

The Data is the New Perimeter

Data-centric security offers the best defense against advanced persistent threats

Overview

There's no question that technologies keep getting better. The trouble is, so do hackers. Regrettably, they often get better faster than the good guys.

This is the reason data breaches have become an unfortunate reality of modern business. The sheer volume and reach of many breaches bear testament to the fact that all kinds of sensitive data—particularly information that can be monetized quickly—have already been compromised or stolen outright.

Out of this environment came an emerging breed of cybercrime that's particularly worrisome. Sometimes referred to as advanced persistent threats, these assaults don't just build on the growing sophistication of hack attacks in general; they play specifically to the information environment as it now exists. While often massive in scope, they lie dormant within the infrastructure until the target is most vulnerable. And what they target is not the technology but the data—specific, high-value data, such as files with employees' personal information, customers' addresses and payment details, legal contracts, design schematics and operational plans pertaining to IP and trade secrets.

Most companies place a high premium on IT security, and believe they have ironclad protection. However, the toll from cyber-attacks continues to climb. That's because there are gaping vulnerabilities in the way defenses are deployed—firewalls, endpoint security and even protected storage can all be bypassed by attackers. The dirty little secret (that most vendors never want you to know) is that with just a little effort, sensitive data can be breached.

Consider this in the context of a different kind of criminal history. While bank robberies have always fired up the public imagination, the most effective thefts seldom occurred inside the bank; Dillinger-like exploits aside, the vaults were usually too secure. Instead, smart criminals waited until the money was out in the open, such as at tellers' windows or being hauled to armored trucks.

Perimeter Security

It's not a stretch to say that many companies still make the same mistake—they focus security strategies on the vault rather than the cash. As before, many favor the approach of building a perimeter around the data—on servers, desktops, laptops, pipes and packets. However, as any CEO will attest, the rapid adoption of cloud and mobile computing, along with the overall consumerization of IT, has caused those perimeters to become fluid, even nonexistent. The data that the bad guys want is now all over the place, from the biggest servers to your iPhone.

But here's another cinematic image: Many banks use dye-protection packs that explode and stain the cash once it's stolen, making it worthless. Imagine doing this to your data—basically, ensuring that even if it gets breached, it will be worthless to the criminals.

That's the essential logic behind a 'data-centric' strategy. In this scenario, the data is protected end-to-end using encryption—regardless of which channels it goes through or where it reaches. It can be accessed only by the intended party and no one else.

This isn't easy: encryption techniques typically rely on long, randomly generated keys, and the process is complex, time-consuming and expensive. However, not all encryption is created equal. There's any number of encryption solutions available, but many bring their own

problems. For example, database encryption only protects data when it's 'at rest'; network data encryption only protects the data when it's between two points of a network. Those using PKI require high operational costs in key management, and are not easily sustainable. Putting in a mix of solutions, meanwhile, can add vulnerability, bring greater complexity, and increase costs without adding scalability.

Key Innovations in Encryption

However, there are now alternatives that are accessible and affordable. Voltage Identity-Based Encryption™ (IBE) takes a completely new approach by using any arbitrary string as a public key, enabling data to be protected without the need for certificates. IBE is stateless and dynamic, as well as easy to use, scale and distribute. It's also efficient at generating and managing keys to scale when sharing unstructured data without the cost of PKI, or Public Key Infrastructure.

The underlying principle here is Stateless Key Management, which represents a major advance by effectively allowing keys to be generated on the fly, derived only from identity information that's already available, such as your email address.

Stateless Key Management is transparent and easy to manage because, from an IT operational standpoint, there's no database to manage. It also works nicely with existing business processes, like electronic discovery and recovery. It's easily compatible with business processes, retains the protection from mainframe to mobile, and goes a long way toward ensuring compliance.

Voltage Format-Preserving Encryption™ (FPE) offers a fundamentally new way to encrypt structured data, such as credit card number or Social Security Numbers. Encrypted data retains its original size/length and format, and, as a result, organizations don't need to make time-consuming modifications to applications or database schemas. This approach makes it possible to integrate data-level encryption everywhere, even legacy business application frameworks, overcoming a hurdle that was previously insurmountable. (FPE is a mode of standard AES, recognized by NIST.)

It's essentially counter-intuitive for corporations to plan for a breach; the thinking is always to prevent attacks rather than prepare for the aftermath. But it's exactly the right philosophy in an environment where many financial services providers have data that, in the wrong hands, is worth more than all of history's greatest bank robberies combined.

The Three Tenets of Information Security

- **Follow the data:** While everyone acknowledges the value of encryption, not all encryption mechanisms are created equal. A data-centric approach that renders stolen data useless to the thieves, regardless of where it's breached, should be the first line of defense.
- **Keys to the kingdom:** The best security solutions have keys that are never stored per se; they're computed only as needed, so they can't be stolen. (The recent RSA SecureID breach shows how the bad guys are getting more sophisticated in going after keys.)
- **Take the target sign off your back:** Cyber criminals look for the highest reward with the lowest protections. If all they get from you is encrypted data, they'll go elsewhere. Data-centric security, built around Format Preserving Encryption (FPE/ FFX), encrypts digital assets in such a way that they remain encrypted wherever they go. Just like dye-stained cash, FPE/FFX turns gold into straw. And that's a sweet victory.

Enterprises that have been at the receiving end of criminals' attention know the difference this security strategy can provide. "Every single breach I know of wouldn't have happened if our end-to-end encryption solution had been there," says Bob Carr, CEO of Heartland Payment Systems, which suffered a severe data breach a few years ago and has since transformed its security structure with a data-centric approach.

Imagine a scenario in which cyber-criminals deploy resources worldwide to penetrate a network and retrieve the data. Then they find the data is worthless, essentially gold turned into straw. That's what end-to-end encryption within a data-centric security strategy offers.

ABOUT VOLTAGE SECURITY

Voltage Security®, Inc. is the leading data protection provider, delivering secure, scalable, and proven data-centric encryption and key management solutions, enabling our customers to effectively combat new and emerging security threats. Leveraging breakthrough encryption technologies, our powerful data protection solutions allow any company to seamlessly secure all types of sensitive corporate and customer information, wherever it resides, while efficiently meeting regulatory compliance and privacy requirements

For more information, please visit www.voltage.com.

v02-22-2013