Global Technology Company Offloads Data Security to ShardSecure, Reducing Overhead and Improving Performance

A global technology company had deployed an expansive security surveillance management system to enhance campus protection around the world. The solution is effective in strengthening the company's overall security posture and physical safety. Now the company's chief concern, from a threat perspective, is preventing nation states and organized crime from obtaining proprietary video and data to launch attacks or for cyber espionage. However, the cost and performance impact to encrypt their streaming CCTV and IoT device data would take a heavy toll. The company turned to ShardSecure and its patent pending Microshard™ technology for a better solution.

CHALLENGES:

A compromised surveillance management system can become the eyes and ears of a malicious actor without the trouble of them gaining physical entry. The system is capable of capturing information shared during formal meetings, casual hallway conversations, on computer screens, and even hardcopy documents, as well as exposing the comings, goings, and routines of key individuals. This creates a treasure trove of sensitive data, including company confidential information, intellectual property (IP), and personal information. Storing and securing data at rest and ensuring it is protected in the event of a compromise is critical for physical safety, data privacy, and IP protection.

It was clear that the surveillance system needed to be protected, but the idea of encrypting this data was deemed unsustainable for two, main reasons:

Performance impact. The organization's surveillance system consisted of thousands of application servers and tens of thousands of CCTV cameras worldwide. The performance impact of enabling encryption for all surveillance data and video would have been staggering. The estimated impact was a 30%-40% performance degradation. Latency this severe was simply unacceptable, and further investment in software and hardware would have been required to compensate for the performance loss.

Expense to encrypt. The company's expense to compensate for the performance impact of encrypting this data would have included: hardware to host hundreds more application virtual machines, application server licensing fees for each virtual machine, and the operational expense associated with managing the expanded complexity of the application, itself, and the key management infrastructure.

SOLUTION:

The company decided to offload the data security function to ShardSecure to optimize performance and reduce overhead resulting from the data generated by the surveillance management system. ShardSecure's Microshard technology is a three-step process that consists of shredding, mixing, and distributing data across multiple storage repositories, and protects data by making it unintelligible and unusable in the wrong hands.

- **Shred:** Microsharding begins by "shredding" files into microshards, which effectively removes the sensitivity of the data. Microshards are typically too small to contain a complete birth date, ID number, address, or other kinds of sensitive data.
- **Mix:** Microshards are mixed across multiple containers along with poison data to make it more unintelligible to unauthorized users.
- **Distribute:** The containers are distributed across multiple, segmented storage repositories of your choosing — multi-cloud, multi-region, or hybrid cloud. Unauthorized reassembly of the microsharded data is virtually impossible.

OUTCOMES:

The company realized several benefits by innovating the way they secure data.

Cost savings. The company estimates dramatic reductions in hardware, software, and power consumption resulted in a total cost savings in the high six figures. They can deploy one ShardSecure virtual appliance cluster in the cloud or datacenter, instead of hundreds of additional virtual machines. And ShardSecure's Microshard technology continuously works in the background to protect data with no need to manage encryption keys and only minimal administration support.

Seamless performance. ShardSecure disassembles and reassembles Microshard data in parallel, as opposed to buffering, which virtually eliminates latency. During investigations, data and video can be moved actively from the datacenter to the cloud for collaboration and analysis with no impact on availability.

Data privacy and physical safety. ShardSecure helps protect data, IP, and personal information by making the company's data incomplete, unintelligible, and of no value to unauthorized users. The company can store larger quantities of data, confidently knowing they are not expanding the attack surface or risk exposure. And with Microshard technology, the security team eliminates the worry and risk of keys being lost or compromised.