DXC TECHNOLOGY

What's next for enterprise security? Look to public cloud

The latest integrated security tools from leading cloud providers could be a catalyst to simplify and modernize IT environments.

In the early days of cloud, security was a key concern for IT executives. However, today's major public cloud providers' security capabilities are more mature, more integrated, and often easier to use than traditional third-party tools.

In fact, integrated security tools now being provided by hyperscalers such as Microsoft, Amazon Web Services (AWS) and Google Cloud are highly effective at securing data, managing identities and ensuring resiliency.

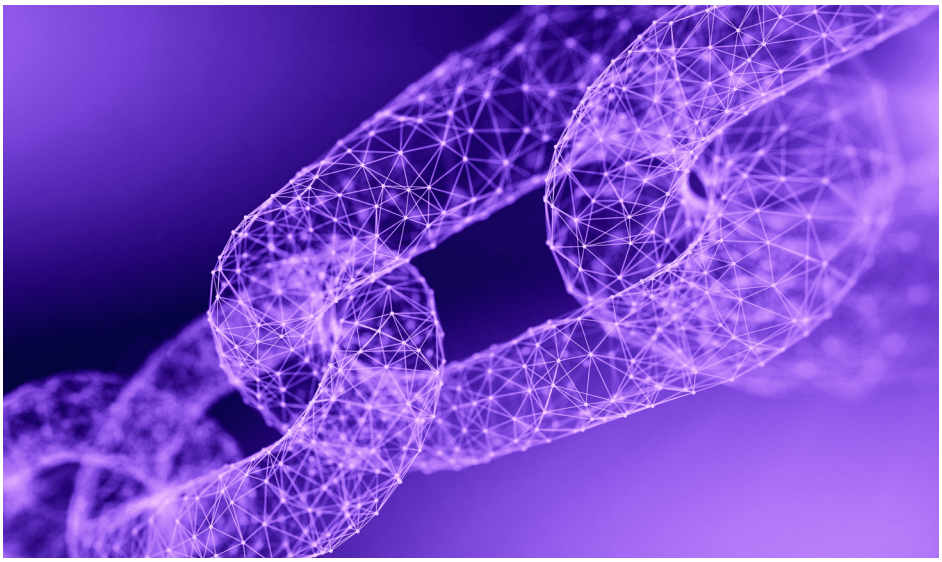
Cloud security now has implications for the whole enterprise. Moving to cloud-native tools offers a new approach to security management and could be a powerful catalyst for modernization. Cloud-enabled security can help organizations simplify complex environments, increase speed and flexibility, and control costs.

Overcoming complexity

With a myriad of third-party security tools available both in cloud and on premises, organizations are often inundated with alerts from a variety of sources. The sheer number of tools — some organizations use more than 50 — makes them difficult to integrate and manage. Compounding the challenge is that third-party tools must be updated frequently to keep pace with innovation and the ever-changing threat landscape.

Unfortunately, many third-party tools are not optimized for public cloud. Organizations are shoehorning in security tools, hoping they can perform important tasks they're not really fit to deliver or continually maintain. In addition, security teams need the skills to support multiple cloud and on-premises platforms.

One result of this complexity: IT departments fail at enforcing the basics of cyber hygiene and configuration. They may lose visibility into their IT assets, allow overly permissive access rights, or leave software unpatched or private services exposed to the internet. These and other related shortcomings can put organizations at serious risk, especially with cybercriminals gaining new levels of sophistication in tactics, techniques and procedures.



The hyperscaler approach

With cloud-native tools baked into their services, cloud hyperscalers have made their controls easy and flexible to use.

Public cloud hyperscalers have an answer to these challenges: a more modern approach to cloud security with built-in capabilities and integration between tools. This same approach can be extended to on-premises systems.

In the past few years, public cloud providers have recognized that organizations' concerns about security are inhibiting cloud adoption. To counter this, the hyperscalers have made massive, multibillion-dollar investments in cloud-native security tools and services. These investments are expected to continue for some time.

Why consider security tools from the hyperscalers? Because with cloud-native tools baked into their services, cloud hyperscalers have made their controls easy and flexible to use. In addition, these companies offer related governance tools, which continuously check to make sure cloud resources are deployed securely and in compliance with best practices and regulations.

As a result, instead of relying on an array of incompatible third-party security tools, organizations can rely more heavily on the standard cloud-native toolsets developers and operators already use every day. Third-party security tools can then be used to fill the gaps for specific needs such as vulnerability scanning. This approach can not only simplify organizations' security-related solutions, but also lower their overall costs.

One of the biggest mistakes to make when moving to cloud is trying to apply traditional enterprise security tools and practices to the new, more complex environment.

Hybrid security: Getting the right fit

Securing hybrid and multicloud configurations requires ongoing effort. When moving to cloud, organizations need new cloud-native tools to be tuned in order to maximize their security posture, decrease complexity and ensure a good return on investment. They also need a consolidated view of security across the entire IT estate.

One of the biggest mistakes to make when moving to cloud is trying to apply traditional enterprise security tools and practices to the new, more complex environment. Now is the time to think in terms of a true cloud-enabled enterprise and adopt the many lessons learned from cloud, reduce complexity and get the basics right.

This does not mean organizations need to go all-in with hyperscalers. In rationalizing tools, it is important to choose tools that fit your organization's security requirements, and ensure they create the desired outcome in your various environments.

How to get started

These three steps will help your organization move forward:

- **Leverage the public cloud.** Choose new ways of delivering security capabilities, including those of your cloud service provider or hyperscaler. That might include replacing instead of upgrading; streamlining patch management; and adopting infrastructure as code. Moves like these also let you automate, examine and test that everything is consistent — since everything is code. In short, question the way you've historically addressed things like patching and malware detection. In the cloud, you can probably perform these operations in a new way.
- **Choose wisely.** While some built-in security capabilities of cloud service providers and hyperscalers can be leveraged globally, others cannot. Take advantage of the tools that can help you. But remember, none can do it all. And some capabilities, such as vulnerability scanning, aren't offered by public cloud companies at all. For these tasks, you may still need third-party tools.
- **Apply the lessons from cloud to traditional environments.** Take the changes in approach, and see where else in your estate you can apply them. You can likely apply lessons learned from cloud to on-premises infrastructure, increase speed and ensure more consistent practices.

How DXC can help

Partnering with AWS, Microsoft, Google Cloud, VMware and others, DXC Technology helps the world's largest companies protect today's hybrid and multicloud environments. DXC's virtual private cloud, managed hybrid cloud and multicloud solutions improve security, control expenses and simplify the management of multiple cloud environments.

DXC professionals offer deep expertise and proven processes in cloud strategy and migration, cyber defense, identity and access management, governance, and risk management. We can help you securely and reliably transform your business.

Authors

David Langlands, vice president, Security Offerings, DXC Technology

Daniel Blander, executive director and chief information security officer, Cloud Migration Strategy, DXC Technology

Darren Robinson, director, Cloud and IT Infrastructure Security, DXC Technology

Learn more at
dxc.com/security

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services across the Enterprise Technology Stack to drive new levels of performance, competitiveness, and customer experience. Learn more about how we deliver excellence for our customers and colleagues at **DXC.com**.