Enterprises Reveal Data Security Priorities

New survey finds most security deployments follow container-level, rather than more secure data-level, approaches to encryption. But enterprises understand at the highest levels that data security is critically important. Taking a proactive strategy will reduce corporate risk and also protect brand and reputation.

The enterprise attack surface continues to expand. Network borders are evaporating as data scatters across cloud, mobile, remote, and partner and other third-party environments. Multiple entry points into the network have appeared, prompting sophisticated data thieves to unite globally and create profitable data-theft businesses.

How are companies coping? IT leaders are aware of both the new risks and the role of data-centric encryption technologies in mitigating those risks, according to a March 2016 survey by IDG Research Services. At the same time, however, many seem overwhelmed by the shifting security environment. They admit they haven't progressed sufficiently toward fully embracing data-level protection as a path to safeguarding data in its various states—at rest, in transit, and in use.

Protecting Data at Rest Is Top of Mind

According to the IDG survey respondents, the enterprise is directing most of its energy and budget into container-based data security and protecting data at rest, such as data stored in a database (Figure 1).

Nearly three-quarters (72%) of respondents ranked securing data at rest as "critical." By comparison, just half (50%) said they consider protecting data in transit across a network critical, while a higher percentage (57%) said protecting data in use (application data) is a top priority.

The problem is, sensitive data that is not protected and is in use by applications, analysts, business process users, and data scientists, is highly vulnerable to cyber-attack. Industry experts have shown that data residing in an application or moving across a network is more vulnerable to external theft. Some reports indicate that more than 80% of data breaches happen at the application level.

There's good news: The survey findings appear to paint a picture of an enterprise security landscape in transition as businesses scramble to build in data security that enables business transformation objectives and compliance with increasingly stringent data privacy requirements. For example, enterprise awareness of data protection and encryption benefits is high (Figure 2). But while more than three-quarters (76%) of respondents associate data encryption with mitigating data breach risks, more than half (52%) also associate it with protecting data in new platforms (cloud, mobile, big data), and exactly half (50%) associate it with compliance to industry security mandates.

Simply put, encrypting at the data level (more granular than a container approach) is key to protecting data at rest, in transit, and in use.

How Enterprises Secure Their Data

How are enterprises securing their data today? Most respondents said they protect data at the whole-disk

Fig. 1. Data Protection Priorities Rated 'Critical'

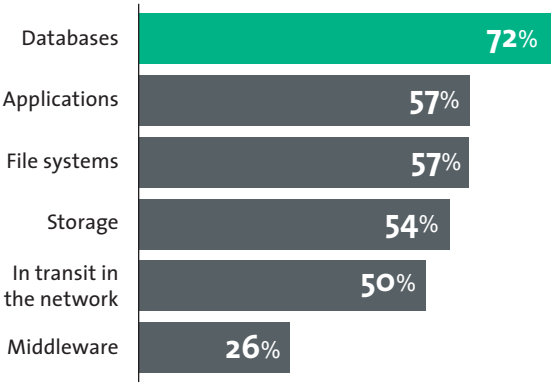
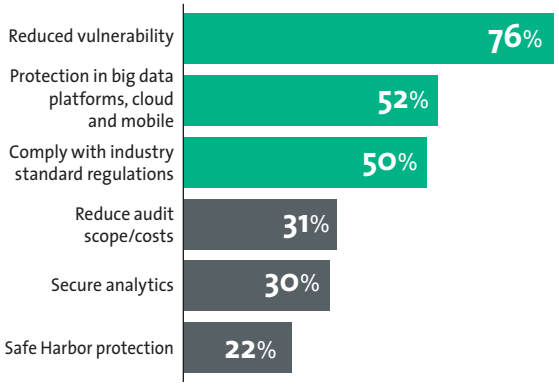


Fig. 2. Benefits of Data Protection & Encryption



Source: IDG Research Services; Base: 54 qualified respondents

IDG

Hewlett Packard Enterprise

level (56%) and at the database (50%) and file (48%) levels. All of these are container approaches, however, that don't account for the fact that data doesn't stay in one place. Gaps can crop up between protected data containers when data moves. In contrast, encrypting at the data level protects the data regardless of what state the data is in and where it is located.

