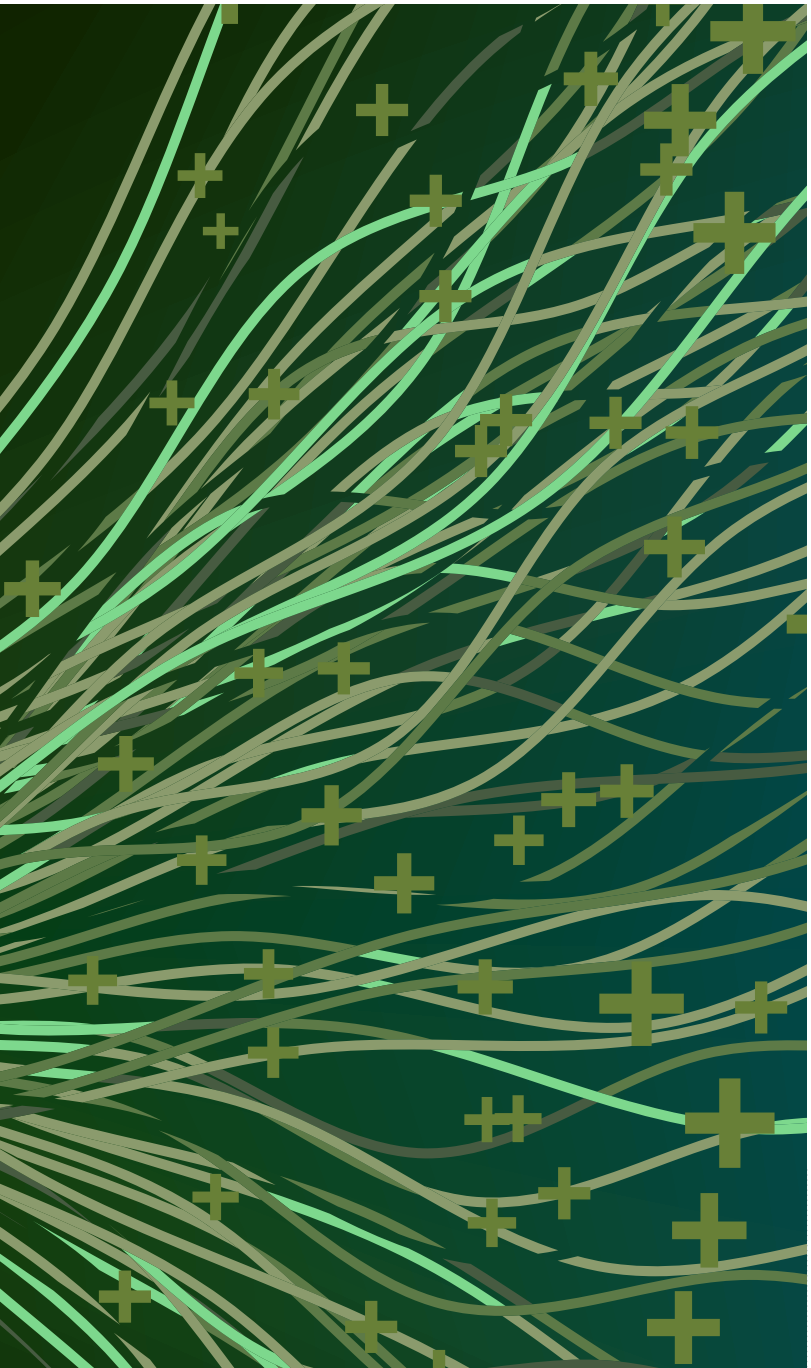
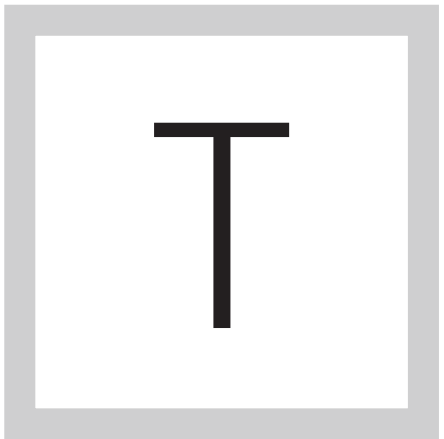


E-Guide

HYBRID CLOUD SECURITY IS NO CASTLE IN THE AIR

TechTarget | SearchSecurity



HE TRADITIONAL MOAT is disappearing as companies embrace new security models, from micro-segmentation to perimeter controls.

HYBRID CLOUD SECURITY IS NO CASTLE IN THE AIR

By David Strom

As CIOs adopt hybrid-cloud strategies, some quickly learn that these environments need new kinds of security models or, at least, contexts in which to apply existing controls and security technologies. Most organizations also find that their environments are not as simple as a pure private plus public cloud. Legacy on-premises systems, software-as-a-service (SaaS) applications, and infrastructure as a service (IaaS) all come into play.

The security tools used to protect public and private cloud resources may still include perimeter-based controls like firewalls, access controls and log management, but fluency in traditional IT security only goes so far. "The nuts and bolts of the way the work gets done is different, in the sense that Spanish is different from French," says Dave Frymier, CISO at Unisys Corp., a global IT services provider in Blue Bell, Penn. "Security teams will have to learn a new language, but they will do the same risk-analysis work they do today on premises."

Companies such as Unisys and ING, a global financial institution headquartered in Amsterdam, are using hybrid clouds as a way to consolidate data centers. The move makes sense: You don't have to provide the up-front capital to house your servers, and you can rent capacity as needed and charge it to an operating budget.

