PATHFINDER REPORT

451 Research® | Advisory

Key Management as a Service

A Concept for Modern Encrypted Data Requirements

FEBRUARY 2018

COMMISSIONED BY

EQUINIX

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About 451 Research

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

© 2018 451 Research, LLC and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication, in whole or in part, in any form without prior written permission is forbidden. The terms of use regarding distribution, both internally and externally, shall be governed by the terms laid out in your Service Agreement with 451 Research and/or its Affiliates. The information contained herein has been obtained from sources believed to be reliable. 451 Research disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although 451 Research may discuss legal issues related to the information technology business, 451 Research does not provide legal advice or services and their research should not be construed or used as such.

451 Research shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

NEW YORK
1411 Broadway
New York NY 10018
+1 212 505 3030

SAN FRANCISCO
140 Geary Street
San Francisco, CA 94108
+1 415 989 1555

LONDON
Paxton House
(Ground floor)
30, Artillery Lane
London, E1 7LS, UK
P +44 (0) 207 426 1050

BOSTON
75-101 Federal Street
5th Floor
Boston, MA 02110
Phone: +1 617.598.7200
Fax: +1 617.357.7495

EXECUTIVE SUMMARY

> "WE'RE SAYING ANYTHING DEVELOPED NEW IS BEING DONE IN THE CLOUD … WE WANT TO GET EVERYTHING WE HAVE OUT INTO THE CLOUD AS QUICKLY AS POSSIBLE."
>
> VOICE OF THE ENTERPRISE, BUDGETS AND OUTLOOK CLOUD TRANSFORMATION, Q4, 2016

We hear this every day. Your business, like those of your colleagues or competitors across the street, already has applications and data in the cloud. The challenge now is to chart a course that best transforms your business to optimize the use of sensitive data in private, public and colocated clouds. The central element of your cloud transformation strategy is the way you manage your encryption keys to secure sensitive data, satisfy compliance mandates and maximize performance.

We all know that leveraging cloud services can enhance the customer experience via improved performance, increase business agility by dynamically shifting workloads when required, and reduce capital expenses associated with purchasing perpetual-licensed products. Leveraging cloud services for applications and data has become so important to your business that it is strategically necessary to use multiple services such as Amazon Web Services, Microsoft Azure, Google Cloud Platform, Rackspace and IBM SoftLayer in much the way you route traffic through multiple internet service providers for redundancy.

Security concerns dominate conversations when it comes to managing corporate data. We know that storing encryption keys with the data violates accepted security fundamentals, but we also know that keys need to be near the data to provide high performance. There also may be privacy considerations when data crosses international borders that necessitate managing encryption keys for sensitive and regulated data whether the data is stored on-premises or in the cloud. The need to support utilization of keys across multiple services while retaining control and accountability is an essential business and compliance requirement. In fact, these themes will resonate throughout this Pathfinder report on the trend for treating key management as a service:

1. **Simplify complexity as data moves across cloud providers and on-premises datacenters.** Securely managing encryption keys requires special expertise – it makes perfect sense that security and technology teams would treat this as a service.
2. **Meet compliance and audit mandates no matter where your IT infrastructure appears.** Encryption is a basic tenet of every government, industry and enterprise security standard because it is imperative to avoid having regulated data fall into the wrong hands in usable forms. Key management as a service efficiently allows you to meet compliance audit requirements as you evolve your infrastructure.
3. **Retain complete control of keys at all times.** Key management architectures need to ensure that your keys never become vulnerable to theft or reuse. In fact, since the leading key management services never have access to key materials, security is actually enhanced so you can focus on your business.

