Voltage security

EXECUTIVE VIEWPOINT

Sathvik Krishnamurthy

PRESIDENT AND CEO, VOLTAGE SECURITY

Sathvik Krishnamurthy has more than 20 years of software industry experience and has been president and CEO of Voltage Security since 2003. At Voltage he led the effort to create one of the fastest growing data encryption companies in the world, with over 1,000 customers across a wide variety of industry segments.

Data-Centric Security Against Tomorrow's Threats

How have data and data management evolved, and why is it important to today's enterprise IT?

I don't think anyone 20 years ago could have predicted the explosion in the amount of data that is available at everyone's fingertips today—specifically across enterprises but also flowing all the way up from and down to the consumer. And because of legal compliance requirements, more and more data is accumulated, despite the fact that getting sensitive data out of your system is a way to start reducing risk. Then you look at the ways organizations are dependent on this data to function, and you quickly see that it's the lifeblood in most of today's businesses.

Give some examples of new kinds of data breaches.

The modern attack these days is getting in through what are referred to as zero-day mechanisms, meaning that no amount of perimeter defense can prevent them. They are malware attacks that can steal the credentials of a valid user and make their way to the internal networks via techniques such as spear-phishing, SQL injection, or rogue USB storage devices. Once they're on the network, they can inherit the permissions of a trusted user and find their way over to more important assets.

Why doesn't the traditional approach of data protection work?

The conventional approach is to create moats around your castle to keep out unwanted intruders. In IT terms, these moats are firewalls and smart screen filters. The problem is that people are exchanging data in the clear with a wide variety of business partners in a variety of ways—mobile, cloud and outsourcing—in spite of the information security risks. So the traditional approach of setting up barriers to prevent infiltration is not even relevant to these data flows.

Explain the data-centric approach.

From the very first point of entry, the data, structured or unstructured, is encrypted. As it is used across data centers, public and private clouds and mobile devices—in use, in transit, or at rest—it remains encrypted. That's important because in the event of a breach, the theft of data is minimized. It makes the cost of mounting an attack much, much higher.

What does Voltage do to support the data-centric approach?

Voltage technology, including Voltage Format-Preserving Encryption ™, Voltage Identity-Based Encryption ™ and stateless key management, provides a single platform with data-centric encryption and tokenization that accommodates business processes consuming both structured and unstructured data. This platform helps our customers protect their data and files in a variety of ways, including in production data centers and public clouds, QA and preproduction environments, on desktops and mobile devices, across the payment processing cycle, and among employees, partners and customers. We have top executives in the biggest banks in the world who say the cost of ownership, time to deployment and a short time to realize a return on investment—even on mission critical legacy infrastructure such as the mainframe—are key criteria for choosing Voltage Security. Our stateless key management approach brings a reduced TCO as there is no need for data replication across data centers, and it greatly simplifies disaster recovery and overall architecture. It also lets our customers scale exponentially to accommodate business needs, and embrace data-level security in and out of the cloud.