Media Contact:
Janet Hohmann
415-975-2236
jhohmann@vocecomm.com

Imperva to Acquire Incapsula and Skyfence; Introduces SecureSphere WAF for Amazon Web Services

Combination creates industry-leading cloud security and compliance offerings while filling dangerous security gaps

REDWOOD SHORES, Calif., February 6, 2014 – Imperva, Inc. (NYSE: IMPV), pioneering the third pillar of enterprise security with a new layer of protection designed specifically for physical and virtual data centers, today announced the company has agreed to acquire cloud security gateway startup Skyfence and has an agreement in principle to acquire the remaining shares of cloud-based web application security company Incapsula. Imperva also announced today the release of SecureSphere Web Application Firewall (WAF) for Amazon Web Services (AWS). The combination of these extends Imperva's comprehensive data center security strategy across the cloud with solutions that are unmatched in the industry.

"Our acquisition strategy for Skyfence and Incapsula are very similar. We seeded Incapsula four years ago because we recognized that cloud delivery would change the web application security landscape," said Shlomo Kramer, CEO of Imperva. "In the case of Skyfence, we believe that Software as a Service (SaaS) delivery models for internally facing corporate applications will substantially change the landscape for data center security and compliance. We are investing in this space early to put us in the best position possible to help new and existing customers."

Gartner predicts global spending on public cloud services will grow from $155B in 2014 to $210B in 2016[1]. As cloud adoption accelerates, enterprises are prioritizing how to integrate and migrate existing systems, from Enterprise Resource Planning (ERP) to Customer Relationship Management (CRM) systems, to cloud-based platforms. Cloud services often run critical applications and store business-critical data, but the majority of

existing security controls do not cover the range of different cloud deployments because they were designed for on-premise applications.

“For some time now, we’ve seen our customers take advantage of cloud-based services to reduce costs and increase flexibility. However, moving applications and data off-premise causes new and very significant risk exposure for organizations,” said Mark Kraynak, Senior Vice President, Worldwide Marketing, Imperva. “The strategy we are unveiling today comprehensively addresses the dangerous security gaps raised by the move to the cloud.”

Imperva’s strategy covers security gaps with multiple cloud deployment models. For internally facing corporate applications, the move to the cloud obviates traditional on-premise activity monitoring and security solutions. To fill this gap, Skyfence delivers a cloud gateway that provides a comprehensive security and compliance stack. For externally facing production applications, the cloud is changing deployment in two ways. Some customers prefer a SaaS model for WAF delivery. Incapsula directly meets that need with an application-aware global CDN platform that provides best-of-breed security, DDoS protection, load balancing, and failover solutions. Other customers prefer an Infrastructure as a Service (IaaS) model by which they can leverage the economies of scale of their cloud provider to realize significant cost savings. For these customers, SecureSphere for AWS allows them to move their applications without sacrificing security.

Imperva Skyfence

The first component of Imperva’s strategy is the agreement to acquire Skyfence. Skyfence protects the internal corporate applications, like employee- and back office-oriented applications that are moving to SaaS delivery models. Despite being internal, these applications allow access from the internet, which exposes them to the vulnerabilities intrinsic to public facing applications. This also creates security challenges and regulatory and compliance challenges as it moves responsibility for housing the data to a third party.

Skyfence has developed a solution providing real time visibility and control over corporate use of SaaS applications, which enforces security policy, protects sensitive

data from external and inside threats, and ensures compliance with standards. Skyfence uses proprietary network traffic analysis and Dynamic User Fingerprinting technology to profile normal user behavior and detect anomalies that could indicate cyber-attacks or inside threats. Through a single, central gateway, the solution provides organizations with the power to discover all of the cloud assets that are in use and to uniformly enforce security and compliance policies in addition to controlling user access to sensitive data, privileged user activity and API access to the service.

There are three main customer challenges driving the need for Skyfence:

- Managing Compliance in the Cloud – Skyfence generates an audit trail of all user access ranging from login events to a full activity log and enables enforcement of the necessary separation of duties between the SaaS administrator and IT security. Administrators can generate activity reports for both internal and external compliance audits and exposure reports for forensic analysis.
- Controlling "Shadow IT" – Skyfence will automatically detect cloud applications that are used without corporate approval and provides risk scores and usage metrics.
- Cyber Intrusion Prevention – The weakest link in many cloud applications' security is the abuse of legitimate user accounts. Skyfence identifies and protects against account-centric attacks including account takeovers, man-in-the-middle attacks, DNS poisoning, and brute force attacks.