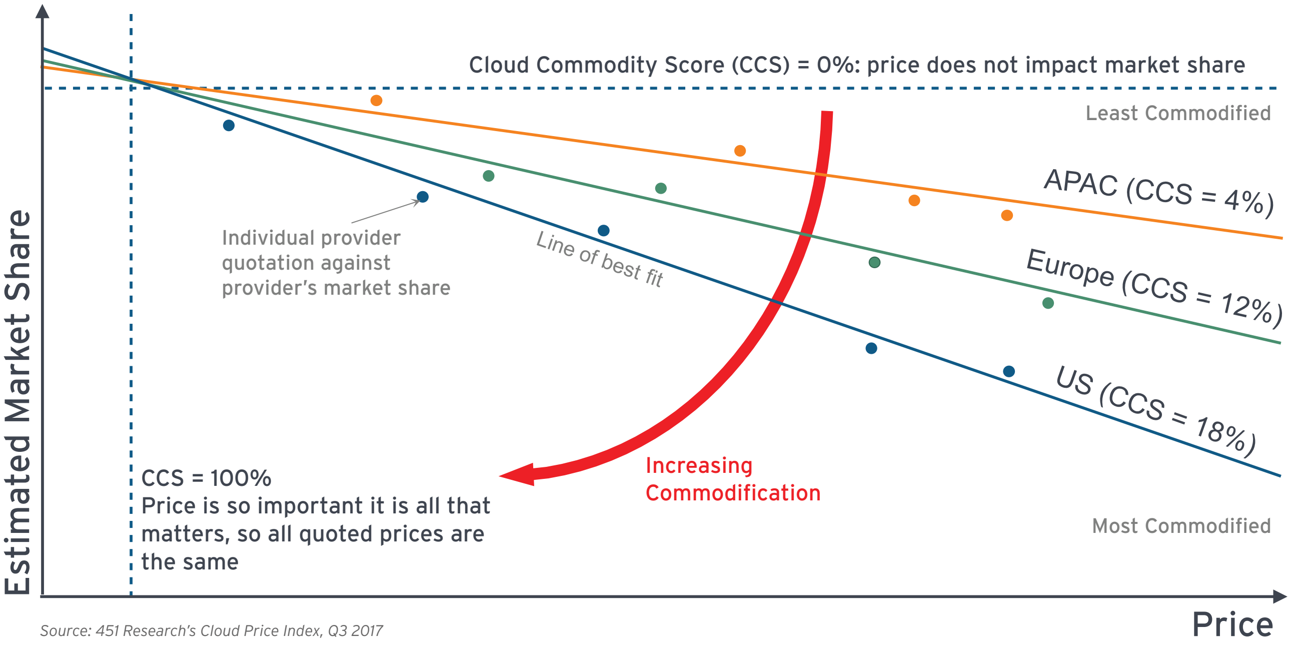
An independent key management service gives you the flexibility to shift workloads between on-premises datacenters and cloud resources while controlling your keys, abiding by compliance guidelines and establishing predictable performance. It would also spare you the complexities and costs of managing multiple encryption keys so you can focus on business initiatives.

This Pathfinder report summarizes the key technical and use-case attributes of key management as a service, a fundamental approach to securely managing data in the cloud. This report is sponsored by the Equinix data and hosting security team.

Private, Public or Hybrid Cloud? The answer is 'Yes!'

The Cloud Price Index from 451 Research highlights economic considerations as a leading driver for organizations transforming management of applications and data with usage scenarios of private, public and hybrid colocation clouds. Research shows a hyper-competitive environment with declining costs of storage and bandwidth leading to commodification of cloud services. Our enterprise recommendations include shorter-term contracts for the best deals as the market evolves. Key management as a service provides organizations with the technical flexibility in moving applications and data to be able to take advantage of market opportunities for various usage scenarios.

Figure 1: Regional Commodification



Source: 451 Research's Cloud Price Index, Q3 2017

1. Private cloud (or on-premises) approaches allow enterprises to control costs by placing applications and data in corporate datacenters. This approach for providing the complete infrastructure may be the most cost-effective where usage patterns are well understood and predictable. However, there is a risk that costs might spiral out of control if the enterprise needs to provision datacenter real estate, servers, storage, power and administration labor to meet demand spikes.

   Enterprises relying completely on private cloud approaches frequently use a physical hardware security module (HSM) to safeguard and manage encryption keys. The HSM provides secure storage in the protected datacenter with authenticated access, at the cost of acquiring specialized hardware and trained administration, which can inhibit business transformation to a cloud-based infrastructure.

