IDC ANALYZE THE FUTURE

IDC VENDOR SPOTLIGHT

Sponsored by: Thales

The speed of change in organizations' data needs and environments is too fast to fashion a targeted product approach for each new use case. Instead, a use case–extensible data security platform closes windows of data breach exposure, speeds time to compliance, and improves operational efficiency.

Data Security Point Products Are Passé: Platforms Pave the Way Forward

November 2020

Written by: Michael Suby, Research Vice President, Security and Trust

Introduction

Organizations' data security challenges are growing with the escalating volume of data that organizations collect, create, use, and store across a sprawling assortment of environments to support a myriad of business objectives.

Cloud adoption is a major contributor to this environmental expansion. According to IDC's *COVID-19 IMPACT on IT Spending Survey* conducted from August 26 to September 6, 2020, cloud services adoption is surging. Over one-third of surveyed organizations either have increased or are increasing their 2020 spending on cloud services over what they originally budgeted for 2020. According to IDC's 2Q20 *Cloud Pulse Survey*, organizations are more likely to use a mix of clouds for their data-intense applications rather than just a single cloud. In that survey, 64% of respondents rated the importance of running applications and data seamlessly across different public and private clouds for artificial intelligence/machine learning (AI/ML) projects as an 8 or above (10 = extremely important). Further, sensitive data is just as likely to be in cloud environments as in private datacenters. According to IDC's 2020 *Data Security Survey,* 98% of organizations already store sensitive data in the cloud.

AT A GLANCE

KEY TAKEAWAYS

- » Organizations' data security needs are intensifying and spanning multiple environments.
- » Inconsistency in data security practices and lack of data visibility are growing risks.
- » Point products may win a battle but lose the war.
- » Comprehensive data security platforms help organizations scale data security by supporting expanding use cases with operational efficiency and flexibility.

With this expanding footprint of sensitive data, organizations' data security needs are intensifying. Prominent among those needs is comprehensive data visibility. Unfortunately, if data visibility is not comprehensive, data security controls will certainly fall short. Correspondingly, the risk of data breaches and being noncompliant with data privacy and security regulations looms larger.

Many organizations have attempted to cobble together specialized data security products from multiple vendors to address a broadening set of data security use cases. This approach is challenging. Each product requires knowledge and experience to operate proficiently and forces security teams to devise processes and workflows to integrate products and administrative dashboards potentially for each use case. Integration can be complex, and it requires talented personnel and budget, which most organizations lack, and there is no guarantee that the organization's data security use cases will be met.

IDC recommends evaluating prospective vendors and their platform-based solutions along with the following criteria:

- Functional comprehensiveness for broad use case extensibility
- Operational efficiency derived from a unified administrative interface
- Flexibility in leveraging cloud-native capabilities and licensing

Data Security Platform Evaluation Criteria

Functional Comprehensiveness for Broad Use Case Extensibility

IT security teams are often constrained by their current data security products. A product originally acquired to address a specific use case may have a long, useful existence for that use case but may be inadequate for other use cases. Moreover, if the IT security team attempts to make do with data security products lacking use case extensibility, trade-offs in security efficacy or operational efficiency, or both, are likely. Simply put, point products have drawbacks.

Platform functionality is an essential building block for addressing current, planned, and unplanned future use cases.

Logically, IT security teams are evaluating a platform approach to better meet their extensibility needs. As they do, IDC's recommendation is to focus on functional comprehensiveness rather than just supported use cases. While existing use cases are helpful, you should be examining the comprehensiveness of functionality within the platform because functionality is an essential building block for addressing current, planned, and unplanned future use cases. In addition, the same use case can have situational differences across organizations. The true measure of meeting use case requirements is in your distinctive situation, and that is well served with a comprehensive set of building block functionalities.

