OMDIA

MARKET RADAR

Publication date
April 14, 2022

Author
Tanner Johnson
Principal Analyst, Data Security, IoT Cybersecurity

Encryption Key Management (EKM) Solutions

Brought to you by Informa Tech

OMDIA

Summary

Catalyst

In this Market Radar, Omdia explores the Encryption Key Management (EKM) market and compares different solutions in this category. In the domain of cybersecurity, there is a triad of requirements that need to be established for comprehensive data protection to be achieved: controlling who can see the data in question (confidentiality), controlling who can change the data in question (integrity), and ensuring consistent access to the data in question (availability). While each of these pillars is essential in its own right, the loss of confidentiality, in particular, can have catastrophic implications, including the loss of intellectual property, loss of customer confidence, and even government fines should an organization be deemed negligent in their handling of their data. One of the primary ways to address the risks associated with the loss of confidentiality is through obfuscation methods such as encryption. However, since it requires the proper management of cryptographic keys, the importance of EKM becomes an essential piece of the process.

Key messages

- Effective data protection is impossible without proper EKM. As more encrypted data is generated with each passing day, there are more corresponding encryption keys that require managing, and as more sensitive data demands encryption, effective management of the corresponding keys still represents a significant challenge for many organizations. Unfortunately, authoritative guidance surrounding these challenges is considerably lacking. While government agencies may create regulations and compliance demands requiring the use of encryption to ensure certain kinds of data are protected, the corresponding process of managing the keys themselves is entirely up to the organization in question. This has helped foster a “false sense of security” scenario where organizations believe they are protected from data theft simply because they have met their individual compliance requirements.

- EKM solutions come in various deployment forms. The foundational bedrock of secure EKM is ensuring keys are handled properly throughout their lifecycle. If the processes an organization adopts with regards to generating or sharing their encryption keys can be replicated or intercepted by adversaries, all keys within that organization become effectively worthless as a protective measure for securing data. Hardware security modules (HSMs) offer considerable benefits when it comes to handling encryption keys. HSMs can offer physical access protection by detecting if the device has been tampered with. This physical protection extends to the secure generation of keys. Additionally, HSMs offer a secure environment for cryptographic functions to operate in. The added protection has resulted in some advanced information security regulations calling for the utilization of HSMs for key management.

- EKM deployments demand comprehensive considerations. As an organization evolves and continues to incorporate additional encryption requirements and corresponding tools, the opportunity for complications surrounding encryption incompatibility or mismanagement becomes greater. EKM systems can help to address many of the complications that stem from trying to combine and securely integrate different encryption tools and policy requirements. By consolidating the management of their encryption keys, the deployment of an EKM system provides any organization with a far more robust data-centric security posture.

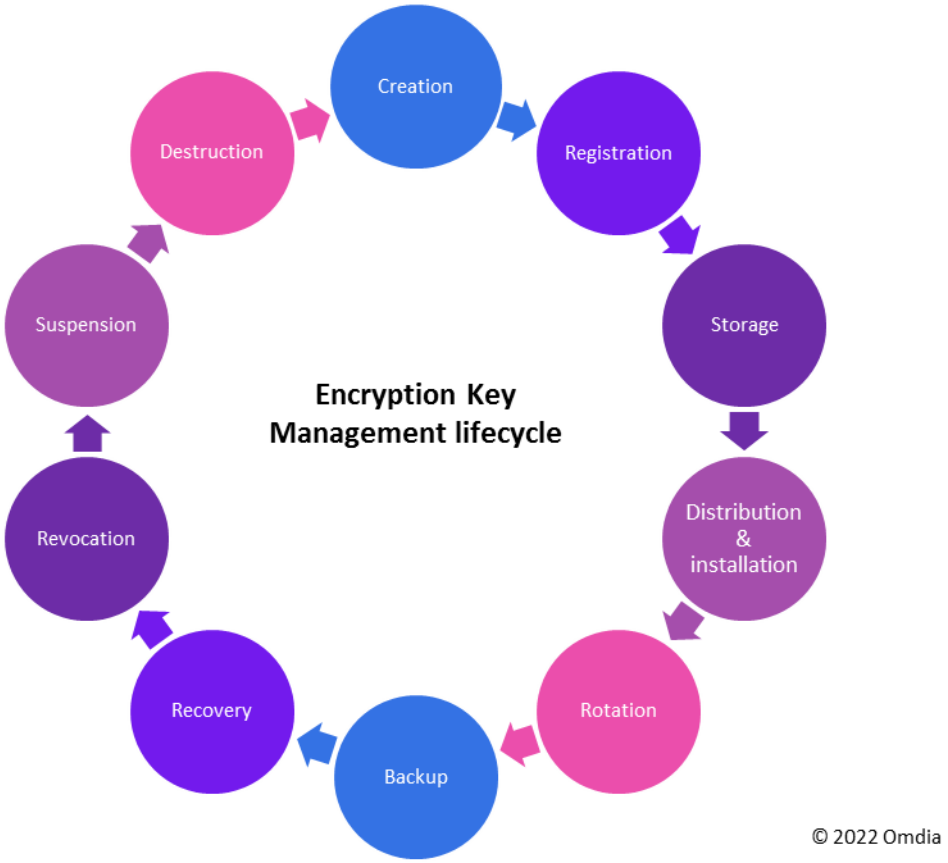
- EKM offers control over the total lifecycle of keys. As encryption keys form the absolute backbone of an organization’s data security efforts, they are truly the “crown jewels” for any adversary to obtain. However, securing the confidentiality of encryption keys demands that the keys are themselves encrypted, which in turn requires specific attention. In response, various deployment options have developed and matured in recent years that help facilitate greater control over the security of keys. HSMs can offer physical access protection by detecting if the device has been tampered with while also ensuring a secure environment for the generation of keys. Additionally, key management services (KMS) have evolved over the years as another type of EKM solution designed to mitigate the risks surrounding the mishandling of an organization’s encryption keys.