Enterprises also work with software-based key management systems. There are open source alternatives for organizations with talented development staff, design expertise to securely handle encryption keys, and the willingness to maintain a software product.

2. Public cloud approaches allow organizations great flexibility in using shared resources in multi-tenant datacenters. Public cloud providers have storage, networking and administrative labor capacity to meet enterprise requirements for scaling performance, staffing and geolocation, for example. Organizations may pay a premium for reserve capacity, expansion or disaster recovery contingencies, and outsourcing staffing issues, but public clouds offer an expedient path for new business opportunities without having to build out infrastructure.
3. Hybrid clouds look to take advantage of the best of private and public clouds. One form of a hybrid cloud architecture is the colocated datacenter where the service provider is responsible for the facility and value-added core services, while the enterprise is responsible for servers, storage and administration. Colocation gives organizations the flexibility to extend their infrastructure without committing to long-term capital datacenter costs.

Using independent key management as a service provides a standard administration process for handling encryption keys, which gives organizations the agility to best serve business applications and data while controlling infrastructure costs. Enterprises will have encrypted data in on-premises datacenters, multi-tenant cloud service provider datacenters, and hybrid environments complete with colocated datacenters. An independent key management service offers the agility required to optimize use of multiple cloud scenarios to securely satisfy customer demand for access to applications and data without sacrificing performance.

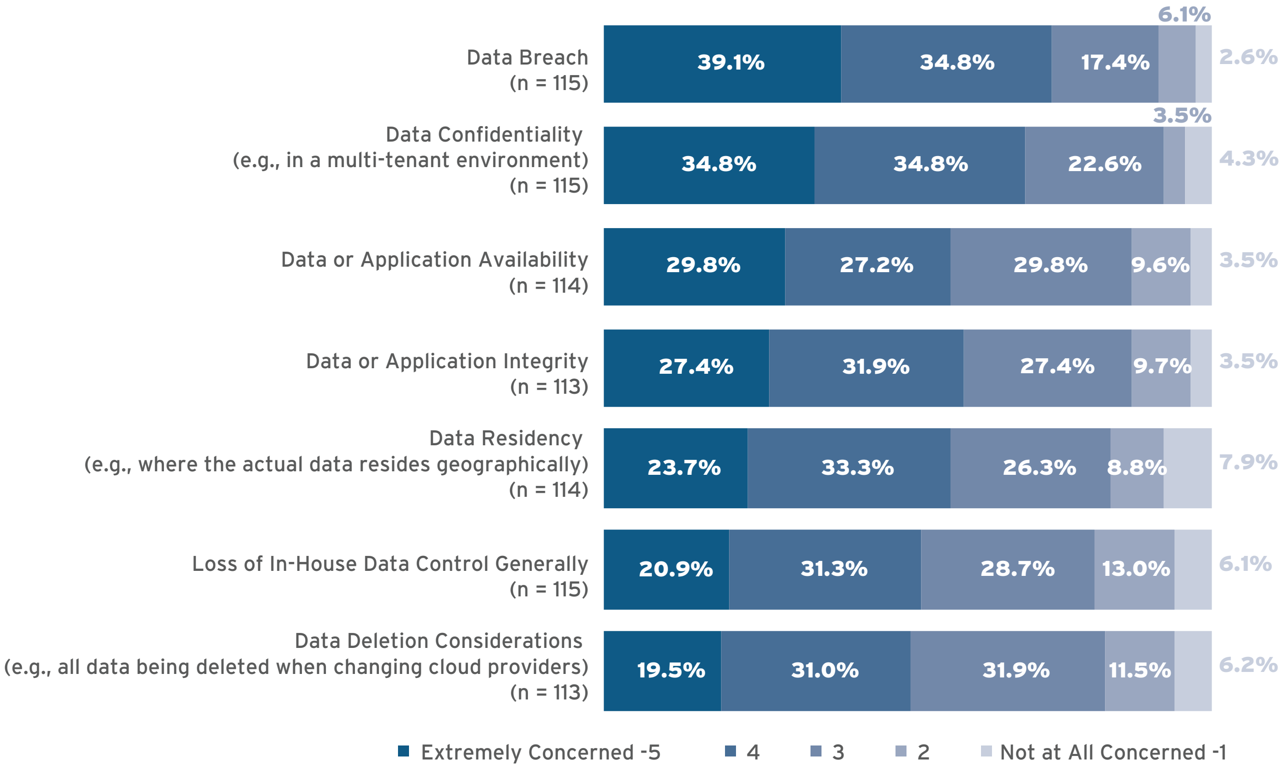
Securing Business Transformation in the Cloud

