Data Security Trends

Companies are increasingly focusing on encryption, database monitoring, and data leak prevention systems for protecting sensitive data.

Hewlett Packard Enterprise

There's growing acknowledgment among security researchers and practitioners that it is next to impossible for enterprises to block all attacks that are directed at them. Given the highly persistent and targeted nature of most modern cyberattacks, many believe a data breach is almost inevitable for most organizations. The reasoning goes that no matter how well protected you are, a determined enemy will always find a way to slip past your perimeter simply because modern networks are so large, complex, and interconnected that it's almost impossible to consistently keep every single entry point secure all the time.

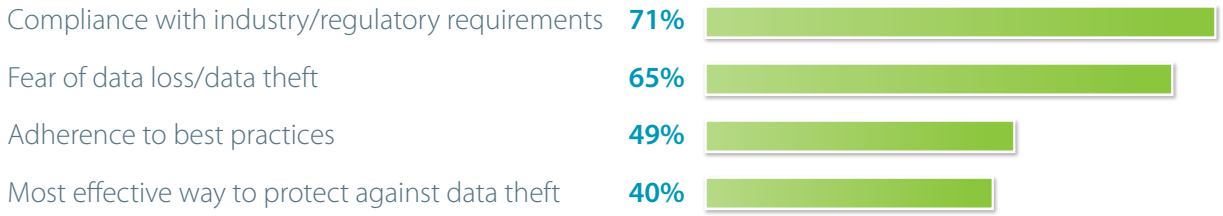
Consequently, there's a greater focus on technologies like encryption, database monitoring, and data leak prevention systems for protecting sensitive data. Rather than relying solely on tools for preventing access to sensitive data, the effort is to mitigate damage if attackers do manage to find a way to access the data.

In many cases, data protection efforts are being driven by regulatory requirements. For instance, 129 respondents to an October 2015 UBM Tech survey of 185 business technology professionals at medium and large companeis pointed to regulatory compliance as the primary driver of their data protection efforts. But that's not the only reason.

For 65% of the respondents, it was fear of data theft and data loss. Another 49% said their data control efforts were spurred by a desire to adhere to best practices, while 40% said it was the most effective way to protect against data theft.

Data protection tools come in various forms and capabilities. Encryption continues to be the most common and widely recommended approach for protecting data. Numerous data protection regulations and industry standards like PCI DSS even require organizations to encrypt data while both at rest and in motion. The rules typically provide a safe harbor for organizations that implement data encryption.

Despite this, many organizations continue to drag their feet on encryption, often with disastrous consequences. For instance, over 80 million Social Security numbers were exposed when attackers managed to gain access to a database belonging to health insurer Anthem Inc. that stored the data in unencrypted form[1]. The company is not the



What has been the biggest driver(s) of data-level security efforts at your organization?

Note: Multiple responses allowed

Data: UBM Tech survey of 185 business technology professionals at companies with 500 or more employees, October 2015

only one guilty of such an omission.

Not very surprisingly, encryption was the most favored data protection control employed by respondents in the UBM survey. A total of 60% of the organizations represented use encryption to protect data in transit from point to point, while 54% said they use encryption to protect data at rest. Both numbers are somewhat higher than expected given the number of recent data breach incidents that have involved unencrypted data.

Even so, it means more than four in 10 organizations have sensitive data stored in an unprotected manner in their databases and are transmitting the data in an unprotected fashion. The exposure that organizations face from this continued failure to encrypt data cannot be overstated. Many consumer class-action lawsuits filed against organizations that have suffered data breaches have invoked a lack of encryption as a sign that the organization had not adhered to recommended security best practices.

Encryption is just one of the options available for protecting data. Other approaches include database activity monitoring tools, data leak/loss prevention systems, and tokenization. Each of these technologies works in different ways to protect data from inadvertent or malicious exposure.

For example, database monitoring tools keep an eye on all activity at the database level and issue alerts on unexpected changes, additions, deletions, or access. The tools have been around for well over a decade and are often considered a critical component of a company's compliance profile.

Data loss prevention products work by monitoring network traffic for data elements, like Social Security and credit card numbers, and alerting administrators when prohibited data attempts to egress a network. DLP tools are often used to monitor for insider abuse but can play a vital role in monitoring for data exfiltration by cyberattackers.

Tokenization is an approach in which a credit card number, SSN, or any important bit of data is replaced with a token comprising a randomly generated number or alphanumeric characters. The token acts as a surrogate for the actual number during all transactions, thereby protecting the number or data element from risk.

Our survey showed organizations using all of these technologies to varying degrees. For instance, 49% of the organizations

43%
Respondents who plan to increase spending on data protection tools

surveyed use database monitoring tools to protect data, making it the second most widely used product in this category after encryption. Slightly less than half (46%) of the respondents are using DLP products to protect against malicious and inadvertent data leaks, while 31% said they use tokenization.

With enterprises increasingly using cloud services to host their applications and data, cloud encryption gateways have emerged as another key component in enterprise data protection strategies. About 29% in the UBM survey said they rely on cloud encryption gateways to protect their data in the cloud.

The numbers present a somewhat mixed picture on enterprise adoption of data protection technologies. On one hand, companies appear to be using a fairly wide spectrum of products to protect sensitive data from compromise. On the other hand, only a relatively small proportion are making the effort to do so.

One glimmer of hope comes from the spending plans that companies have for data protection tools. The proportion of respondents who plan to increase spending on data protection tools (43%) is greater than those who said spending will remain the same over the next 12 months (33%). Only 6% expect spending for the category to fall in the next year.

[1] *http://www.wsj.com/articles/investigators-eye-china-in-anthem-hack-1423167560*