Omdia view

As the concept of “perfect security” is a fantastical myth, the reality is that complete prevention of unsanctioned exfiltration of sensitive data is impossible. However, there are numerous options available that can help organizations protect their data by making it effectively worthless to those who extract it, namely when it is concealed or obfuscated through various cryptographic methods. These methods may include encryption, tokenization, masking, and other concealment techniques. Each of these tools provides a unique capability to conceal the exact contents of data by demanding additional components such as ciphers or keys with which to decode the information, so it is once again legible.

One of the most fundamental methods of protecting data from compromise is through the utilization of encryption. The process of encryption transforms cleartext data into an illegible form known as ciphertext, using an algorithm to encode data with a cipher or cryptographic key. The number of keys involved in the process determines whether the encryption is symmetric (using one shared key) or asymmetric (using separate keys in tandem). Regardless of the chosen encryption method, the keys themselves are the cornerstone of an organization’s data protection efforts. If mishandled, keys can fall into nefarious hands, which could grant unlimited access to all encrypted data. Additionally, the mismanagement of these keys could ultimately prevent authorized users from accessing their encrypted data when needed. These challenges further illustrate the necessity for an effective EKM solution. Omdia recognizes a 10-step process in the EKM lifecycle, compiled from direct vendor input, as well as the National Institute of Standards and Technology (NIST), as shown in **Figure 1**.

Figure 1: The Encryption Key Management lifecycle



Source: Omdia

Omdia has identified the various features and functions that comprise the EKM lifecycle in order to provide for the differentiation between the leading EKM products on the market. These key capabilities comprise the totality of the numerous and comprehensive steps throughout the EKM lifecycle.

Recommendations

Recommendations for enterprises

The market for various encryption products and solutions is a mature one that has evolved and progressed steadily over the last several decades in response to the growing demand for the effective concealment of data. The number of threats to confidentiality that helped spur the rapid proliferation of encryption technology in recent years has also witnessed considerable growth. A wide range of factors have contributed to this, including, but not limited to:

- Consistent reports of high-profile data breaches.
- The increased size and scale of sensitive data being generated.
- A growing number of government regulations and mandates.
- Internal policy and compliance requirements.

As encryption keys help form the lifeblood of all modern data security efforts within an organization, mismanagement of these keys can be catastrophic to the continuity of operations. They are essential for the protection of data at rest, in motion, and in use at the application layer. Due to the sensitivity and criticality of an organization's data, some may be reluctant to outsource their key management strategy to a security vendor. However, to shift enterprise focus from the complex technological processes involved, it is recommended that enterprises utilize third-party solutions for encryption key management, which can free up resources to address and maintain general business security operations.

Recommendations for technology vendors

- In the face of evolving and dynamic security threats, EKM solution providers must look toward incorporating additional capabilities to stay competitive. As cyberthreats have evolved, protection solutions have correspondingly emerged that provide comprehensive countermeasures to these individual threats. Over time, niche solutions have been designed to address specific security threats. However, if disparate systems are adopted and deployed over time within an organization, they can add considerable complexity to the data security effort. Vendors should look to structure their EKM offerings in a format that helps reduce this complexity while streamlining provisioning and deployment.

- Unfortunately, cyber-adversaries are also continually innovating and adapting their attack campaigns, looking for any flaw(s) to exploit. In this new dynamic, challenges are evolving rapidly as nation-state actors are now capable of anonymously funding cybercriminals and digital mercenaries to conduct sophisticated attacks while maintaining plausible deniability. To stay ahead, EKM vendors need to focus their attention on maximizing usability while maintaining interoperability with other encryption solutions. This will require establishing partnerships with other vendors to ensure clients maintain compatibility with any legacy encryption systems currently deployed in their ecosystems.

Defining the EKM market

Definition and characteristics

EKM solutions provide organizations with a comprehensive and secure method of controlling the most critical component of their data security and obfuscation practices: their encryption keys. Due to the complex nature and absolute criticality of these types of solutions, the market for EKM solutions is quite competitive and includes offerings from a wide range of technology and security product providers. Understandably, many of the vendors offering EKM solutions are some of the largest contributors to the overall data security market itself. These solutions have gained significant popularity in recent years due to the growing demands surrounding the protection of greater amounts of data while maintaining compliance with an ever-changing dynamic of national and international data security compliance and regulatory demands.

The EKM offerings put forth by these vendors also come in a wide array of deployment options. These include, but are not limited to, HSMs and KMS. While similar to HSMs in core function, key management services also offer a centralized capability for exercising control over the entire encryption key lifecycle, but without the supplemental concerns that can surround the selection of a security appliance or the provisioning of the selected device. KMS can also facilitate the secure rotation, suspension, or destruction of keys no longer in use, as well as maintaining compliance with numerous regulations.

As an organization evolves and continues to incorporate additional encryption requirements and corresponding tools, the opportunity for complications surrounding encryption incompatibility or mismanagement becomes greater. EKM systems have been developed in order to assist organizations in addressing many of the complications that stem from trying to combine and securely integrate different encryption tools and policy requirements. This challenge becomes even more significant as greater amounts of sensitive data are generated that require protection through encryption. By consolidating the management of their encryption keys, deploying an EKM system provides any organization with a far more robust data-centric security posture.

Key capabilities and vendor landscape

Data-centric security is essentially a strategy that focuses more specifically on the resiliency of the data itself rather than on the countless hardware and software security solutions available. The intent and purpose behind encrypting data is to conceal it from unauthorized individuals. If properly and securely encrypted, the theft of data becomes more of negligible concern as the data is effectively worthless without the corresponding decryption key.

While the benefits of deploying an EKM solution are clear, an EKM deployment itself does not absolve organizations from their continued data security responsibilities. The comprehensive discovery of an organization's data that requires encryption (in all its forms, functions, and locations), as well as the respective policies that govern the encryption keys themselves, will require regular evaluations. These continued steps are essential components to any effective EKM deployment, but as each organization likely has unique requirements based on their respective industries and geographies, these steps must be accomplished internally.