There are many reasons why enterprises allocate budget to migrate IT infrastructure into the cloud. They can be as simple as adding services the organization did not have before, or as complex as adding resource capacity and performance due to business growth, geographic expansion or finding better business terms.

The security performance issues of placing data in the cloud where it is closest to user and applications are varied and no less challenging, as shown in Figure 2. The leading concerns revolve around the classic definitions of confidentiality, integrity and availability, particularly when it comes to the subtleties of internationally located datacenters. However, business issues also affect security concerns when it comes to how data is backed up, effectively deleted, shifted between cloud providers and other elements that IT needs to control.

Figure 2: Data-related concerns regarding hosted cloud

Q. Please rate your concern with the following potential issues with hosted cloud solutions (Hosted Private Cloud, IaaS, or PaaS). - Data Related Concerns



Source: 451 Research, Voice of the Enterprise: Information Security, Budgets and Outlook 2016

Encrypting data for cloud environments is quite different from traditional file and disc encryption. Not only are audit requirements for compliance more complex to document, but the operational practices require a fine attention to detail. We suggest asking each key-management-as-a-service vendor to describe critical requirements including:

1. **How are keys created?** Master keys must be unique to your organization, and must be able to be validated; encryption keys derived from the master must also be securely created.
2. **Can you securely distribute keys to new services?** The last thing you can afford is a bad actor impersonating your business when distributing keys for the first time. Ensure that key exchanges are authenticated at every step to reduce the risk of attackers inserting themselves into the process when your business is vulnerable.
3. **Can you easily assimilate encryption keys from corporate resources or existing services?** Many cloud service providers retain customer master keys at additional expense to enable backup and recovery operations. The key management service needs to assume responsibility for cloud-provider keys that the business already relies on or those that the customer already owns and utilizes in a 'bring your own key' scenario.
4. **What steps are taken when you expand key management to other clouds?** You need to reduce operational risks to your business by using multiple cloud services and applications. Ensure that you can replicate your keys and management processes as your business balances its risk across multiple cloud providers.
5. **How do you manage key rotation and refresh policies?** Keys have natural lifespans – they need to be immediately refreshed for you to be confident of a full recovery from a breach. As a result, data that is encrypted under one key must now be accessible with a new key. It is not always practical to decrypt data with the old key and then re-encrypt with the new key, although that is the easiest to visualize.

6. **Where are retired keys retained so you can access archived data?** Your data may have a longer lifespan than your keys. For instance, HIPAA requires data to be retained for the life of the patient, but the actual lifespan of your keys may be shorter than the lifespan of the data. Ask your 'key management as a service' vendor what happens to old keys so you can access archived data without worrying that others may have copies of the keys.
7. **How do you protect exposing keys to the key management service, as well as privileged administrators?** It is imperative that your keys never be unveiled to the service or your privileged users. We recommend a complete zero-trust attitude when it comes to key management to avoid inadvertent or malicious disclosure of your keys.

Security that Performs in Architecture Considerations

The key management service provides a control point for accessing encrypted data with flexibility to place the control point on-premises or in the cloud. Separating issues regarding people, locations, clouds and data from datacenter infrastructure complexities is a major benefit of key management as a service. The independent key management service, in addition to providing administrative support for secure encryption key maintenance, must deliver additional architectural elements to seamlessly fit into your technical infrastructure.