Rather than invest in more real estate, you can leverage the services and expertise of IaaS providers and rent the equipment only when it's necessary. "IaaS has made great strides from the major cloud vendors and moved beyond the initial consumer-oriented clouds of five years ago," says Frymier. "We now have a complete virtual infrastructure that can be used to build secure environments, with a business-class service that is a cut above the consumer versions of the past."

Security can be built in when the consolidation happens, making the cloud just as secure as a traditional raised-floor data center. The banking industry has put together its own architecture and network standards, with input from early adopter ING, whose former CIO and global COO Steve C. Van Wick serves as chairman of the Banking Industry Architecture Network's board. It includes implementation guides to build in the appropriate security levels upfront.

The best strategies involve using cloud-native or cloud-first security tools, instead of forcing traditional technologies that don't necessarily translate, such as firewalls or intrusion prevention devices, to cover both on-premises and cloud-based environments.

Whether you are migrating internal assets, adopting external cloud services, or combining private and public clouds with on-premises servers, here are five general strategies that many CIOs have settled on to mitigate security concerns:

1. **Ratchet up user education and communication.** Sticking your head in the sand isn't really a strategy. "You can't just become the party of no," says Richard Seroter, vice president of product for CenturyLink Technology Solutions in St. Louis. Parent company CenturyLink Inc., which acquired Web hoster Savvis in 2013, offers a self-service cloud or managed services at data centers globally.

"If a user has a credit card, they can deploy apps anywhere and on any cloud," he says. "Instead of swooping down at the end of a project with all sorts of restrictions, learn how to collaborate with operations and users upfront."

Home

Hybrid Cloud Security Is No Castle in the Air

According to Seroter, this approach has some other benefits as well: "Security becomes a part of every customer briefing we do," he notes. "We don't wait for the customer to ask us about security, but instead try to take an active approach so that our clients understand the shared responsibilities we have—we try to have as frank a conversation as possible on how they secure access to their data."

You also have to be aware of potential regulations and legal ramifications, and educate your employees. "A key part of our cloud migration strategy was working with our legal department to define a new information security framework, which was launched in early 2014," says Ed Happ, global CIO of the International Red Cross and Red Crescent Societies in Geneva, Switzerland. In 2013, the organization extended its agreement with Microsoft to move as many as 80 of its 187 National Societies to cloud computing services, including Microsoft Office 365. The goal was to free up capacity and IT spending, and address the digital divide by providing smaller National Societies around the world with access to the same tools.

The Red Cross found that more than 95% of its information was either public or internal, and did not require additional levels of security beyond what commercial applications provided. For the remainder, according to Happ, the Red Cross put together information and made it available on its intranet to

help users worldwide match the tools to their particular needs and information security requirements. This included training videos and other guidelines on how to secure applications.

2. **Use stronger authentication methods to secure cloud access.** When all of your resources are just a username and password away, it makes sense to implement multifactor authentication (MFA) and single sign-on methods (SSO) to better protect these assets. The SSO tools are getting better at supporting a wider array of cloud-based applications and implementations. Typically, these products supply two URLs: a portal page for users with a single login to their apps and a management portal for IT administrators.

Most SSO products now automate the logins for thousands of applications. Some SSO tools such as SecureAuth, Okta, Ping and Centrify can specify MFA for particular applications as part of a risk-based authentication approach. This makes using SSO a powerful, protective tool and can secure logins better than relying on users to choose individual passwords. It also means that IT can play a more critical role in defining cloud-based assets and matching up the appropriate security levels.

3. **Start using encrypted emails and file transfers to protect your communications.** As more of your communications takes place over the Internet, you need to do a better job protecting this information, and the best way to do that is by using encrypted emails and file transfers. If you haven't looked at either, both security approaches are now easier to use.

The International Red Cross is employing a zero-knowledge email client. This approach uses a shared passphrase to decrypt your message and for your correspondent to compose a reply to you. In some cases, the recipient can read the message by just authenticating himself with a couple of mouse clicks. After this first communication, the recipient is now able to exchange encrypted messages with you quite easily. The result avoids having to preselect a common communications tool for passing secure messages. The Red Cross is also making use of a file transfer service that encrypts files at rest and in transit. Both of these products are used in situations where the most sensitive communications are required, such as message exchanges between governing boards or other high-level work.

Home

Hybrid Cloud Security Is No Castle in the Air

4. **Implement better access-roles definitions to control your virtual machines (VMs).** As you deploy more virtual infrastructure, you need to up your game in terms of protecting which users have access to the VMs. Products like Hytrust and Catbird can be used to put in place more granular access controls, so that users, for example, can run applications residing on a VM but they can't start, stop or delete the entire VM. And what's more, these tools can operate in both the data center and in the cloud. These technologies and others can also be used to log access, just like other security products that have role-based access controls. "We can't always keep you from doing bad things but we can implement role-based access controls carefully, so VMs can be isolated from each other and users have appropriate levels of access," says Seroter.

5. **Prepare for the coming world of micro-segmentation and virtual containers.** Tools like Docker containers can help focus your resources in the cloud and more closely target your workloads and needs. Rather than bringing up an entire VM, you can just initiate a virtual process or automatically link to a series of processes for specific tasks. "Containers

can live 10 seconds or 10 days," says Seroter, "And you have to know how to assess that attack surface because it is a very different animal."

Micro-segmentation products such as FireHost can programmatically provision network and security services and policies for particular workloads. They can set up specific network VLANs and firewalls and enforce those policies at the virtual network interface. "Security pros need to be ahead of these emerging trends and know their limitations and how they can be used safely," Serator says, "not just prevent something from being deployed."

DAVID STROM is a freelance writer and professional speaker based in St. Louis. He is former editor in chief of TomsHardware.com, Network Computing magazine and DigitalLanding.com. Read more from Strom at Strominator.com.

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.