Like with any third-party supplier, special consideration should be taken when choosing any EKM vendor. While some organizations may be forced to manage their own keys due to regulatory compliance issues, those not bound by this restriction need to engage in due diligence when choosing an EKM vendor. If an organization does choose a third-party provider, there must be a definitive understanding established between vendor and client outlining where the key management responsibilities of the EKM vendor end, and where those of the organization in question begin.

EKM market radar capabilities

All of the vendors covered in this report offer a robust set of features and a balanced portfolio of capabilities that help meet the complex demands of any EKM solution. Additionally, the vendors we explored in this research offer solutions across all major geographies and have traction with, and a strategy to target, mid-to-large-sized organizations. Omdia has identified a number of features and functions that provide differentiation between the leading EKM products on the market. These key capabilities comprise the verifications of the numerous steps in the encryption key lifecycle.

Key creation

This is the initial stage in the lifecycle surrounding the essential processes for securely generating new, unique, random, and unpredictable keys for use in encrypting data. If keys are not generated securely, they can be easily guessed or duplicated, making them effectively worthless for securing data.

Key registration

This is the process of associating a key with a particular user, system, or policy. This is to ensure the effective purpose of each encryption key as well as to identify what users or specific systems require access to the respective key.

Key storage

This provides a means of securely storing encryption keys in a manner that isolates and protects the key from any nefarious sniffing tools. If encryption keys cannot be securely stored, retrieving them during a crisis can be challenging.

Key distribution and installation

This stage ensures that keys are transmitted securely from their storage location to the system or user requiring access. The provisioning process for keys must be secure and verified in order to prevent insecure misconfigurations.

Key rotation

This criterion provides a means of mitigating risks associated with the exposure of older keys and the corresponding data being protected by regularly swapping out older keys. This process is an essential piece of secure key management as it ensures that the organization isn't vulnerable due to the continued use of legacy or outdated keys.

Key backup

This provides a safeguard for the restoration of any encryption key that has been accidentally lost or destroyed. As any form of encryption is worthless without its corresponding decryption key, having an effective backup strategy is an essential component of any encryption deployment.

Key recovery

This criterion outlines the processes for requesting approval for access to encryption keys, likely following a system disruption. Without an effective process for recalling keys currently in use, the key management process is severely hampered.

Key revocation

This process ensures that any encryption keys suspected of being compromised can be securely revoked and replaced as needed. As keys continue to age over time, the opportunity for discovery grows, which requires a secure means of removing them from use.

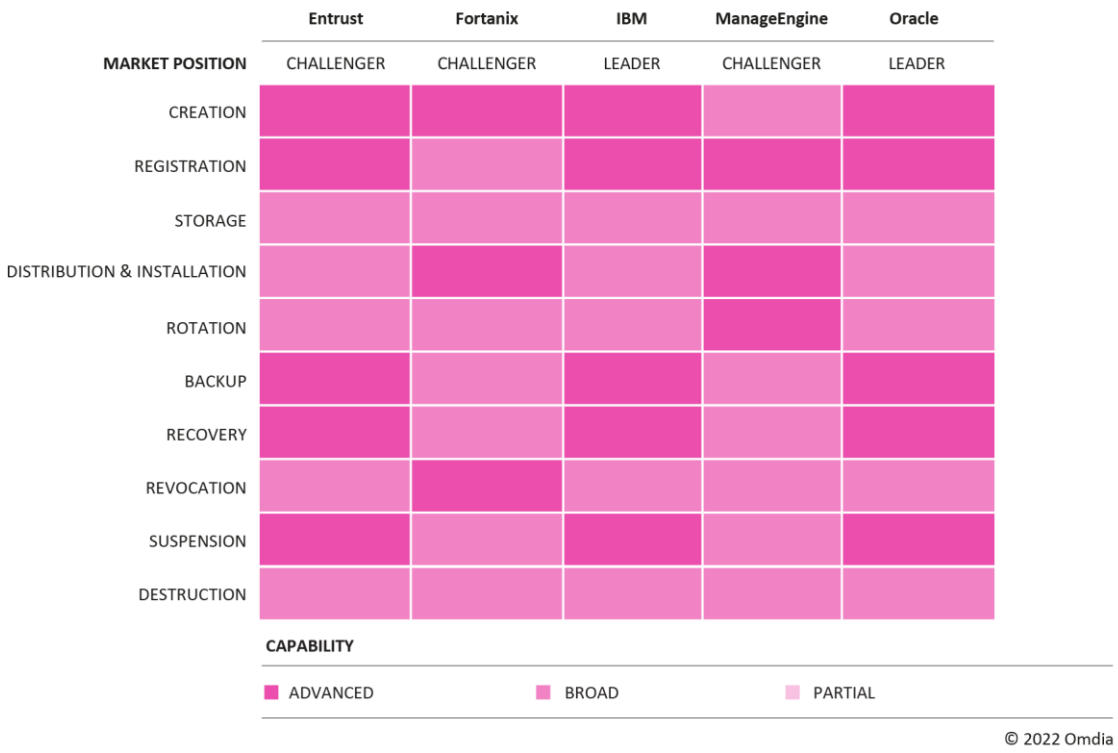
Key suspension

This stage surrounds the process of removing an encryption key from organizational operations, either temporarily or permanently. As personnel and structural changes occur within an organization, suspending the use of certain keys allows organizations to assess the value of each.

Key destruction

This is the process of ensuring that encryption keys that no longer require preservation are securely destroyed, including all key backups. Every key that is not securely destroyed remains a liability for the organization that created it.