1. Integrate with existing infrastructure components, such as policy handling, cloud exchanges, HSMs and administrator account directories to handle requests for encryption services and encryption key maintenance.
2. Deliver usage analytics and reporting to streamline security oversight, performance insights and compliance reporting. Logging of operations is essential to demonstrate security and compliance with your security policies.
3. Allow for layers of the architecture to be distributed between private, public and colocated cloud environments. Key management as a service yields agility and flexibility for deployment of encrypted business data, which requires an agile, flexible architecture.
4. Provide for automated key maintenance functions from authorized administrators. Make it simple to manage keys throughout their lifecycle – generation, usage, rotation and retirement.
5. Minimize the operational impacts of planning and training for performance, availability and compliance.

User friction deriving from performance issues can be the kiss of death as businesses transform to cloud infrastructures. If not properly designed, the fetching of keys to encrypt and decrypt data during read/write operations can add unacceptable latency to application performance. When it comes to key management as a service, there are a few performance principles to follow.

Deploy key management at the traffic exchange point to lower the risk of latency, a critical concept when distributing data across multiple cloud environments – a likely scenario for performance, security and economic considerations. Optimally, encryption keys should reside *near* the data for performance, but never *with* the data for security. Placing keys near the data reduces the time required to fetch keys for cryptographic operations, clearing the path for application performance. This can become critical if the application design calls out for keys every time it needs to read and write sensitive data.

The functional security and performance tenets of key management as a service for supporting encrypted data are prime for implementation as a cloud service. Your business will be moving encrypted data between multiple public cloud providers, multiple private cloud datacenters, and possibly multiple colocation datacenters. Placing key management at the traffic exchange point enables secure use across multiple private, public and colocated clouds without administering the complexity of multiple key repositories. Prudence suggests that a trusted independent key management service allows you to run your infrastructure with the confidence that your keys are being safely handled – a more secure and convenient approach than moving encryption keys from cloud provider to cloud provider.

Conclusion

Key management as a service is a concept whose time has come. Unless you are in the security industry, you are not in business to manage encryption keys across multiple providers and locations. Our recommendation is to evaluate independent key management as a service, starting with on-premises data and then expanding into the cloud. Evaluate the operating cost savings of the service, keeping in mind the savings over purchase of servers and software and operational costs in personnel to manage and maintain your own key management hardware. In our view, key management as a service just makes sense.

