Imperva Skyfence Cloud Gateway

While AWS provides many of the essential building blocks for securing cloud workloads, customers have the ultimate responsibility for ensuring that both administrative actions and the Web management console infrastructure are monitored and protected. As Ed Ferrara of Forrester notes: "In the AWS world, security is a shared responsibility. AWS is not going to secure your applications or software infrastructure for you. AWS' responsibility stops at the abstraction point between its services and the applications you deploy. It's up to security and risk pros to engineer the correct security atop AWS. AWS provides key security building blocks, but it's still your responsibility?"

The Skyfence offering augments the native AWS audit capabilities by delivering real-time controls to protect administrative accounts, and enables alerting for high risk tasks or critical operations. Monitoring and enforcement includes preventing account takeover attacks (e.g. brute force, stolen credentials, man-in-the-middle); auditing user activity in real-time, and change control enforcement at the AWS Management Console, to protect against hackers and malicious insiders from getting direct access to sensitive data and resources.

Imperva customers who purchase SecureSphere WAF for AWS as an annual BYOL subscription receive, as part of the package, a Skyfence Cloud Gateway for AWS Management Console, for the term of their purchase at no additional cost. This will provide a customer the visibility, monitoring, and controls over activity that administrators and users are performing within the AWS management console.

Benefits of the Skyfence Cloud Gateway include:

- **Policy Enforcement**
  Blocking access or forcing multi-factor authentication in response to an account takeover, suspicious activity or high risk operations.
- **Profiling**
  Complete profiling of user/administrator behavior and their endpoint devices.
- **Monitoring**
  Centralized monitoring of administrator activity including screen views, data changes and configuration modifications performed via the AWS Management Console or through API calls.
- **Separation of Duties**
  Ensures administrators and IT security each have appropriate access and permissions according to their job function.

Skyfence for AWS integrates the basic capabilities of Amazon CloudTrail, adding real-time monitoring, profiling, and account protection features required for securing critical infrastructure in AWS environments. Together, Skyfence and CloudTrail enable secure access management, monitoring, and reporting of critical AWS Infrastructure.

3.2 Blueprints

The Imperva data center security solutions protect high value data and critical applications in AWS, as they do in the on-premise world. In addition, Imperva has gone to great lengths to leverage the additional functionality offered by AWS to enhance the offering for those customers who deploy their assets in the Cloud. Imperva is the only company that is able to offer these comprehensive data center security solutions and address the most common problem in migrating web applications to the Cloudinsufficient security. This is demonstrated below through two validated blueprints.

The following section will discuss these offerings:

- SecureSphere WAF for AWS + Skyfence Cloud Gateway + Incapsula Application Delivery Cloud
- Skyfence Cloud Gateway + Incapsula Application Delivery Cloud

3.2.1 Managed WAF, DDoS and CDN with Cloud Access Security

(SecureSphere WAF for AWS + Incapsula Application Delivery Cloud + Skyfence Cloud Gateway)

The combination of the following components are offered, all "under one roof":

- SecureSphere WAF for AWS
- Incapsula Application Delivery Cloud
- Skyfence Cloud Gateway

The grouping of these products provides an unprecedented layered security approach for web applications in the Cloud. This architecture provides comprehensive WAF capabilities alongside advanced DDoS protection to monitor and protect data assets, and is complemented by monitoring all privileged user access, via the AWS Management Console, to data residing in the Cloud.

Customers purchasing the SecureSphere WAF for AWS as an annual BYOL subscription will receive the Skyfence Cloud Gateway and Incapsula Application Delivery Cloud products as part of the package, at no additional cost for the term of the purchase.