Figure 2: Omdia heatmap for EKM solutions



Source: Omdia

The Omdia Heatmap for EKM solutions is colored as follows:

- **Advanced capability:** The vendor demonstrates very strong capabilities and/or capability in alignment with what Omdia explored as part of this research.
- **Broad capability:** The vendor offers better-than-expected capabilities that are well-suited to the needs of most businesses.
- **Partial capability:** The vendor provides expected capability but lacks some of the advanced capabilities assessed as part of this research.
- **Limited capability:** The vendor provides limited (or none) of the expected capability explored as part of this category.

The categorization of each vendor is as follows:

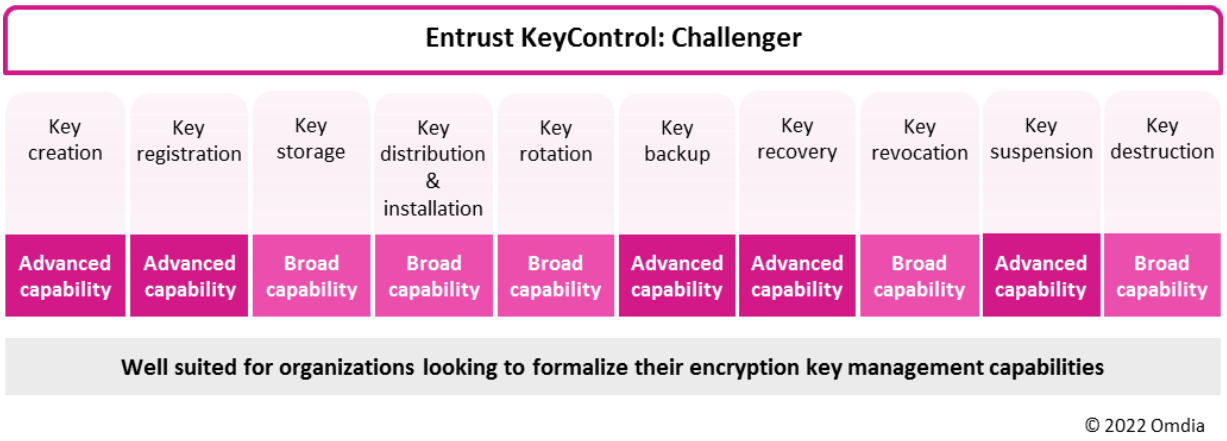
- **Market leader:** This category represents the leading solutions that provide advanced capabilities across six or more areas explored and which we believe are worthy of a place on most technology selection shortlists.

- **Market challenger:** The solutions in this category offer some advanced or broad capabilities, have appropriate functionality across other areas, and should be considered as part of a technology selection process.

Vendor Analysis

Entrust KeyControl

Figure 3: Omdia Market Radar recommendation—Entrust KeyControl



Source: Omdia

Why consider Entrust?

- Entrust KeyControl (formerly HyTrust) is an EKM system designed with interoperability and scaling in mind. In this same vein, KeyControl supports a variety of Key Management Interoperability Protocol (KMIP)-compatible encryption agents. KeyControl provides universal key management for KMIP clients, as well as offers KMIP multi-tenancy support, granting system administrators the ability to isolate environments for security and compliance.

- As a considerable market challenger, Entrust has sought to bolster its market presence by focusing directly on interoperability. A considerable challenge when adopting any security solution is ensuring proper integration with an organization's current technological ecosystem. If a solution cannot be integrated easily with legacy components already in place, that product is likely to be dismissed as a viable choice, even if the solution itself offers advanced functionality and capabilities over its competitors. KeyControl allows for easy integration with both customer master keys as well as native keys within Microsoft Azure and AWS systems. This interoperability provides greater granular control and management for any organization that wishes to generate its own encryption keys and integrate them into Azure and AWS while also providing lifecycle management for keys.

- Entrust KeyControl offers a secure and interoperable option for EKM amongst organizations, regardless of size. KeyControl provides effective key management that can be easily scaled to meet organizational demand as needed. Furthermore, the solution was designed to integrate with current Entrust solutions, such as the FIPS-140-2 Level 3 Entrust nShield HSMs easily.

Roadmap and areas of future focus

- An important strategic focus for Entrust is to position its KeyControl product as an advanced EKM solution capable of assisting organizations in exercising greater protection and granular control over their respective encryption keys. With a considerable increase in the sheer volume of cyberattacks in recent years, along with the scale of breaches and growth in activity from malicious actors showing no signs of slowing, maintaining effective controls over an organization's encryption keys is more critical than ever in order to maintain business operations.

- Entrust knows that in order to maintain its competitive edge in this space, it will need to continue fostering the partnerships they've already established, as well as look to gain new partnerships for future integrations and interoperability when available. Entrust is also aware that they need to continue to empower their customers by allowing them more granular control over their respective keys, when necessary, while seeking to utilize their partnerships to integrate any legacy components into a future service relationship with the company.

- Improving the breadth and ease of integrations that KeyControl has with other digital workplace capabilities is also an area Entrust should look to explore. Specifically, developing integrations with other cloud security, secrets management, and certificate authority solutions would be useful in delivering even greater data security insights and granular controls to potential customers. Through these collaborative partnerships, Entrust can position KeyControl as a capable alternative to the larger market players.