Content Furnished by

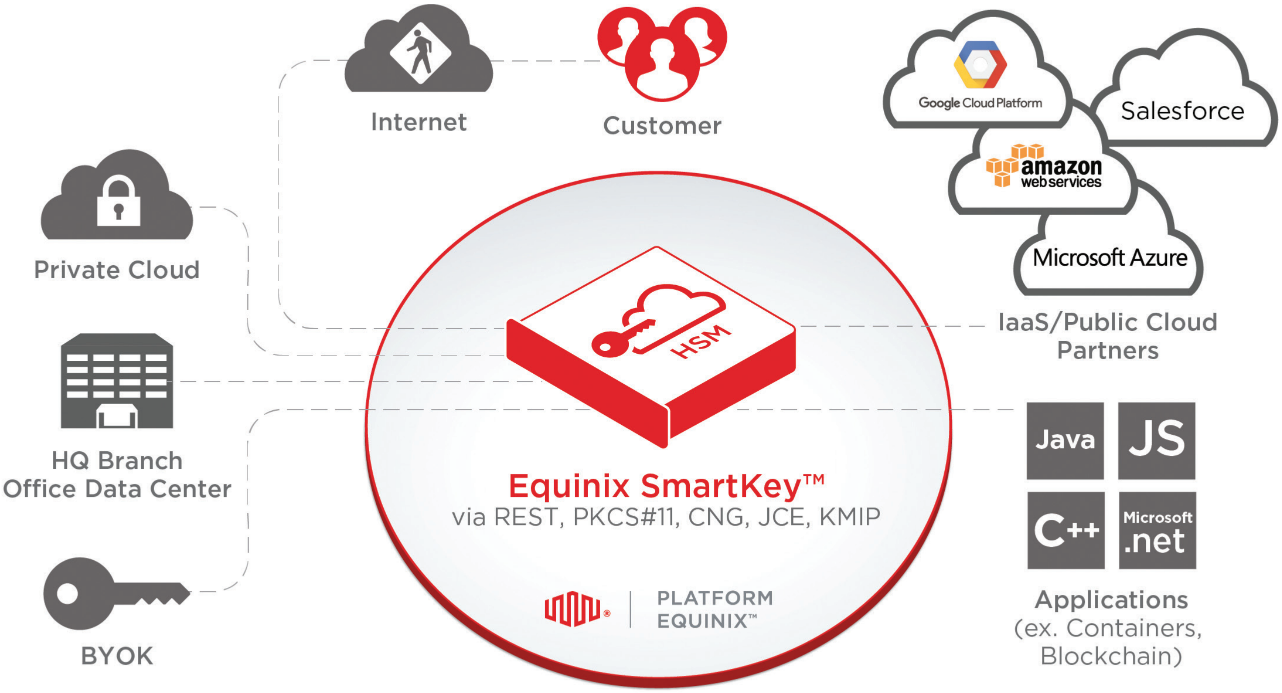
EQUINIX

Reinventing HSM as a Service with cloud ready encryption, key management and tokenization at the digital edge

Innovation and opportunity transform into competitive advantage in today's digital economy. As enterprise business models become increasingly interdependent, interconnection at the digital edge is essential to success. Furthermore, with enterprise IT executives expecting 60% of workloads to run in the cloud by 2018[1], the implications for security are dramatic. Where enterprise security perimeters were previously built around the enterprise datacenter, these controls must now be reshaped for cloud. The new security control point must be implemented at the intersection of people, locations, clouds and data.

Introducing Equinix SmartKey™ - a global SaaS-based secure key management and cryptography service which simplifies data protection in public, private, hybrid or multicloud environments. Operating independently or as part of Platform Equinix, SmartKey provides internet scalability, secure key storage, encryption and tokenization services; addressing performance and GRC requirements while keeping keys at the digital edge, close to clouds and carriers resulting in:

- Simplified key management with single source
- HSM-grade security with easy-to-use cloud service with built-in encryption and tokenization
- Data Sovereignty by providing key management with collected data/storage hosting in local/regional metros
- Lower latency performance and high availability with keys being at the traffic exchange point of all major clouds replicated across multiple locations
- Complete key secrecy



With SmartKey, enterprises can keep keys at the Digital Edge in close proximity to the data by strategically applying an Interconnection Oriented Architecture™ (IOA™) approach on Platform Equinix™. This strategy enables Enterprises to engage with users while securely integrating with clouds and digital business services.

Platform Equinix, a secure, global and digital platform used by over 8,500 companies, allows enterprises a competitive advantage via:

- New digital business models allowing collaboration with the right partners, direct access to 2,750+ leading cloud/ IT and 1,500+ network providers, and secure, lowest-latency (<10 milliseconds), shortest routes to new opportunities at the edge
- An unmatched global footprint that brings enterprises inside the top markets on five continents in premium, highly secure and reliable facilities
- Interconnection in dense and thriving industry ecosystems—including cloud, networks, financial services, online advertising, content, and digital media and entertainment
- Data and analytics located adjacently close to users for improved response times and distributed scale, reducing the amount of data traversing the networks

Operating the only global interconnection platform in 44 markets across five continents, Equinix empowers enterprises with:

- HSM as a Service enabling enterprises to have complete control of keys at the digital edge
- Agility to solve security challenges in the cloud
- Seamless IT transformation – driving innovation forward to meet demands of the digital world

GLOBAL DATA CENTERS

180+ Data Centers
44 Metros
100% Renewable Power Pledge
Interconnect to markets anywhere

INTERCONNECTION SOLUTIONS

240,000+ Cross Connects*
Connect directly to the clouds, people and places that matter to you

BUSINESS ECOSYSTEMS

9,500+ Companies
210+ of Fortune 500
Access the right partners to re-architect IT and compete as a digital business

PROVEN EXPERTISE

99.9999% Uptime Record
Global Solutions Architects™ prepare you for tomorrow, today, so you're always up and running with access to the help you need to transform

The global interconnection platform for the world's leading businesses.

*Data shown does not reflect cross connect data for recent Verizon acquisition.

1. *Source: 451 Research Blog Enterprise IT Executives expect 60% of workloads will run in the cloud by 2018, September 1, 2016*