IDC recommends that organizations look for a comprehensive data security platform with the following functions:

- **Full data life-cycle care.** The life cycle of data crosses multiple functions, and each function is critical to uninterrupted cradle-to-grave data security. The functions are discovery, classification, risk analysis, protection, user access control, policy and key management, migration, and destruction.
- **Feature richness.** At the individual function level, data security requirements and business objectives vary such that "one size fits all" simply lacks the versatility that organizations demand. Organizations should consider the following subset of functions when evaluating platforms:
    - **Discovery.** The platform should have the ability to discover structured, semistructured, and unstructured data wherever that data is stored (e.g., in files, folders, file shares, databases, data lakes, cloud storage).
    - **Classification.** A combination of ready-to-use data classification templates is an important feature, as is the ability to create custom classifications and apply risk analysis for data classification. Classification templates specific to prominent regulations (e.g., General Data Protection Regulation [GDPR], Payment Card Industry Data Security Standard [PCI DSS], and California Consumer Privacy Act [CCPA]) assist organizations in being compliant.

- **Protection.** Regulations, data class, and business use are all relevant factors in choosing the optimal approach to protect data. Multiple crypto options (encryption, format-preserving encryption, tokenization, masking) are important but not enough. Depending on circumstances, risk-based access control and audit logging are also valuable complementary additions to cryptography. With a range of data protection options, guided remediation is a beneficial feature, or working with trusted advisors and vendors, so less experienced personnel do not become paralyzed by multiple choices.
- **Policy and key management.** Deployment options in policy and key management functions serve organizations' need for flexibility to apply these functions to environments where organizations' data lives. Policy and key management functions may be deployed in the cloud or on premises and in virtual appliances and hardware security module (HSM) form factors. Some organizations will also need to be standards compliant with key management and data sovereignty statutes (e.g., Federal Information Processing Standard 140-2 [FIPS 140-2] and GDPR).
- **Migration.** The hybrid (on-premises and cloud) and multicloud footprint of organizations' data practically guarantees that data migration will be necessary. Along with this certain outcome is the importance of migrating data from one environment to another without sacrificing availability, producing protection gaps, or causing policy and operational inconsistencies. A data security platform requirement is to equally support on-premises, hybrid, and multicloud environments to support migrations and data repatriations.

» **Environment agnostic.** Data is neither static in location nor dormant. It is present in multiple environments, and the previously listed functions must consistently operate wherever data that requires protection is present. This includes end-user and non-user devices, on-premises datacenters, private clouds, public clouds (infrastructure as a service [IaaS] and platform as a service [PaaS]), and software-as-a-service (SaaS) applications. Data security platforms that are not agnostic undermine organizations' ability to tie policies to data and avoid gaps in data protection between the different environments.

» **Turnkey technology integration.** Even with support for a wide range of functions consistently applied across a range of environments, it is unlikely that any data security platform vendor can organically or via technology licensing have all the capabilities organizations want integrated. Plus, organizations' journeys to a single data security platform could transpire over a lengthy period and may never be fully realized. Nevertheless, users want minimal friction among coexisting functions. If either or both circumstances correspond to your organization's needs, you should investigate the platform vendor's breadth and depth of technology integrations.

» **Application developer friendly.** Defining and bolting on data protections as an application transitions from development to test and then production or is already in production is unfortunately the risky reality for most organizations. Data security is not part of the application development routine. Yet it could be if the data security platform provider offers easy-to-use toolsets for developers and organizations to institute data security as a standard developer practice. There is also a risk management aspect to offering APIs for developers, while only the SecOps or IT team controls key management and policies. This separation of duties ensures that developers have the minimal amount of control when adding crypto and tokenization routines into their applications. The key management life cycles and crypto policies, such as dynamic data masking rules, remain with the IT team. This creates the ability at scale for fundamental enforcement of separation of duties and meeting best practices.

Operationally Efficiency Derived from a Unified Administrative Interface

Shortages in security talent is an industrywide, perennial challenge. Consistent with the laws of supply and demand, the cost of security talent further adds to organizations' challenges, especially in hiring and retaining experienced personnel. As previously described, a data security platform approach brings together and integrates multiple critical functions and broadens use case extensibility. Yet full realization of the risk-reduction benefits of a platform will be elusive if manageability is lacking and difficult to achieve with an understaffed data security team.

