SafeNet Ushers in New Era of Elastic Encryption by Announcing World's First Crypto Hypervisor

Multi-tenant, High-Assurance Key Vaulting for Cloud Migration

- SafeNet announces the Crypto Hypervisor, believed to be the first solution that delivers high-assurance key vaulting and encryption services on demand in a cloud operational model.
- Total cost of ownership can be significantly lowered by deploying up to 95 percent less hardware and streamlining crypto administration.
- Centralized control is now possible through unified administration of elastic crypto services complemented by role-based, tamper-proof logs for simplified compliance.

HONG KONG – April 24, 2013 – At a time when confidence in perimeter security is waning, and organizations are increasingly facing business pressure to adopt cloud strategies and consolidate their data center resources, the question of how to securely migrate data to public, private, or hybrid cloud environments has become a primary concern. As part of its Secure Breach strategy, SafeNet today announced limited availability of the SafeNet Crypto Hypervisor, enabling organizations to virtualize their crypto resources in an efficient and scalable way, and ensuring that all data can be safely encrypted, even as it moves in a virtualized environment, in order to prevent data loss.

With the SafeNet Crypto Hypervisor, IT departments and service providers can deliver on-demand, elastic key vaulting and encryption services for data protection across physical, virtual, and cloud environments in minutes instead of days. The solution's high assurance encryption services fit the cloud operations model and the full cost and innovation advantages of virtualization can be exploited without compromising security or compliance. IT maintains full, centralized control of the delivery of encryption services such as secure key storage. Users have full control of their encryption service, and can be assured that other tenants and administrators cannot access their encryption keys.

"Although encryption is becoming more common, data is only as safe as the keys protecting it," said Christian A. Christiansen, Program Vice President of Security Products & Services with IDC. "Storing the keys in special-purpose hardware, such as a hardware security module, is the recommended best practice. However, until now, hardware encryption solutions have not provided sufficient agility and flexibility needed in virtualized and cloud environments. Rolling out a virtual application that requires encryption, signed digital certificates, or other PKI functions can often add days or weeks to a project."

SafeNet's Crypto Hypervisor solves these issues by extending and virtualizing the market-leading SafeNet Luna SA 5 Hardware Security Module (HSM) to fit into the operational models of virtual and cloud environments. The Crypto Hypervisor can be centrally controlled and configured by crypto administrators using the new SafeNet Crypto Command Center. The administrators can build a catalog of services available on the Crypto Hypervisor. Users can now log in to a web portal to view a catalog of services that they have permission to create. These users can provision the services they need on demand on shared physical hardware. This process can reduce new service rollout from days down to minutes.

SafeNet's Crypto Hypervisor provides customers with the following benefits:

- **Cloud-compatible crypto**: Built for the cloud operational model, the Crypto Hypervisor enables organizations to consolidate crypto efforts, eliminate 'islands of encryption', and create a more secure and efficient operation. Organizations can use as little as five percent of the hardware they use today for the same amount of encryption services.

- **Lower total cost**: For the first time, a catalog of encryption services can be defined by the centralized administration team. Now, different users in different organizations can order these high-assurance key vault services on demand from this online catalog. New services that used to take days or even weeks to deliver can now be enabled within minutes, and without the intervention of a centralized IT organization.

- **Central control**: The Crypto Command Center can manage hundreds of independent virtualized HSMs. Strong audit controls with tamper-evident, digitally-signed logs are maintained for all functions. This centralized control and logging allows customers to build a center of excellence around encryption and simplify the audit process.

- **The most secure key vault available**: The Crypto Hypervisor technology virtualizes the field-proven and trusted SafeNet Luna HSMs, which currently provide protection for over $1 trillion in daily financial transactions; offer five nines of availability; and are trusted by enterprises and governments around the world.

SafeNet Executive Commentary

"The move to virtualization and cloud has revolutionized the way we store and protect data. This necessitates a similar revolution in the way in which crypto resources are shared and managed. Prior to the introduction of Crypto Hypervisor, it was a very manual and slow process for IT departments to deliver encryption services in the cloud, which slowed cloud adoption. Now, starting an encryption service is equivalent to a simple process like spinning up a new VM."

Tsion Gonen, Chief Strategy Officer, SafeNet, Inc.

Customer Executive Commentary

"Landis+Gyr is the global industry leader in smart grid energy management solutions for electricity, gas, and water utilities. Our customers set very high expectations of security and privacy protections on our metering solutions. PKI-based architectures are the best way we have found to secure the meters, prove integrity of the reported data, and protect customer privacy. SafeNet technologies have been critical in assuring that we continue to meet our customers' requirements. We appreciate their continuous innovation because it gives us confidence that SafeNet will continue to be able to help us solve our customers' most challenging security and privacy concerns."

— *Tim Weidenbach, Vice President of Product Management*
Landis+Gyr

"Xceedium relies on SafeNet's capabilities to deliver high assurance versions of Xsuite, the company's privileged identity management platform. SafeNet's Crypto Hypervisor has the potential to be a game-changer in the way we employ crypto resources. Xsuite protects very large hybrid-cloud enterprises and the Crypto Hypervisor design is right in line with Xsuite's architecture and our customer scalability, cost and security requirements."

— *Mordecai Rosen, Executive Vice President Business Development*
Xceedium

SafeNet's Crypto Hypervisor runs on SafeNet Luna SA 5 HSM hardware, which is currently available. The Crypto Command Center bundle is orderable now for future delivery. Luna 5.2 HSM software and Crypto Command Center are available now on a limited basis for select customers. Visit www.safenet-inc.com/CHV to learn more. SafeNet will be demonstrating the new Crypto Hypervisor this week at Infosecurity Europe at stand #F85.

Supporting Resources:

- Crypto Hypervisor: http://www.safenet-inc.com/cloud/hsm/crypto-hypervisor/
- Crypto Hypervisor Blog: http://bit.ly/138HtSv
- Secure Breach Microsite: http://www.securethebreach.com
- Follow SafeNet on Twitter, Facebook, YouTube and LinkedIn

About SafeNet

Founded in 1983, SafeNet, Inc. is one of the largest information security companies in the world, and is trusted to protect the most sensitive data for market-leading organizations around the globe. SafeNet's data-centric approach focuses on the protection of high-value information throughout its lifecycle, from the data center to the cloud. More than 25,000 customers across commercial enterprises and government agencies trust SafeNet to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments.