Adapting Cloud Security and Data Management Under Quarantine

With remote operations in place, organizations face mixed IT environments that could raise new concerns as they maintain operations.

The necessity of teams working remotely while under lockdowns can put new strains on data management and security even in the cloud. Whether an organization previously established a cloud-based infrastructure or is accelerating a migration plan, the shift to remote operations opened the door for additional considerations IT leaders must deal with. Data management company ZL Technologies and enterprise cloud computing company Nutanix shared their perspectives on what has changed for cloud security and data management under changes brought on by the pandemic.

The mass movement to work from home has introduced a variety of new security concerns, says, Kon Leong, CEO of ZL Technologies. His company works with financial institutions such as Citibank and Wells Fargo, as well as automakers Honda and Toyota. Kon says organizations in these times must pay special attention to security above the network layer, particularly in the application and content layers, to watch out for internal threats. The trouble is, an internal threat may already be authenticated and authorized to operate within the system. “How do you manage against bad players on the inside?” he asks.

Image: WrightStudio - stock.Adobe.com

Analyzing data as well as who has access to it can help pin down who the bad actors might be, Kon says. Such a task can be difficult since the data is typically in silos. Regulations such as Europe’s GDPR (General Data Protection Regulation) and the CCPA (California Consumer Privacy Act), treat data as data regardless of silos, Kon says. Such regulations can compel organizations to make data available in one location and easily deleted on command. “They don’t give a damn how many silos you have,” Kon says. “That’s the elephant in the room no one’s really addressing.”

The spread of COVID-19 may have accelerated cloud adoption, but it happened in a fragmented, piecemeal fashion, Kon says. “In the next six months, I think you’ll see a more organized migration.” He anticipates a massive convergence between analytics and governance obligations will also take place.

The current state of affairs is not something envisioned by many business continuity plans, says Wendy Pfeiffer, CIO of Nutanix. Most organizations are operating in a hybrid mode, she says, with infrastructure and services running in multiple clouds. This can include private clouds, SaaS apps, Amazon Web Services, Microsoft Azure,

and Google Cloud Platform. Though this specific situation may not have been planned for, the cloud allows for unexpected needs to scale and pivot, Pfeiffer says. “Maybe we envisioned a region being inaccessible but not necessarily every region all at once.”

Normally it can be easy to declare standards within IT, she says, and instrument an environment to operate in line with those standards to maintain control and security. Losing control of that environment under quarantines can be problematic. “If everyone suddenly pivots to work from home, then we no longer control the devices people use to access the network,” Pfeiffer says.

Such disruption, she says, makes it difficult to control performance, security, and the user experience. It can lead to mixed environments that can include consumer technology made up of whatever is on hand in the user’s home, says Pfeiffer. For example, employees might connect to their corporate network through public internet access, over a MiFi device, through mobile phones, or even gaming computers.

Furthermore, she says there may be increased comparisons of enterprise applications with consumer applications because both types of apps are accessed side-by-side on the same personal devices. She says the higher ease of use found among consumer applications could put pressure on enterprise IT to offer such capabilities.

The benefits of cloud migration and software-defined resources are hard to ignore, Pfeiffer says. Nutanix transitioned a year and a half ago, she says, from traditional switches and routers at data centers to having a third-party software-defined network that runs on commodity hardware. This allows for making changes remotely by managing infrastructure as code via software, which would not have been possible in the old model. “We paid a lot less for CapEx,” Pfeiffer says. “We have a much smaller team now that reconfigures our network. We’re not paying for CCIE (Cisco Certified Internetwork Expert) level skills.”

There is a security tradeoff, she says, to remote operations running through the cloud. “The attack surface is much broader than before,” Pfeiffer says, increasing the need to monitor and build tools around such demand.

As circumstances evolve over the long term, organizations might introduce mixed operations where some staffers return to office worksites while others do not, Pfeiffer says. Pressures from remote work and in-office work models could require further reallocation of resources. Global networks already see increased demand, which she says is not likely to change if some of the workforce returns to offices. Pfeiffer says there will be a need to increase network capacity on all fronts, including out to the edge. “We need better remote infrastructure,” she says.