Security focus shifts to the edge

As government agencies adapt to more-remote operations, new data security strategies are needed

Effective data security has always meant anticipating the next "new normal." Staying ahead of potential problems in the uncertain conditions of 2020, however, has been an epic challenge.

The pandemic-induced pivot to "maximum telework" also produced new work challenges, and brought a new urgency to rethinking data security. Previously unseen vulnerabilities became daily problems, insider threat risks multiplied, and insufficient data access controls became glaringly apparent.

"All of those remote devices, remote offices, remote laptops—the secure devices that you've been maintaining for a long time—have information on them," explained David McCarty, Hitachi Vantara Federal's Data Intelligence Business Lead. With the shift to remote work, he said, "your data is probably sitting on a laptop, on a mobile device, sitting in someone's Web browser cache … it's all being stored and maintained outside of your network."

"What you want to be able to do," he said, "is own that information and be able to push it, manage it, audit it and control it at all levels"—regardless of where it resides.

The answer, said McCarty, is a hybrid cloud architecture that allows the organization to pivot its security focus "from the data center to the edge"—with the edge defined by the mobile devices and access routers used by remote workers to access and transfer data.

Hitachi's solution is the Hitachi Content Platform and its file sync-share application HCP Anywhere, which allows access on any mobile device and is back-ended by true object storage.

The result is to effectively move and shore up security boundaries for the new normal of mobile devices and widescale telework. "Extend the boundaries of the digital workplace to provide timely access to relevant data across geographies or in the cloud," McCarty said. "Drive higher productivity, centralize data management, replace traditional NAS storage, and enable real-time data protection."

In nuts-and-bolts terms, HCP Anywhere is sync-share technology that is plugged into an on-premises cloud. It allows users to scale, is easy to manage, supports legacy and contemporary protocols like FTP/SIS, SMTP, WebDev, REST, S3 and others, and is built on commodity architecture.

Although most organizations had data security plans in place for some level of remote work, few were prepared for the scope and duration brought by the pandemic, and the cost-benefit calculus has shifted.

The right data security strategy will help public and private sector organizations comply with existing regulatory requirements, such as FISMA and TIC, even as their operating environments change dramatically.

"Having a cloud entity on-premises and also accessing cloud governance inside a public or controlled cloud is really the best option," said McCarty, noting that it is not just Hitachi and other private cloud entities that are moving to a hybrid cloud approach, but also the largest public cloud service providers.

"Having a cloud entity on-premises and also accessing cloud governance inside a public or controlled cloud is really the best option."

– DAVID MCCARTY, DATA INTELLIGENCE BUSINESS LEAD, HITACHI VANTARA FEDERAL

Where and how can a CISO start to approach such a transformation? "I always recommend a discussion first to make sure that this is something you're ready to do," said McCarty. "This isn't drop-and-replace kind of technology. Start at the very smallest pieces, the gigabyte/terabyte level, have a few users test it, then ask: 'Is this something we can employ? and 'How simple is it to adopt?'"

Hitachi Vantara is working with a large organization that has already transformed its file sync-share completely to this architecture in the wake of the pandemic. The organization had been in the testing phase when the pandemic hit, realized it had a ready solution based on positive feedback and results, and was able to move quickly to adoption. "Instead of using unsecure devices and then trying to figure out how to secure them on the back end," McCarty said, "they are getting a secure device in place already," and then start to open up the avenues to different applications.

"This is a long discussion, but the tools are there. You can adopt quickly by taking small steps and then starting to expand it."

Article Source: Public Sector 360 Workshop: Tools and Tactics for Better Telework | June 3, 2020