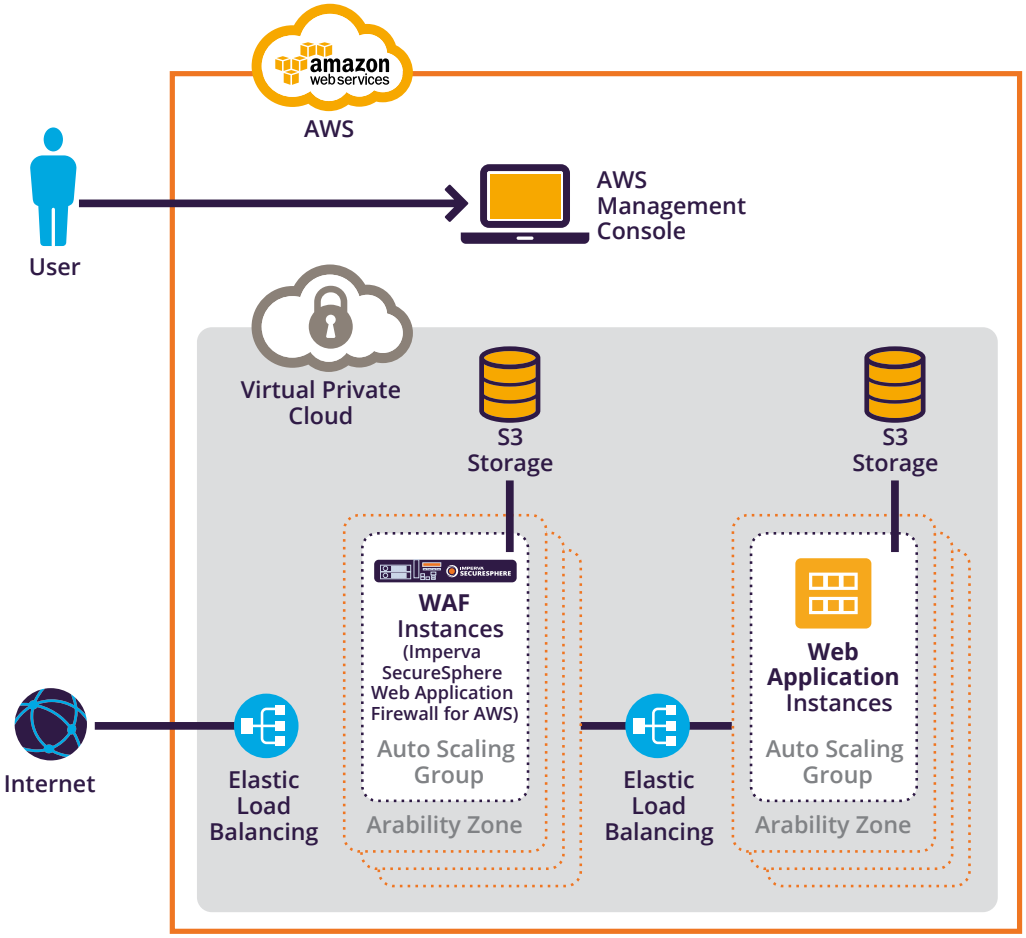

Diagram 3: An AWS data center deployment protected by Imperva SecureSphere & Incapsula Application Delivery Cloud & Skyfence Cloud Gateway

3.2.2 WAF-as-a-Service (WaaS) with Cloud Access Security

(Incapsula Application Delivery Cloud + Skyfence Cloud Gateway)

For those customers who are interested in a WaaS solution rather than a customer-managed WAF, the Incapsula solution features a PCI-certified Web Application Firewall, as a service. The DDoS and bot protection, along with two-factor authentication and granular access control, makes this solution attractive to those interested in minimal WAF management. In this architecture, WaaS is provided and complemented by Incapsula's advanced DDoS protection, CDN, and load balancing capabilities, while leveraging the Skyfence Cloud Gateway for the monitoring of all privileged user access via the AWS Management Console to data residing in the Cloud.

