The Real Story on Encryption in the Cloud

By FedScoop Staff

The federal government has moved to the cloud faster than anybody expected. In some cases, the government has outpaced its commercial counterparts in cloud adoption.

According to a recent survey by Thales and analyst firm 451 Research, nearly half of federal agencies used more than five infrastructure-as-a-service (IaaS) vendors and more than 100 software-as-a-service (SaaS) applications. But with this transition several concerns have also been raised, including the increased number of vulnerabilities stemming from shared infrastructures; security breaches in the cloud; and the complexities surrounding custodianship of encryption keys.

IT security spending in government is on the rise and most agencies are pushing their security dollars toward endpoint and network security. Yet despite the concerns about data security — particularly around insider threats, stolen credentials and advanced persistent threats — few agencies are taking full advantage of modern, centrally managed encryption capabilities to secure their data in the cloud.

"What holds agencies back from using IaaS oftentimes is the sensitivity of the data," said Brent Hansen, Thales' federal chief technology officer. "But if you can bring your own encryption to IaaS, that's the real value of what transparent encryption and access control provides.

Whether it's standing up databases, applications, containers, or analytic workloads, if it's IaaS, we've got your encryption covered."

Breaking the encryption myth

The federal government's hesitancy in embracing encryption is not totally unexpected and the myths surrounding encryption remain alive and well.

"When people think encryption they think 'oh, it's going to kill performance, it's going to be complicated and it's going to break everything in my application stack,'" said Hansen. "That's an old-school mentality. It's 2018. We've alleviated all of those concerns."

According to Hansen, the myth of the encryption-performance hit persists because everyone in security has failed at least once or twice with an encryption service. But Thales' ability to work at the kernel level enables the company to sidestep the traditional performance downsides of using encryption.

"Encryption is math," Hansen said. And in the past that processing had to take place on the server's main CPUs to the detriment of all other tasks. "For performance, we offload to the crypto hardware acceleration that's already built into the motherboards of every server that has been manufactured in the last five years," he said. "You're taking the encryption load off of the CPU and that's what gives us our single digit performance."

The finer points — data encryption key management

There's another potential downside to encryption that has scared off its share of federal IT security professionals: key management. The keys that are used for data encryption, regardless of the specific encryption technique, have a lifecycle … much of which is driven by regulatory compliance.

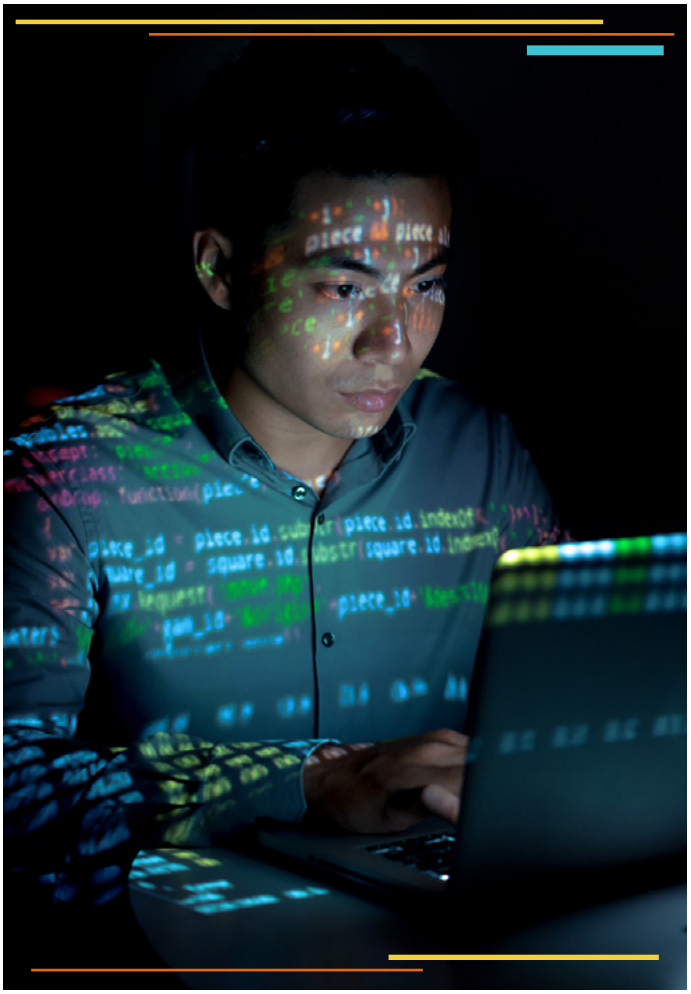
For example, the payment card industry (PCI) requires data encryption keys (DEKs) to be rotated on a relatively frequent basis (typically every 24 months). The impact of rotating DEKs can be significant, possibly even resulting in application downtime.

But managing encryption keys can quickly become a nightmare — if you let it.

Encryption keys can be easily abused depending on the permissions you extend to a cloud provider, Hansen said. "If I'm a developer or a database administrator, I'll just create my own key vault and create keys for whatever I need. Then, the next thing you know you have an 'n-to-many' relationship of people who can create keys and use them, and that compounds into [multiple] key vaults and there's just no insight" he said.

"It's very easy to have a 'wild, Wild West' situation when it comes to key management in the cloud."

"It's very easy to have a 'wild, Wild West' situation when it comes to key management in the cloud," said Hansen. "And it gets even more complex when you have multiple clouds."



Such a mentality also opens up the agency to potential insider threats, said Hansen.

"When you are putting data in the cloud you are trusting administrators with the most important thing you have," he said. "How do you know internal cloud administrators are not looking at your data? Cloud insider threat is a real attack vector that you can protect yourself from if you are the owner of encryption keys."

Some have argued in favor of self-encrypting hard drives. But, as Hansen points out, that will only protect against physical theft. "Each storage controller has a key that encrypts the disk. When it turns on, that key accesses information and anyone [in possession of the device] then has access to information. This builds a false sense of security," he said. And if you take steps to store the key elsewhere, you need to know where that key is stored and how to access it, he said.

Others, like Oracle, Microsoft and IBM, have offered transparent data encryption modules.

Although they are bringing some native encryption to the table, agencies still have to store the keys outside the system. To be fair, those companies are not encryption companies. And while it may seem like a free value-add to a contract, there will likely be added key management and storage costs. Likewise, those encryption modules will not be able to provide data or analytics on effectiveness.

But the way Thales does key encryption with access control gives agencies a double control around data encryption. Bringing your own encryption to the cloud not only protects data at rest in the cloud, but gives agencies the ability to impose access controls to protect sensitive data from insider threats.

"You can reduce insider threats by orders of magnitude if you eliminate the task of decrypting data from all administrative accounts."

"You can reduce insider threats by orders of magnitude if you eliminate the task of decrypting data from all administrative accounts. This by no means compromises their ability to do their jobs," Hansen said.

The power of a centrally-controlled encryption management service in this context is clear.

It offers:

1. Superior data protection and reduces the risk of catastrophic data losses
2. Greater visibility and insight into user and administrator access to agency data while helping identify potential insider threats
3. Increased ability to manage data across multiple cloud and on-premises IT environments and,
4. Greater assurance that encryption practices align with federal security standards and regulations.

Click here to learn more about data encryption keys and management services.

This article was produced by FedScoop for, and sponsored by, Thales.

fedscoop THALES