DXC.technology

White Paper

Moving to hybrid IT? Make sure security isn't left behind

February 2018

Today's smart technology environments combine public, private and other clouds. That can provide great benefits — but only if security is built in.

Today's new hybrid IT approach lets organizations tap into the public cloud, private clouds, conventional IT, mobility and more to create a single, comprehensive set of compute services. But security in this environment is far too often treated as a separate element. That's a big mistake, and a dangerous one.

When organizations neglect security, they risk costly breaches that can negate hybrid IT's many benefits, including a shift of CAPEX dollars to OPEX, greater flexibility and improved scalability. What's needed is an integrated model for security, which ensures that the movement of data and workloads, as well as the data-sharing between public and private clouds, will be completely protected.

In this white paper, we describe why hybrid IT requires a new approach to security, outline a dozen best practices, and show how DXC Technology can help your organization safely implement hybrid IT.

Consider a public-cloud application that depends on, and shares data with, an application run from a private data center. Both environments will need to be secured as part of a single integrated view. Similarly, while various elements of a hybrid IT environment may need different tools and techniques, these must be organized under a unified security strategy. That means single compliance and governance models as well.

New security approaches will be needed because the public cloud creates new attack surfaces. That's a serious issue in light of the fact that many organizations hope to move up to 80 percent of their legacy applications to the public cloud. In today's cloud-first environment, older tools designed to protect legacy IT no longer suffice. Most of the security tools that companies are using today will need to be either remediated or replaced.

In addition, moving to the public cloud makes it far easier for organizations to accidentally expose their sensitive data and workloads. With the rise of "shadow IT," all it takes is one naive user mistakenly placing sensitive files in public cloud storage and suddenly an organization's data is at risk.

On top of all that, hackers and cyber criminals are getting more sophisticated, and there's a growing need for regulatory compliance worldwide.

In fact, chief information officers (CIOs) and chief information security officers (CISOs) who fail to create an integrated security strategy as part of their move to hybrid IT will put their organizations at serious risk. These organizations will likely need more time to resolve security incidents, exposing themselves to greater damages. And they'll be less able to quickly and accurately predict where the next attack or breach is likely to occur, potentially exposing themselves to even more attacks and losses in the future.

Best practices for secure hybrid IT

Cyber security in today's hybrid IT environment must be relentless. What's needed is an "unblinking eye" that's always watching and, in the event of a breach, always ready to respond, quickly and consistently.

On the one hand, cyber security involves lots of relatively simple activities. On the other, these activities must be done repeatedly and consistently — that is, all the time.

Start by taking an approach that's **holistic**, not just tactical. The approach of "I'll just move this workload to the cloud and secure it" is no longer sufficient. Instead, you'll need a strategy for the entire perimeter of your hybrid cloud environment, one that includes not only security, but also identity and access management (IAM), monitoring, and more. Also include a cloud-readiness assessment to plan the transformation of your applications and infrastructure.

Here are a dozen key steps that will help keep your hybrid IT environment safe and secure:

- **Assign duties and responsibilities.** Talk with your cloud service providers to find out who's responsible for what. Which tools should you use, and how? And how do you connect these new tools with those you already use?
- **Adopt policies.** You'll need policies to manage the explosive growth of bring-your-own-device practices. You'll also need policies to manage your service providers.
- **Start with identity.** In a hybrid IT environment, your organization's ability to accurately authenticate every user's identity is essential. So is your ability to quickly determine which workloads, applications and data each user is entitled to view, change and share.
- **Apply AI.** Artificial intelligence and analytics tools can correlate security telemetry to information stored in your organization's data lake. In this way, they can provide you with an integrated view of your organization's total data pool, not just the data in single environments. And by analyzing this data, AI tools can also detect your most urgent security threats today, and predict where they're likely to occur tomorrow.

Hybrid IT —- The options increase

The public cloud is just the beginning. Today's organizations can manage workloads across hybrid IT environments that include private clouds, virtual private clouds and more. Here are some of the options on your hybrid IT menu today:

- **Public cloud:** Amazon, Google and Microsoft are among the suppliers offering public clouds for storage, app dev and more. Prices are competitive, and security has been greatly improved.
- **Private cloud:** Looking for greater security? A private cloud keeps your data and applications far closer to the vest. At the same time, an integrated private cloud management platform can connect and manage public and private clouds together.
- **Virtual private cloud:** A hybrid approach allows you to privately access multi-tenant computing resources on an otherwise public cloud.
- **Vendor services:** Software suppliers are beginning to offer integrated cloud services. VMware, for one, offers a service that extends a private cloud into a virtual managed cloud running in an Amazon data center. Microsoft's Azure Stack is similar, but works in the opposite direction, bringing public cloud services to a user organization's on-premises private environment.
- **Brokered services:** These provide an interconnection between public and private cloud services, offering a single central location from which to manage all workloads. They can also sort services by security, latency and region. Some also automate the movement of workloads based on user profiles.