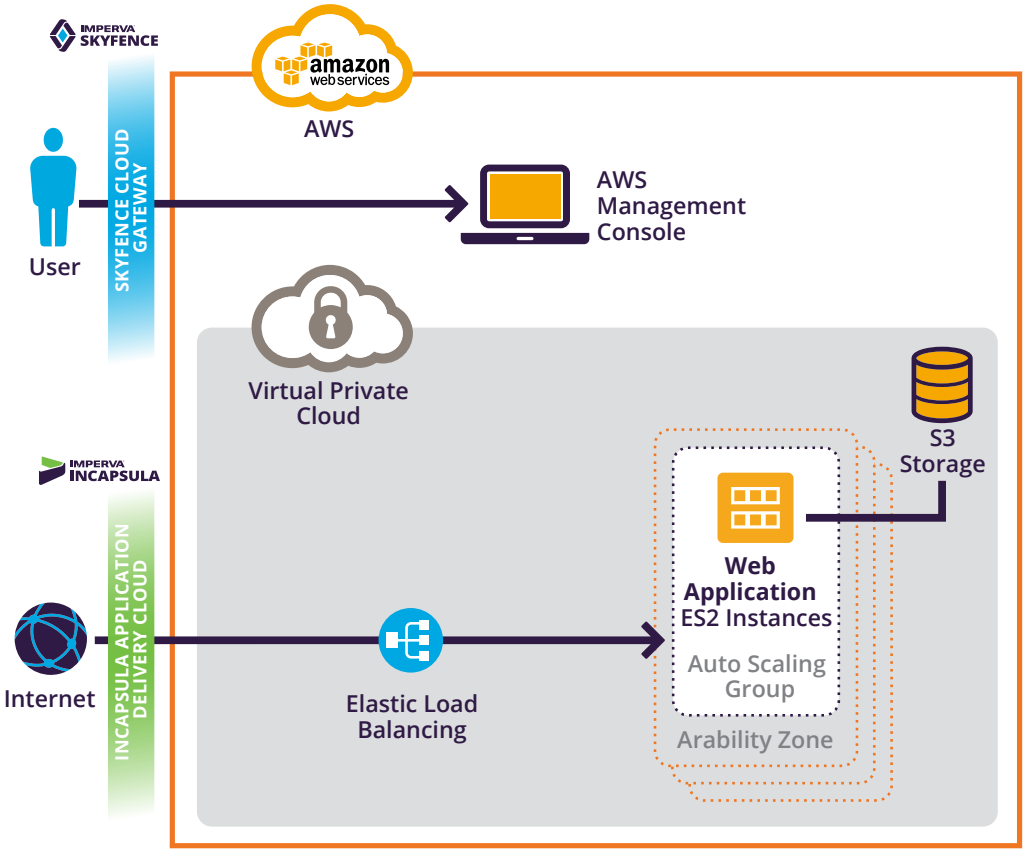

Diagram 4: An AWS data center deployment protected by Incapsula Application Delivery Cloud + Skyfence Cloud

4. The Imperva Solution: Leveraging All Things AWS

SecureSphere WAF for AWS leverages the capabilities of AWS, providing the same elasticity and ease-of-deployment that AWS customers have come to expect from the world's largest public cloud. SecureSphere WAF for AWS customers can take advantage of important AWS features like CloudFormation, Elastic Load Balancing, and CloudWatch.

- **CloudFormation (CF Templates)**
  Provide easy deployment, scaling, and elasticity of solutions into the AWS cloud. Customers can define network and elasticity parameters which provide the ability to use Scaling Groups in different Availability Zones.
- **Elastic Load Balancing (ELB)**
  ELBs balance the network traffic, detect unavailable instances, and routes around them, resulting in reduced downtime.
- **CloudWatch**
  CloudWatch Alarms are used to detect critical issues such as high CPU or bandwidth utilization, then automatically spawn new WAF instances; automatically register them with the SecureSphere Management Server; and synchronize the security settings.

IMPERVA OFFERINGS	SECURESPHERE WAF FOR AWS	SKYFENCE CLOUD GATEWAY	INCAPSULA APPLICATION DELIVERY CLOUD	PACKAGE I: WAF (SECURESPHERE, INCAPSULA, SKYFENCE)	PACKAGE II: WAAS (INCAPSULA, SKYFENCE)
Attack Mitigation via Managed WAF	●			●	
Profile	●	●		●	●
3rd Party Scanners Integration	●			●	
Identify Malicious Sources	●		●	●	●
3rd Party SIEM Integration	●		●	●	●
Bot Protection	●		●	●	●
DDoS Protection			●	●	●
CDN			●	●	●
Load Balancing & Failover			●	●	●
Attack Mitigation via WAF as a Service			●		●
Account Takeover Mitigation		●		●	●
Cloud Access & Audit		●		●	●

Diagram 5: Infrastructure-as-a-Service contain Imperva components SecureSphere, Skyfence, and Incapsula

5. Case Studies

While there are many use cases for the products and architectures described in this document, the following three are typical scenarios, and represent how many Imperva customers secure their AWS applications today.