Market impact

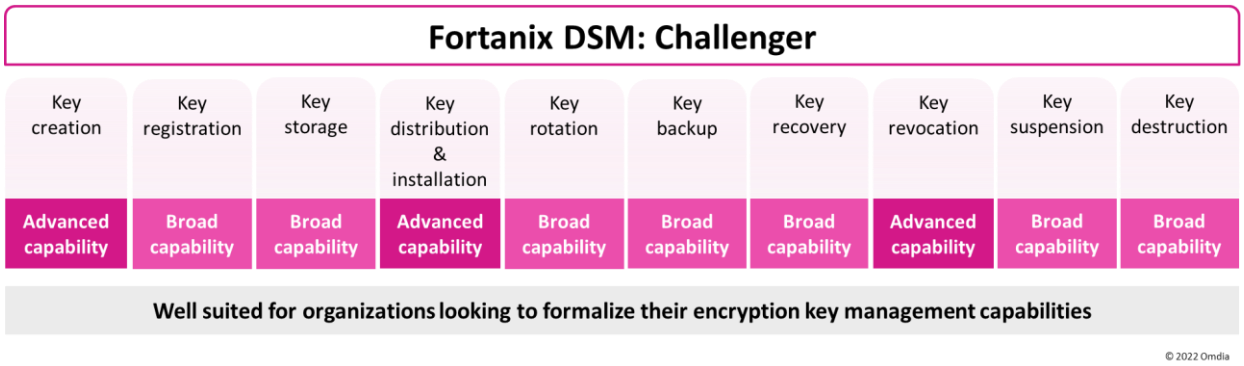
- Datacard Corporation was founded in 1969 by Willis Drake. The company was focused on providing some of the first magnetic stripe credit and identification cards to come to market. For the next several decades, the company maintained its position as a leader in this space until it began introducing additional internet security capabilities such as SSL certificates, public key infrastructure, and root key services into the larger company portfolio. It wasn't until 2013 that Datacard acquired Entrust, resulting in the birth of Entrust Datacard Corporation.

- Entrust clients have expressed positive reviews regarding KeyControl's advanced EKM capabilities and how the solution is affordable, easy to use, and scalable with necessary workload growth. Entrust clients span multiple vertical markets, including the financial industry, government institutions, traditional enterprises, healthcare services, and even retail markets.

- Entrust offers a truly comprehensive range of well-developed and advanced EKM solutions, giving the vendor a solid footprint in traditional enterprise environments. Entrust has worked diligently through a mature partnership program to bring EKM functionality to customers without requiring them to abandon their legacy third-party systems. These considerable investments and developments will allow Entrust to continue to compete in a market populated by much larger and more mature entities.

Fortanix Data Security Manager (DSM) Solution

Figure 4: Omdia Market Radar recommendation—Fortanix DSM



Source: Omdia

Why consider Fortanix?

- Fortanix DSM is a data security solution deliverable via software as a service (SaaS) or on-premise that is part of the company's overall broader information protection and management efforts. Fortanix promotes this offering as the world's only data-first encryption cloud solution that runs on their proprietary Confidential Computing platform. This SaaS offering allows a multicloud approach to protect critical information regardless of where the data itself is stored. Through this comprehensive process, Fortanix DSM can assist organizations in their efforts to improve their overall security posture through the utilization of key management, secrets management, and tokenization, and through advanced integrations with various cloud service providers. Additionally, in an ever-evolving and dynamic organizational environment, regulatory compliance becomes an added challenge. The Fortanix DSM platform can help businesses streamline compliance with a growing number of regulatory legislation requirements.

- Historically, EKM solutions have struggled to find a balance between the competing requirements of security, cost, and ease of use. Legacy HSMs have traditionally offered secure methods of EKM capabilities in a secure and tamper-resistant environment, but these solutions often come at a high cost, are complex to operate, and offer limited cloud integrations. The evolution of cloud KMS offerings has helped to address some of these limitations, but these solutions are frequently tied to specific cloud vendors and often store the data being protected in the same location as the encryption keys, which is inherently insecure. Fortanix has worked to establish an offering that brings the best of both worlds together. The Fortanix DSM was built with the cloud in mind, offers the same level of protection as HSM and KMS systems, and ensures that keys are stored separately from the data needing protection, all while remaining cloud-agnostic.

- Fortanix has worked to establish strong relationships and integrations with cloud vendors such as Microsoft's Azure, AWS, and Google Cloud. This is in addition to the partnerships with confidential computing vendors such as Intel and IBM. By establishing a comprehensive

set of capabilities surrounding a SaaS-delivered security solution, while providing deep integrations with advanced privacy-enhancing technologies such as confidential compute, Fortanix can boast an in-depth EKM security offering.

Roadmap and areas of future focus

- Fortanix has made considerable efforts to provide a wide ecosystem of integrations which is of strong appeal to the many organizations concerned with "vendor lock-in." Security solutions can be costly and are typically the hardest to see immediate returns from on any investment. Organizations traditionally concerned with being stuck within a particular vendor's ecosystem are likely to find active integrations within Fortanix's DSM solution that operate seamlessly with their legacy infrastructure.

- The complexities involved in the practice of EKM are considerable, especially for organizational entities looking to establish stronger controls over their keys. The Fortanix DSM offers a means of securing encryption keys that is both secure, simple, and scalable to the needs of the organization in question. The entire system is built using FIPS-140-2 Level 3 certified hardware while remaining instantly available and deliverable via the cloud. Furthermore, the SaaS method of delivery for EKM can help to future-proof itself against evolving regulatory and compliance requirements.

- Fortanix has obviously recognized the inherent benefits of establishing greater numbers of plugins and integrations within its DSM portfolio. As these integrations help to ease the transition of would-be clients into the Fortanix ecosystem, the company is more than aware of the importance of maintaining and maturing the integrations already in place while working to establish more interoperability through continued integration development.