- **Gain greater visibility, audit and reporting.** Although separate tools now exist, the next frontier will involve their integration. The larger goal: a single view into your hybrid IT environment's security standing.
- **Adopt DevSecOps.** This approach essentially bakes security into the DevOps process, rather than bolting it on at the end, as has been traditionally done. DevSecOps is a proactive approach to ensuring that all your new applications are kept highly secure.
- **Embrace the self-service model.** Many public cloud services offer self-service to provision resources and services, and this is dramatically different from the traditional IT approach of work orders and service requests. To proceed safely, ensure that all security-automation features are engaged so that your newly provisioned services and resources will have automatic security built in.
- **Approach cloud security from an enterprise perspective.** First, understand the workloads that could be migrated to the cloud. Second, understand each workload's enterprise-security requirements. Third, select the cloud platform and architecture. Fourth, understand the shared responsibilities between you and your service providers. Finally, adjust your existing security approaches and solutions to focus on IAM, data protection, privacy and more.
- **Implement key security capabilities.** These will likely include data-centric security; dynamic infrastructure hardening; monitor/detect/respond; continuous regulatory compliance; and shared access management.
- **Scan data on use.** Data stored in the cloud has a serious security limitation: It cannot be scanned for malicious content. For this reason, you'll need to establish processes that let you scan contents accessed via cloud storage "on the fly." You'll also need to be able to re-scan repositories when a type of malware is known to have spread into the wild.
- **Follow industry best practices.** With so much work done in this area, there's no need for you to reinvent the wheel. One good place to start is with the Cloud Security Alliance's data-security life cycle.
- **Gain new skills.** Training will be vital. That's because securing hybrid IT involves new approaches, such as software-defined networking and microsegmentation, and these require skills your staff is unlikely to already have. Don't neglect training!

DXC: Your guide to a secure hybrid IT environment

Fortunately, when securing your hybrid IT environment, you can turn to DXC Technology for help and guidance. For more than 50 years, we've been securing core IT systems for many of the world's leading businesses and governments. Today, DXC employs more than 4,000 security professionals worldwide. As a vendor-agnostic, prime security integrator, we also offer industry-leading, end-to-end security solutions and around-the-clock security management and monitoring.

You can turn to DXC for a broad array of services to make your hybrid IT environment secure — both inside and outside your data center. We've been marrying our traditional approach to cyber security with new tools and approaches for today's hybrid IT environments. That includes focusing on the integration of a continually evolving set of services that include IAM, cloud broker monitoring and network capabilities.

For example, DXC's Managed Cloud Access Security Broker can help your organization protect its most sensitive data. This solution first identifies all cloud applications being used by your organization. Next, it determines which applications should be sanctioned. And finally, it creates and enforces security policies through continuous monitoring and threat analysis. That's powerful and secure.

You can also turn to DXC for an overarching view of your hybrid IT environment, which is far better than the more common piecemeal approach. DXC's security-first mind-set can help you shape your security standards, share responsibilities with your third-party suppliers and provide for an in-depth defense.

Contact us at www.dxc.technology/contact_us to find out how to create a security strategy for your hybrid IT architecture that's truly integrated.

What's coming next?

To prepare for the future, you have to know what's coming. Here are our top predictions for cybersecurity in the age of hybrid IT.

Everything as an API. In the future, virtually all traffic will be web-based — HTTPS to the cloud. Even today, most new cloud services are API-enabled. As a result, the need for enterprise firewalls is coming to end. But you'll still need a way to inspect data content for anomalies, malicious content and other indicators. API keys will be the new password, ensuring that the right person or entity has the right access to an API function to access the right data.

Serverless computing shifts the focus back to data. With the compute function highly virtualized, you no longer manage a web server, and only storage is persistent. While that can produce faster spinups and lower costs, it can also restrict your visibility into your data's location and content. As a result, workload management, encryption and IAM will all become increasingly important.

Security as a service. Cloud-based security services, offered on a subscription basis, will become the new normal. They'll offer all the benefits of other as-a-service offerings, including the move of OPEX spending to CAPEX, greater flexibility and scalability, lack of costly on-premises equipment, and reductions in floor space as well as power requirements and related costs.

More regulation. New rules include the European Union's General Data Protection Regulations (GDPR), which go into effect in May 2018. These will create complex and potentially costly responsibilities for any organization holding data on any EU citizens. Similarly, China has tough new cyber security laws that require foreign firms operating in the country to buy mostly Chinese-made telecom gear and to store financial data within the country's borders. And in the United States, the Federal Communications Commission's recent decision to repeal "net neutrality" rules is likely to have serious security implications for service providers and users alike. These and other regulatory moves will create new costs and complexity for organizations striving to comply.

More sophisticated cyber attacks. Think of this as an arms race. Cyber criminals are mounting new threats and more frequent attacks, creating even more damage and losses. To protect themselves, organizations will need to get more sophisticated, too.

About the authors

Chris Moyer, vice president and general manager of security for DXC, has spent more than 25 years building business and technology solutions for clients in several industries across multiple geographies. In previous roles, he has led solutions, transformation projects and delivery assurance. Chris is also a member of the Institute of Electrical and Electronics Engineers.

James Miller is DXC's chief technology officer and vice president for cloud and platforms. In this role, he builds key client relationships, advises senior leadership on technology trends and initiatives, and provides oversight and thought leadership to grow DXC and client business. Previously, Jim was the industry chief technologist for manufacturing, automotive, aerospace and defense, and strategic accounts at Hewlett Packard Enterprise.

Andreas Wuchner is DXC's chief technology officer of security innovation. He has more than 20 years' experience in all areas of information security, IT cyber security and information risk management. Prior to joining DXC, Andreas was chief information officer of security technology for UBS in Switzerland.

Michael Dutton is lead security architect for DXC's managed security services in Australia. He has collaborated with DXC's cloud services delivery for several years to ensure that security solutions provide enterprise-level protection for hybrid and public cloud, aligned to Agile cloud methods and automation. Michael has 15 years of experience in information security, enterprise security architecture, consulting and regulatory compliance.

Ilya Joel-Pitcher leads DXC's Azure advisory and global Center of Excellence. He focuses on supporting customers with strategic advice and best practices to accelerate their digital transformation with Azure services. Ilya has over 18 years' experience covering transformation strategy, enterprise architecture and hybrid cloud adoption.

Learn more at www.dxc.technology/cloudsecurity

February 2018