Imperva Incapsula

The second component of this strategy is our agreement in principle to purchase of the remaining stake in Incapsula to deliver security for external facing production applications like online banking, online gaming, and retail applications. Through an application-aware global Cloud Delivery Network (CDN) platform, Incapsula provides websites and web applications with best-of-breed security, DDoS protection, load balancing, and failover solutions, available as standalone services or as an integrated solution.

- Incapsula's enterprise-grade PCI-certified WAF protects customers' websites or applications so that they are secure and available. Based on Imperva's industry-leading technology and experience and using a SaaS approach, Incapsula's

security experts protect customers against new and emerging threats.

- Incapsula DDoS applies mitigation outside of a customer's network, meaning that only filtered traffic reaches the host. Incapsula maintains an extensive DDoS threat knowledgebase, which includes new and emerging attack methods. This constantly-updated information is aggregated across the entire network, identifying new threats as they emerge, detecting known malicious users, and applying remedies in real-time across all Incapsula-protected websites.
- Incapsula's CDN is a powerful network of data centers located around the world that delivers full site acceleration. On average, websites using Incapsula's CDN are 50% faster and consume 40%-70% less bandwidth.
- Incapsula's Layer 7 Load Balancing and Failover balances traffic across multiple web servers directly from the cloud. This allows websites and applications to scale beyond the capacity of a single web server without requiring a local load balancing appliance or virtual appliance.

Over four years ago, Imperva anticipated that the WAF market would be ready to take advantage of cloud delivery models, so the Imperva team invested in Incapsula as a majority owned subsidiary. Imperva intends to bring Incapsula fully in house to allow for scale as the demand for Incapsula technology grows.

Imperva SecureSphere WAF for AWS

The third component of this strategy is Imperva's new SecureSphere Web Application Firewall version for Amazon Web Services. Similar to Incapsula, this product is primarily for externally facing production applications, but for customers that want to take their on-premise solution to the cloud or that prefer a "do it yourself" model for application security. Enterprise customers are making a strong push to move their customer facing applications to Amazon Web Services so that they can realize significant infrastructure savings by managing load peaks with temporary Amazon capacity. With SecureSphere for AWS, customers can replicate their existing on-premise security controls as they migrate to the cloud.

SecureSphere WAF for AWS was designed to natively take advantage of Amazon Web Services infrastructure. Leveraging Amazon Cloud Formation, WAF instances are created and moved along with the applications they protect, including across Availability

Zones, allowing for fast deployment of large enterprise-scale environments with minimal operational overhead. Instances of SecureSphere are created or removed from the deployment following Amazon's auto-scaling policies. These abstractions can dramatically improve the efficiency of IT and security operations teams.

SecureSphere for AWS has been in limited availability since late 2013 and will be generally available in March 2014.

Imperva expects the acquisitions of Skyfence and Incapsula to close in the first quarter of 2014.

About Imperva
Imperva, pioneering the third pillar of enterprise security, fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centers. With an integrated security platform built specifically for modern threats, Imperva data center security provides the visibility and control needed to neutralize attack, theft, and fraud from inside and outside the organization, mitigate risk, and streamline compliance. Over 3,000 customers in more than 75 countries rely on our SecureSphere® platform to safeguard their business. Imperva is headquartered in Redwood Shores, California. Learn more: www.imperva.com, our blog, on Twitter.

Forward Looking Statements
This news release contains forward-looking statements, including those regarding our belief that the combination of our SecureSphere for AWS, Skyfence and Incapsula will enable us to offer a comprehensive solution that addresses the dangerous security gaps raised by the move to the cloud; the anticipated benefits to Imperva of the contemplated acquisitions of Skyfence and Incapsula; the expected timing of the completion of the transaction; and the ability to complete the transaction considering the various closing conditions. These forward-looking statements are subject to material risks and uncertainties that could cause actual results to differ materially from those in the forward-looking statements. Investors should consider important risk factors, which include: the risk that Imperva will be unable to successfully integrate Skyfence and Incapsula, the risk that Imperva will have difficulty retaining key employees of Skyfence and Incapsula; the risk that our development expenses are greater than we anticipate; and other risks detailed under the caption "Risk Factors" in the company's Quarterly Report on Form 10-Q filed with the SEC on November 12, 2013 and the company's other SEC filings. You can obtain copies of the company's SEC filings on the SEC's website at www.sec.gov.

###

[1] Ed Anderson, Lai-ling Lam, Chad Eschinger, Susan Cournoyer, Joanne M. Correia, Laurie F. Wurster, Ruggero Contu, Fabrizio Biscotti, Venecia K Liu, Tom Eid, Chris Pang, Hai Hong Swinehart, Morgan Yeates, Gregor Petri, Warren Bell
Gartner Report, “Forecast Overview: Public Cloud Services, Worldwide, 2011-2016, 4Q12” February 8, 2013