Survey respondent Joel Rosenblatt, director of network and computer security in the Columbia Information Security Office (CISO) at Columbia University in New York, explains it this way:

> *"Almost all compromises start out as phishing in some form—getting someone's credentials and using them to access data. The stolen corporate data leaves your database using the encryption you have in place, preventing you from seeing it leave," he says. "[But if] the data is FIELD-encrypted, someone can steal the entire database but will be unable to read the good stuff (the fields that you have encrypted). This is not easy to do, but it will provide real security for your data, not 'check box' security."*

Interpretation and Recommendations

Some enterprises might stick with familiar security approaches at the expense of protecting against new risks. This is borne out by the survey results, which show a current emphasis on container-based approaches.

Yet "the ability to support a changing environment" was the second biggest obstacle to security cited by respondents (46%) after difficulties with long-term security management (57%). And today's security landscape requires newer technologies that mask sensitive information by replacing the original data with an encrypted value or a random token.

Tokenization and format-preserving encryption (FPE) are two such approaches. Both involve replacing the original data with an encrypted value or a random token. For example, AES-FPE takes traditional Advanced Encryption Standard (AES) encryption much further, however, by keeping data formats intact; few or no changes to database schemas and applications are required, and no formatting conversions are necessary when the encrypted values move from mainframes to open systems. Only 15% of respondents said they are using FPE, however, perhaps because it is so new.

Stateless key management is an FPE-related technology that securely derives keys on-the-fly. This approach reduces IT costs and eases management burdens by eliminating the need for a key database and the corresponding hardware, software, and IT processes required to protect the database continuously or the need to replicate or backup keys from site to site.

Glossary of Encryption Terms

- **Database-level encryption**—Granular encryption within a relational database at the element level, such as a column or field.
- **Data-level, format-preserving encryption (FPE)**—A method of encryption at the field or sub-field level, to preserve structured and semi-structured data by encrypting a plaintext of some specified format into a ciphertext of identical format. Some FPE approaches will also preserve logical value of the data such as referential integrity, and date ranges.
- **Data-masking**—Hiding original data with random characters or data in a field to protect sensitive data.
- **File-level encryption**—Encryption of individual files or directories by a file system.
- **Tokenization**—Process of substituting a sensitive data element, such as a credit card number, with a non-sensitive equivalent, referred to as a "token," that has no extrinsic or exploitable meaning or value.

Tokenization is highly publicized by the Payment Card Industry (PCI), which has strict customer information protection requirements, and 30% of respondents said they were using this method. A newer form, called stateless tokenization, precludes having to store highly sensitive customer and other data in a database, randomly generating tokens that have no relationship to actual personal account numbers. The PCI considers tokenized data systems out of scope; not having tokenized systems audited by PCI reduces compliance requirements, complexity, and cost for the enterprise.

Conclusion

Security risks and solutions have grown multidimensional, and new rules apply when data spills over corporate borders into the cloud and data lakes, and onto mobile networks and public Internet connections. Encrypting data at the data level keeps it safe regardless of what state it is in and where it moves.

Instituting new encryption processes enterprise-wide can be daunting, so experts recommend starting with the most sensitive data, and then prioritizing data that is the most valuable. This will help you develop a framework to address all your data platforms, applications, big data and Internet of Things (IoT) networks, payment-processing devices, and cloud services with format-preserving encryption and tokenization technologies.

Learn more at **www.hpe.com/software/DataSecurity**

About the study

IDG Research Services conducted a Quick Poll in March 2016 to determine how companies are coping with their security challenges, data protection priorities, and solution adoption plans. The study involved 54 IT professionals across a wide cross-section of industries and company sizes.