Therefore, IDC recommends that organizations take a very close look at the platform from an administrator's perspective. Is the platform's administrative interface built for operational efficiency — that is, learned quickly, logically assembled, and comprehensive? In addition, data security administrators are privileged users, and if their privileged access is unbounded, misused, or compromised (e.g., account takeover), the data security platform regresses in its primary objectives of protecting sensitive data and minimizing the risk of data breaches. To that end, we recommend examining data security platforms for the following administrative-supporting and administrative-controlling features:

- Single interface with multiple, role-based views
- Segmentation of duties
- Multifactor authentication supported
- Privileged user access controls and audit logs
- Data flow visibility and control
- Guided data access policy creation
- Push-button policy evaluations and deployments
- Wide portfolio of compliance report cards and automatic alerts
- Multitenancy support to create smaller management domains

Flexibility in Leveraging Cloud-Native Capabilities and Licensing

IDC recommends that organizations examine flexibility from two angles. The first angle is cloud-native capabilities. In the cloud market, cloud providers are fiercely competing for customers, and one area of competition is in cloud-native security capabilities such as key management, encryption, data discovery and classification, privileged access management, and user access control. The cloud providers are certainly on the right trajectory in choosing to compete on security. According to IDC's December 2019 *Cloud Security Survey,* "lack of sufficient security tools" tied "advanced malware" as the top contributing factor to recent breaches in IaaS environments. Another contributor is misconfigurations; according to Verizon's 2020 *Data Breach Investigations Report,* configuration errors in cloud storage are increasing.

While customer acceptance of cloud-native security features varies, IDC contends cloud providers will continue to advance their cloud-native security features. Correspondingly, cloud-using organizations will appreciate flexibility to mix and match functionality from their cloud providers and with the functionality of their data security platform vendors.

In addition, bring your own key (BYOK) options offered through the data security platform allow organizations to retain control of their key material in protecting their data in cloud environments. For multicloud-using organizations, third-party cloud-neutral security platforms simplify operations by abstracting the unique security administration between the providers, provide consistent controls in hybrid environments, and enable higher levels of data portability because the encryption and data security policy can move between cloud providers.

The second angle of flexibility is licensing. If usage and new use cases are difficult for organizations to predict in advance, licensing flexibility can be a positive offset. For example, licensing flexibility to scale usage with protections from surges in fees and to expand use cases in a frictionless manner (e.g., a new licensing agreement is not needed) will benefit organizations experiencing difficulty in predicting future needs. In addition, licensing flexibility can be a low-risk/low-cost means to trial new platform capabilities.

IDC recommends that organizations add flexibility in managing cloud-native data security capabilities and licensing to their vendor evaluations.

Considering the Thales CipherTrust Data Security Platform

With a lengthy data security pedigree, Thales launched its CipherTrust Data Security Platform in September 2020. Centrally managed through the CipherTrust Manager, CipherTrust Platform integrates market-tested products spanning data discovery and classification, encryption, access control, tokenization, and key management. Recognizing that data security is a cyclical process, the platform offers CipherTrust Data Discovery and Classification to proactively scan and classify data, measure risk, and report on sensitive data that doesn't meet an organization's data security and compliance policies. A comprehensive set of remediation techniques can be selected from the same console.

Cloud environments, as documented previously, are rapidly expanding in data use and storage. The CipherTrust Platform provides customers with flexible options for operational consistency across multicloud environments. The CipherTrust Manager operates in public and private clouds as well as on premises. The platform delivers consistent cloud-neutral security across different environments and complements cloud-native security by scanning for exposed or out-of-policy sensitive data with CipherTrust Data Discovery and Classification. It also simplifies the management of encryption key life cycles of both BYOK and natively created keys that are used with cloud-native encryption in AWS, Microsoft Azure, Google Cloud Platform, IBM Cloud, and Salesforce with CipherTrust Cloud Key Manager.

CipherTrust Platform supports a multitude of customer use cases. CipherTrust Transparent Encryption is one of Thales' notable solutions because it delivers data-at-rest encryption, granular access controls, and data access logging to help organizations meet compliance reporting and best practice requirements for protecting data. For example, CipherTrust Transparent Encryption Live Data Transformation ensures zero downtime during encryption and conducts seamless key rotation. CipherTrust Transparent Encryption for SAP HANA secure HANA's Persistent Layer. CipherTrust Security Intelligence Logs streamline compliance reporting and accelerates threat detection in partnership with security information and event management (SIEM) systems. Other distinctive capabilities include Container Security, which supports policy-based encryption of data stored in containers. Efficient Storage provides strong data protection while maintaining storage efficiency techniques such as compression and deduplication. The Teradata feature provides high-performance encryption for Teradata databases.