Market impact

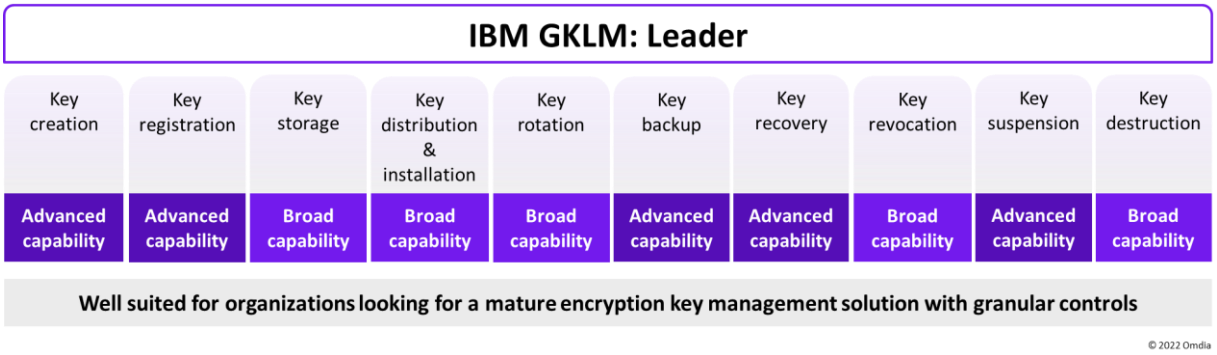
- Fortanix has created and delivered an EKM solution that works across different industry verticals and provides dedicated services in support of its overall market approach here. Fortanix DSM is well suited for deployment by a wide range of organizations and businesses across various verticals, including government, healthcare, financial services, technology, and professional service verticals.

- Due to the attractive quality of its comprehensive integrations, as well as the partnerships the company has established, Fortanix DSM has strong international adoption amongst organizations of all markets and sizes. The SaaS delivery method allows potential clients to utilize the auto elasticity of the cloud to scale on-demand with their respective organizational needs without having to concern themselves with capacity, upgrades, and hardware replacement.

- Driven by the increased demand and prioritization that organizations have around EKM solutions, Fortanix reports strong revenue associated with its EKM product over the last financial year. Omdia recognizes Fortanix's EKM proposition as having the broad market mindshare and awareness shared by some of its peers in this space. The strong capabilities present in the DSM portfolio make it a solution that will meet the needs of businesses of different sizes and key management maturity.

IBM Security Guardium Key Lifecycle Manager (GKLM)

Figure 5: Omdia Market Radar recommendation—IBM Security GKLM



Source: Omdia

Why consider IBM?

- In the domain of comprehensive data security, few names carry as much weight as IBM. IBM Security's Guardium Key Lifecycle Manager (GKLM) provides a centralized key management solution for all encryption demands. In addition to managing encryption keys, IBM's GKLM helps to ensure that organizations align with guidance for Payment Card Information (PCI), as well as NIST. Furthermore, GKLM offers automatic key rotation to maintain complete and comprehensive encryption key security.

- Over the various iterations of the solution, the IBM GKLM has worked to maintain data redundancy and high availability options via encryption key clones, as well as a multi-master key setup. In previous releases, the GKLM solution allowed for one master server and upwards of 20 clones. However, any new keys could only be created by the master server, while replicated keys could be obtained from any clone. In subsequent releases of GKLM, IBM provides customers with the option to replace all potential encryption key server clones with up to 21 master servers. This allows any new keys to be generated by any master server, and that key can be replicated to all other master servers in real-time.

- In order to maintain their innovative approach, IBM's GKLM solution was developed to include a version designed for containerized deployment in addition to their traditional delivery model. Containerization offers additional levels of security natively since containerized applications can run as isolated processes that operate independently of other containers. As a result of the isolated environments provided via containers, it helps to prevent any malicious code that has affected one container from impacting others, or potentially infecting the entire host system. The containerized offering of GKLM has maintained nearly all of the benefits of a traditional deployment, with only minimal loss to specific operational features.

Roadmap and areas of future focus

- IBM offers an intuitive set of core EKM capabilities and has solidified its position as a market leader in this space. GKLM has already become the preferred key management solution for a wide range of banks, financial institutions, and their respective partners. Additionally, research institutions, universities, and life science firms comprise a good deal of GKLM clients. Lastly, local, state, and federal government agencies have also sought to deploy GKLM capabilities, most notably the City of New York being amongst the list of customers utilizing IBM's EKM capabilities.

- IBM recognizes the importance of ensuring interoperability with legacy customer systems and, as a result, has worked to integrate HSM capabilities into their GKLM solution. In addition to HSMs, IBM has developed their GKLM solution to be deployed on a large assortment of storage devices and media. IBM recognizes the importance of broadening the overall footprint of storage devices that GKLM is compatible with. By increasing interoperability options, IBM is ensuring GKLM remains an attractive offering for enterprises and businesses by remaining compatible with a wide range of legacy infrastructure.

- With the most recent release of the GKLM solution, IBM is looking towards the future with some of its latest enhancements. The solution has been adapted to include operational enhancements that allow integration with Post-Quantum Cryptography (PQC) Safe 3592 storage devices via support for AES-256 bit symmetric keys. Additionally, GKLM helps to provide support for the Certificate Chain of Trust, as well as espousing mutual-TLS based authentication between IBM's Enterprise Key Management Foundation (EKMF) and the GKLM solution.

Market impact

- IBM was founded over a century ago in 1911, and the company is headquartered in Armonk, New York. IBM delivers EKM and other data security solutions to customers across all industries, including healthcare, finance, government, retail, and academia. IBM managed to accumulate over $57bn in revenue in 2021 and understandably has a primary presence in the US. However, IBM has made considerable inroads into Europe, the Middle East, and Africa. The company has roughly 20% of its revenue stemming from the Asia & Oceania region.