5.1 Case Study 1: Hosted Ecommerce Application Protection

Digital Media and Gaming Company Protects Cloud-based Apps and Services on AWS with Imperva

In anticipation of a major product launch, an online gaming company decided to host its e-commerce applications on Amazon Web Services (AWS), rather than invest significant time and money upgrading physical data centers. Delivering services in the Cloud exposed the organization to web attacks, data theft, and fraud and without question, this required ironclad defenses. They quickly deployed SecureSphere WAF for AWS in time for the release, and immediately protected the company's applications from attacks. Designed exclusively for AWS, SecureSphere integrates with key AWS technologies, allowing the company to take advantage of all the benefits of cloud infrastructure.

Requirements

- Full protection from advanced cyber attacks, for high-value applications running on Amazon Web Services (AWS).
- The ability to distinguish attacks from unusual, but legitimate, behavior, by correlating web requests across security layers and over time.
- The ability to scale, as application traffic rises with seasonality.

Solution

SecureSphere WAF for AWS: Imperva's enterprise-class Web Application Firewall (WAF) designed to protect applications running in the world's largest public cloud.

Bottom Line

- The organization deployed SecureSphere WAF for AWS in three days—just in time for a major product launch—and protected the company's applications from attacks, immediately.
- SecureSphere WAF for AWS scaled automatically, with unanticipated levels of traffic.
- Imperva is the only vendor with an enterprise-grade WAF that scales elastically with the AWS web applications it protects.
- The organization replaced all other WAF technology across the organization, standardizing on Imperva.

5.2 Case Study 2: Cloud Trading Platform Infrastructure Protection

Social Investment Network Maximizes Availability of Its Online Trading Operations with Incapsula's Infrastructure Protection Service

In July 2014, the investment network's infrastructure experienced a massive network DDoS attack on a full C-class of IP addresses. The volume of traffic in this attack overpowered their defenses, and even caused serious connectivity issues with its ISP. As a result of the attack, the company's trading systems were completely down.

Requirements

- A solution that could be activated for an entire subnet
- Able to safeguard its services against both floods of web traffic and Direct-to-IP DDoS attacks
- An anti-DDoS solution that could be onboarded immediately

Solution

The Incapsula Infrastructure Protection Service, an on-demand security service that safeguards critical network infrastructure from volumetric and protocol-based DDoS attacks.

Bottom Line

- Blanket DDoS protection for multiple protocols and services
- On-demand protection for entire subnets using BGP announcements, allowing the customer's many origin IP addresses to quickly and easily mitigate attacks.
- Protection against Layer 7 application attacks using Incapsula's always on web application protection technology

5.3 Case Study 3: Administrator Activity Monitoring and Account Protection

Financial Services Company Protects AWS Management Console with Skyfence

IT Staff at this financial and funding organization required better monitoring over users managing Infrastructure-as-a-Service offerings including databases, storage and server instances primarily through Amazon Web Services. While the organization also required better visibility over use of file sharing services (e.g. Box) and CRM apps (Salesforce.com), the top priorities was securing accounts and monitoring AWS management activity. The organization had been using some of the native auditing (CloudTrail) and two factor authentication provided by AWS, but realized they needed more features, reporting, and scalability above and beyond what these native tools provided.

Requirements

- Ensure only authorized IT users are accessing Amazon Web Services Management Console for IT Operations
- Enforce multi-factor authentication on critical tasks such as start, terminate and reboot for any IT resource running in AWS
- Full reporting and auditing to meet compliance regulations

Solution

Skyfence for AWS solution monitors user activity and provides account takeover protection for all users of the AWS Management Console.

Bottom Line

- Enables workflow to provide alerts and controls over critical administrative tasks
- Centralizes visibility and control for all AWS administrator activity (Web console & API calls)
- Separates administrative duties and privileges for administrators and IT security/compliance
- Generates logs and reports for auditors to meet SOX and other regulations
- Enforces step up multi-factor authentication for any action or task
- Protects against account takeover and use of stolen credentials

6. Conclusion

Imperva security solutions are changing the cloud security landscape. With Imperva, you get the security you need to move web applications to the cloud, but without the inherent risk. The Imperva solutions for web application security, DDoS protection and safeguarding SaaS applications provide the peace of mind required to focus on business, and not on the security infrastructure to accommodate business. To take an AWS "test drive," learn more, or purchase Imperva solutions, please visit www.imperva.com.