In addition, CipherTrust Transparent Encryption provides transparent server-based encryption of data stored in AWS storage, including AWS S3 buckets, closing one of the cloud industry's most common security gaps. The product also applies granular access controls based on access initiator (e.g., user or application), requested operation (e.g., read or write), when access is requested, and resources engaged (e.g., directory, files, drives, devices). An example of applying this capability is privileged user access control, where a root user could be allowed to do his/her job functions on files and databases without ever being able to see the data in clear text, hence thwarting insider threats and malware.

The platform's extensive customer use case support has allowed customers to expand their adoption of CipherTrust capabilities as their needs warrant. With use case expansions orchestrated through the centralized CipherTrust Manager, administrators are not hampered by having to learn the nuances of another administrative interface. It also creates a consistent data security environment across multicloud, hybrid cloud, hosted, remote, and traditional datacenter environments.

The CipherTrust Platform is a well-rounded data security solution that should perform well against our recommended evaluation criteria. It bears repeating that Thales isn't new to the data security platform market. The CipherTrust Platform is a next-generation data security platform that leverages a lengthy history of serving customer data protection needs and supports currently deployed Vormetric and KeySecure products.

The CipherTrust Platform is a next-generation data security platform that leverages a lengthy history of serving customer data protection needs and supports currently deployed Vormetric and KeySecure products.

Challenges

The challenges facing Thales are not unique to the company; they apply to all vendors of data security platforms. First, some customers may be concerned with overreliance on a single vendor (i.e., vendor lock-in) and may fear not all pieces of Thales technologies will innovate at the same pace as point products. However, Thales can counter with its history of innovation, which includes field-proven solutions from SafeNet and Vormetric. Moreover, the invisible hand of competition compels the company to innovate and maintain a comprehensive and growing list of technology partners and integrations. On price, Thales and other platform vendors will appropriately cast contract negotiations in terms of the operational savings that accrue from a unified, functionally broad platform that supports numerous use cases. Moreover, with an extensive customer base, Thales will be pushed by its customers to continue designing more out-of-the-box solutions for new customer use cases.

Second, cloud-native data security features can have a powerful influence on cloud-only organizations that have standardized on a single cloud provider. While this circumstance exists, organizations operating in multiple clouds are more prevalent and introduce complexity in managing all data security functions, such as life-cycle key management, uniformly. Plus, Thales can make a separation of church and state argument to customers along the lines of using cloud providers for infrastructure and application services while protecting their data assets through an independent third party.

Conclusion

While the future is never fully predictable, the trends of hybrid and multicloud environments are strong and further strengthened as organizations reflect on the lessons learned from the COVID-19 pandemic. As organizations spread their digital footprints outward both to clouds and with a more distributed workforce, orchestrating consistent data security practices through an assortment of products from multiple vendors is costly. This fragmented approach is neither sustainable, as flexibility becomes a more significant and painful casualty, nor advisable, as end-to-end visibility suffers and the risk of administrative errors and oversight increases. In addition, operational complexity in security benefits threat actors. A confused or distracted opponent is easy prey. IDC's advice to organizations is to start evaluations of data security platforms as soon as possible. Your data is one of your most treasured assets and should be protected as a treasured asset. Otherwise, your data assets could become someone else's treasure.

About the Analyst

Michael Suby, *Research Vice President, Security and Trust*

Michael Suby is a Research Vice President in IDC's Security and Trust research discipline. In this role, Mr. Suby concentrates on endpoint security and, in collaboration with IDC team members, engages in a wide and evolving spectrum of security and trust topics.

MESSAGE FROM THE SPONSOR

About Thales

Today's enterprises depend on the cloud, data and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored – from the cloud and data centers to devices and across networks. Our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day. To learn more about the Thales CipherTrust Data Security Platform visit ***https://cpl.thalesgroup.com/encryption/data-security-platform***.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
5 Speen Street
Framingham, MA 01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com