

THALES E-SECURITY CLOUD PARTNER PROGRAM

The Thales e-Security Cloud Partner Program enables service providers to deliver best-in-class data-centric security services to end customers. The program is available for infrastructure-, platform-, and software-as-a-service providers, as well as managed service providers (MSPs), managed security service providers (MSSPs), cloud service providers (CSPs) and hosting service providers (HSPs).

Enterprise executives considering cloud service offerings have security and compliance as top-of-mind concerns. Addressing these concerns enable service providers to command premium pricing, attract larger addressable markets, and gain higher service adoption rates. But service providers must address the following requirements:

- Prevent exposure to data breaches.** Organizations that manage personally identifiable information (PII) must establish strong controls and guard against data breaches to mitigate the risk of brand damage and lost business. Solutions are needed to avoid the costly data breach notifications required by regional data privacy laws, including but certainly not limited to, US state laws and the newly adopted EU General Data Protection Regulation (GDPR).
- Safeguard intellectual property.** Many organizations face increasing government- or organized crime-sponsored attacks on intellectual property. Organizations must increase efforts to secure intellectual property (IP) from advanced attacks as well as malicious insiders, partners, and contractors.
- Control privileged users access.** Cloud customers want control over who can access their data and who can't. Preventing insiders, including cloud, root, network, and system administrators, and even unauthorized programs from accessing restricted data is critical in enabling service providers to establish customer trust and confidence.
- Meet compliance requirements.** Addressing compliance mandates such as the Payment Card Industry Data Security Standard (PCI DSS) or the Health Insurance

Portability and Accountability Act (HIPAA) requires demonstrable controls for sensitive data, including privileged user access controls and data-at-rest encryption.

- Offer customer key management.** End customers want to have the flexibility to manage their own encryption keys, so they retain control over who can decrypt the data, no matter where it is stored or copied.

The Vormetric Data Security Platform enables service providers to address these requirements, without re-architecting storage or recoding applications, making it easy to deploy. The platform supports a broad range of operating systems, including Windows, Linux, and UNIX, as well as databases and big data environments to meet customers' diverse requirements. The architecture is multi-tenant ready, allowing you to meet your deployment and administration requirements and effectively support and service your customers. The Vormetric Data Security Manager (DSM) controls data access policies and keys for all Data Security Platform encryption offerings. It can be deployed either on your customers' premises or in your cloud. With form factors to meet your operational and security requirements, the physical DSM appliance meets up to FIPS 140-2 Level 3 for key management, while the virtual DSM appliance is FIPS 140-3 Level 1.

PROGRAM FEATURES AND BENEFITS

Thales delivers technical, marketing, sales, and support resources to Thales e-Security Cloud Partner Program members. We help partners design, promote, and extend their value-added security services to fuel increased cloud workload adoption and generate incremental recurring revenue opportunities. Thales will promote program members to customers worldwide, enabling partners to reach new prospects and expand their customer bases.

Program Features	Benefit
Flexible Usage-based Licensing and Pricing	Aligns pricing and license consumption with service provider delivery models.
Quarterly Business Reviews	Ensures the partner and Thales are aligned to meet mutual business objectives.
Thales Sales Champion	Manages sales, pricing, and purchasing and takes responsibility for the overall success of the business relationship.
Thales Technical Champion	Acts as a technical sales advocate to assist with product, training and support needs.
Thales Marketing Champion	Supports joint go-to-market, sales enablement, and solution selling. Assists with customer testimonials and communication activities to generate new business.
Cloud Partner Training	Provides access to training and professional services at partner rates.

Program Requirements	Description
Service Provider Licensing Agreement (SPLA)	Establish an annual Thales Cloud Partner pricing and purchase agreement.
Certified Technical Staff	Have at least two engineers certified in Vormetric Data Security Platform products.
On-site Demo/Lab Environment	Have at least one Vormetric Data Security Manager (physical or virtual) deployed to support technical readiness activities and end customer demo/proof of concepts.
Cloud Partner Sales Contact	Assign a designated sales contact to coordinate sales activities with Thales.
Cloud Partner Marketing Contact	Assign a designated marketing contact to coordinate go-to-market and sales enablement activities with Thales.

CLOUD DEPLOYMENT MODELS FOR SERVICE PROVIDERS

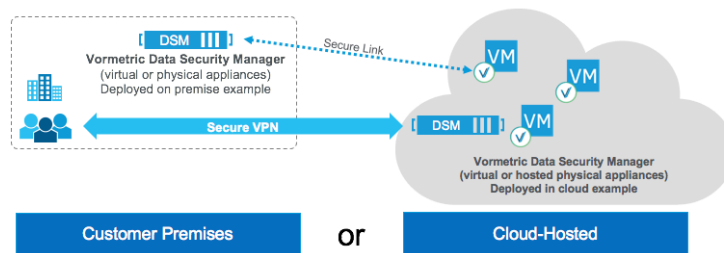


Image 1. IaaS, Cloud Hosting and Managed Service Providers

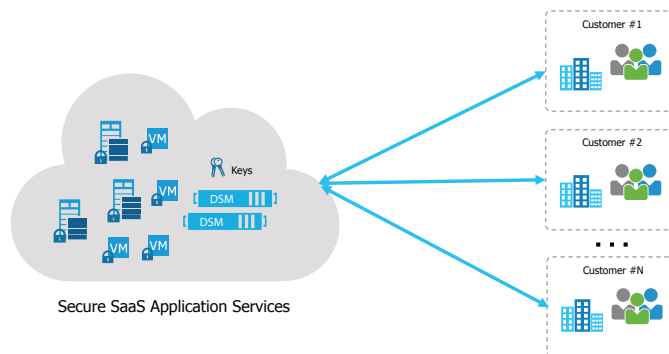


Image 2. Software-as-a-Service Providers

FOR MORE PROGRAM INFORMATION CONTACT:

C.J. Radford
 Vice President, Cloud.
cradford@thalessec.net
www.vormetric.com/cloudpartners