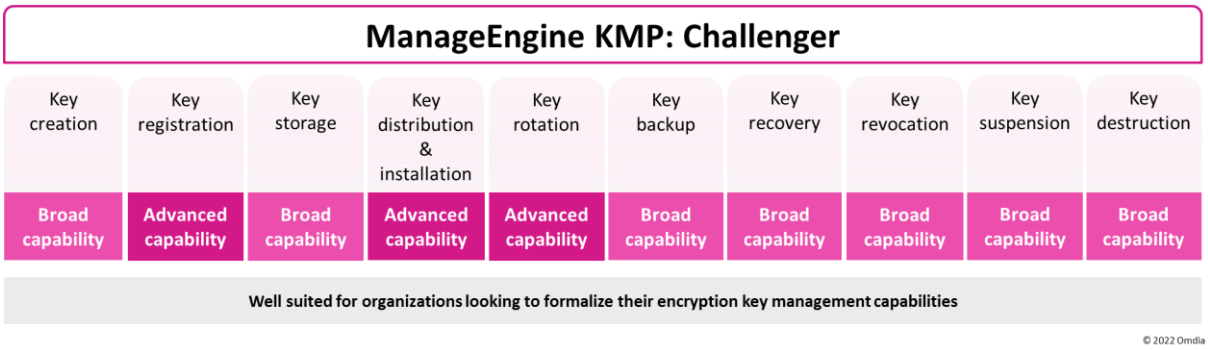
- Due to IBM's already hefty position in the data security market, their GKLM product appeals to organizations of all sizes. Additionally, there is no limit to the type of market that can utilize the advanced EKM features available in the GKLM solution. However, the EKM market is competitive, so it will be imperative that IBM maintain its innovative approach to future-proofing its EKM offering. IBM's size can also be a potential hindrance when compared to smaller, nimbler EKM vendors. IBM will need to maintain the momentum they've developed in this space—along with focusing on increasing interoperability—if they are to maintain their leadership in this domain.

- IBM has worked diligently to establish a substantial partner ecosystem that is continuously evolving and maturing. In addition to these partnerships that help maintain interoperability with legacy systems, IBM has invested considerably into addressing the complexities surrounding regulatory compliance and standards adherence. From PCI-DSS to HIPPA and

GDPR, amongst others, IBM is dedicated to the protection of financial, healthcare, and private data for their clients.

ManageEngine EKM

Figure 6: Omdia Market Radar recommendation—ManageEngine KMP



Source: Omdia

Why consider ManageEngine?

- ManageEngine's Key Manager Plus boasts a comprehensive set of EKM capabilities for enterprises and organizations alike throughout all markets as a mechanism to protect their most critical data. In response to the growing reliance on encryption keys as a means of user authentication, the trend toward the utilization of password-less authentication continues to rise. ManageEngine's Key Manager Plus provides organizations with a centralized and secure key management solution to mitigate the risks associated with the unauthorized proliferation of encryption keys that could threaten the confidentiality of organizational information.

- Key Manager Plus comes with a suite of advanced security features built-in by design. The solution offers dual AES-256 encryption at both the application and database levels while inherently preventing the master encryption key from residing with the encrypted data. The solution has several integrations with identity stores such as Microsoft Active Directory, any LDAP compliance directory service, as well as RADIUS. Furthermore, Key Manager Plus utilizes industry-leading key generation standards applying NIST recommended encryption algorithms, as well as the ability to incorporate additional passphrases for encryption keys.

- Key Manager Plus offers advanced privacy settings that empower clients to have greater granular control over the confidentiality of their data. Key Manager Plus allows for audit trails to be purged, removing sensitive information no longer required for operations. The solution offers two levels of password protection for all exported files, including a global password for all users, as well as allowing individual users to generate their own. The solution offers controls for personal data exposure in any generated reports, allowing admins to make or hide any private details in data. There are provisions to allow any notifications to be sent to email addresses not associated with the solution. Lastly, the solution allows admins the option to control product activity tracking to conceal the activities from the ManageEngine platform.

Roadmap and areas of future focus

- With competitors such as Oracle and IBM, ManageEngine is a definitive underdog in the space of EKM. As a result, the company knows it must look to establish comprehensive partnerships with other security vendors, such as Sectigo and Entrust, in order to help facilitate advanced capabilities such as certificate management in addition to their key management offerings. Additionally, the company is working to incorporate support for ACME encryption protocols, Machine Identity Management, a cloud version of Key Management Plus, and a private Certificate Authority (CA) option into their EKM offering.

- ManageEngine's strong focus on encryption keys security will see the vendor further invest in capabilities that support businesses looking to embrace stronger EKM functionality. The pandemic saw a massive shift towards remote working as a means of containing the contagion, and organizations have had to develop long-term plans that incorporate hybrid work in response to this new operational environment. As a means of incorporating security as far left in the development process, the company is looking to integrate development operations into their encryption key solution for added application security.

- As a smaller player in the domain of EKM, ManageEngine is looking to incorporate several substantive integrations into its platform in order to help to maintain its competitiveness against larger players in this domain. One of the most noticeable limitations is the company's lack of ability to integrate with HSMs. While ManageEngine is readily aware of this comparative limitation, the company is actively working to address this by incorporating HSMs in future releases.

Market impact

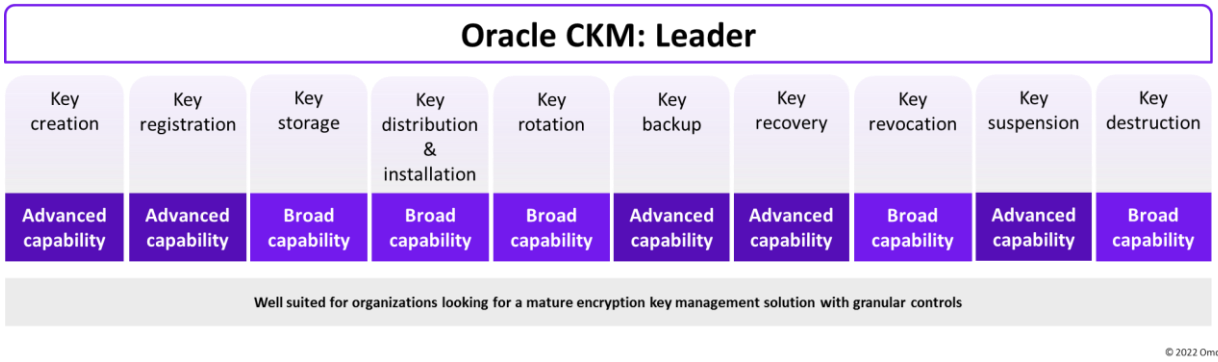
- Founded in 1996, ManageEngine was originally classified as a network management company named AdventNet. Headquartered in Pleasanton, California, the company was renamed ManageEngine in 2002 as the IT management software division of its parent company, Zoho Corporation. Since its inception, ManageEngine has sought to increase its overall foothold in the IT management space by incorporating greater collaboration and integration through an advanced and comprehensive partnership program.

- While ManageEngine's Key Manager Plus offers a comprehensive suite of advanced functionality and capabilities regarding SSH encryption key management, another significant component of the solution provides additional support for SSL certificate management for securing websites and transactions. With the ability to offer a combination of both key management and certificate management in the same solution, Key Manager Plus has managed to differentiate itself in this market.

- ManageEngine's Key Manager is currently adopted by organizations across numerous verticals and supports a variety of different use cases. While primarily focused on enterprise IT environments, Key Manager Plus provides the capability for organizations to streamline the management of their respective "secrets." By offering granular visibility and control over keys and certificates simultaneously, Key Manager Plus allows its clients to maintain their uptimes, while addressing security incidents as they occur, at the same time from the same solution.

Oracle Cloud Key Management

Figure 7: Omdia Market Radar recommendation—Oracle Cloud Key Management



Source: Omdia

Why consider Oracle?

- Oracle Cloud Key Management offers a unique perspective when it comes to encryption key management as the company provides multiple cloud encryption options that allow clients to select an offering that is best suited to their specific needs. As part of the Oracle Cloud Infrastructure (OCI), the KMS solutions offered include Oracle Management Encryption, KMS Vault, KMS Virtual Private Vault, and KMS External HSM.

- Oracle's Managed Encryption offers the simplest capability to manage, as it's entirely controlled by Oracle, so it limits customer access to keys. The KMS Vault allows customers to control and manage their own respective keys and offers multi-tenant HSMs to securely handle encryption keys. KMS Virtual Private Vault continues to grant the customer control over their own keys while deploying a single-tenant HSM. Lastly, KMS External HSM allows clients to maintain complete control over their own keys while utilizing on-premises HSMs.

- As complex as the handling of keys can be, Oracle's KMS adds additional flexibility to the creation of keys. The Oracle KMS uses a FIPS 140-2 Level 3 HSM as the default method for the storage and processing of keys. The benefits of standalone HSMs are considerable, as they offer tamper-resistant functionality by default. However, Oracle KMS grants clients flexibility if they want to use a software option to store and process keys on server memory, encrypted with a HSM key while the data is at rest. The solution helps organizations maintain compliance with evolving regulations and allows clients to bring their own key (BYOK) into the OCI.

Roadmap and areas of future focus

- Oracle's KMS currently has several features offering distinct capabilities for clients. While Oracle's KSM solutions currently offer both software-generated and HSM keys, the company is looking to establish external HSM capabilities, including hold your own key (HYOK) functionality. Oracle is also displaying a dedicated commitment toward future-proofing its solutions by incorporating bleeding edge capabilities into the OCI. Oracle's KMS roadmap

includes future plans for adding “confidential computing” functionality to its solution, as well quantum cryptography and next-generation HSM capabilities.

- Oracle’s Cloud Key Management service is a solution that integrates seamlessly with the library of other Oracle products. For example, Oracle DB solutions natively integrate with their KMS offering. Oracle uses transparent data encryption (TDE) to protect data-at-rest in Oracle databases. The system uses a two-tier key architecture that involves a data encryption key (DEK) managed by Oracle that is responsible for encrypting customer data, and the TDE Master Key (MEK), which is configured by the database admins and encrypts the DEK. The TDE MEK is managed entirely by the customer, including the key’s lifecycle and its rotation. The MEK itself is stored in the Oracle KMS protected by FIPS 140-2 Level 3 certified HSMs.

- Oracle also distinguishes itself by offering Cross-Region Replication (CRR) for its encryption keys. Oracle’s KMS system is designed to provide automatic and asynchronous replication of keys to any region within a predefined realm. However, the customer controls both the keys and destination region necessary for key replications. As a result, CRR helps clients facilitate and meet compliance with any disaster recovery requirements.

Market impact

- The Oracle Cloud Key Management solution has been lauded across a wide range of market applications. Retail clients have deployed Oracle’s solution in order to protect sensitive workloads. Healthcare agencies have used the KMS-dedicated and FIPS140-2 Level 3 compliance HSM storage for keys in compliance with multiple regulatory requirements. Financial institutions have managed to use their own keys from on-premises, while other KMSs utilize cloud providers to protect their respective data. Telecommunication clients rely on KMS in order to manage the various applications and services in Oracle Cloud, such as SaaS, DBaaS, and a variety of storage options.

- Oracle has managed to develop its software and cloud capabilities considerably in the last 40+ years since its inception and has become a powerhouse in the software and security markets. As a result of the company’s maturity, clients have an expectation of advanced capabilities with regard to their products. OCI’s KMS system offers both centralized and customer-controlled key management that offers high availability, with 99.9% service-level agreement (SLA) and service level objective (SLO) availability. The solution also supports both symmetric and asymmetric encryption, as well as digital signing and verification.

- Oracle’s approach is one that advocates and endorses the value of a consolidated suite of products from a single vendor while simultaneously maintaining the value of interoperability stemming from established partnerships. Oracle’s maturity, advanced capabilities, and increased functionality within this domain establish them as an obvious leader in the EKM market. Oracle will need to maintain the balance they’ve created in their portfolio between complete management of client requirements and granting customers granular controls over their own security.

Appendix

Methodology

This report utilizes responses to a comprehensive Omdia capability matrix, in addition to briefings. This was accompanied by insights gathered via TrustRadius and secondary research and data sources.

Author

Tanner Johnson, Principal Analyst, Data Security, IoT Cybersecurity
askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com
askananalyst@omdia.com