Adaptive Cloud Security

Fortify and Enhance Your Cloud Security Platform

Table of Contents

Executive Summary

Today's organizations rely heavily on cloud applications in order to be at the forefront of digital innovations, and to keep their users connected and their businesses thriving. Cloud innovations help keep organizations competitive in the ever-changing and demanding digital marketplace, with new applications and cloud services enabling businesses to be more agile, adaptive, and responsive to pressing market demands, user expectations, and employee productivity. But for businesses to be as agile and adaptable as they need to be, the applications they use need to be configured and secured consistently, everywhere they reside.

In this new age of mass teleworking, the plethora of Internet-of-Things (IoT) and bring-your-own-device (BYOD) workforce applications and devices have expanded the network and created many new network edges and cloud edges, which has consequently exploded the attack surface. Research shows that an estimated 70% of the workforce will be working remotely at least five days a month by 2025.[1] This sudden shift to remote teleworking has accelerated the expansion of the traditional local-area network (LAN), wide-area network (WAN), and data center edges to include multiple hybrid cloud environments, a new, more agile WAN, SD-Branch, and IoT networks. In fact, according to the 2021 Flexera State of the Cloud report, 92% of enterprises now have a multi-cloud strategy, and 80% have a hybrid cloud strategy in place.[2] On average, enterprises use 2.2 public clouds and 2.2 private clouds, and cloud adoption continues to accelerate.

Secure Your Apps, Everywhere They Go

Organizations need to place the applications they use at the compute edge, closer to the user, for maximum performance. Today's companies are building compute or moving applications from a centralized cloud to a distributed cloud or even multiple distributed clouds that sit geographically closest to the user or device that needs access to their applications. It's also becoming easier to consume applications on-demand or as Software-as-a-Service (SaaS), as flexible consumption models proliferate the marketplace to satisfy user demands. Yet, not all applications can be migrated to the cloud. As a result, most organizations will be deploying and utilizing hybrid or multi-cloud solutions for some time to come.

And now IT teams find that they have to support thousands of mobile workers and their new remote home offices—with cyber adversaries targeting IoT devices, such as home entertainment systems, home routers, and connected security devices. Each of these IoT devices introduces a new network "edge" that needs to be defended. This has put pressure on security teams to figure out how to extend security monitoring and enforcement out to every device. Applications and the ease and speed of accessing those applications and data are the lifeblood of digital innovation. However, applications are now incredibly dispersed and on the move.

Applications follow the available infrastructure, and your security needs to meet them there:

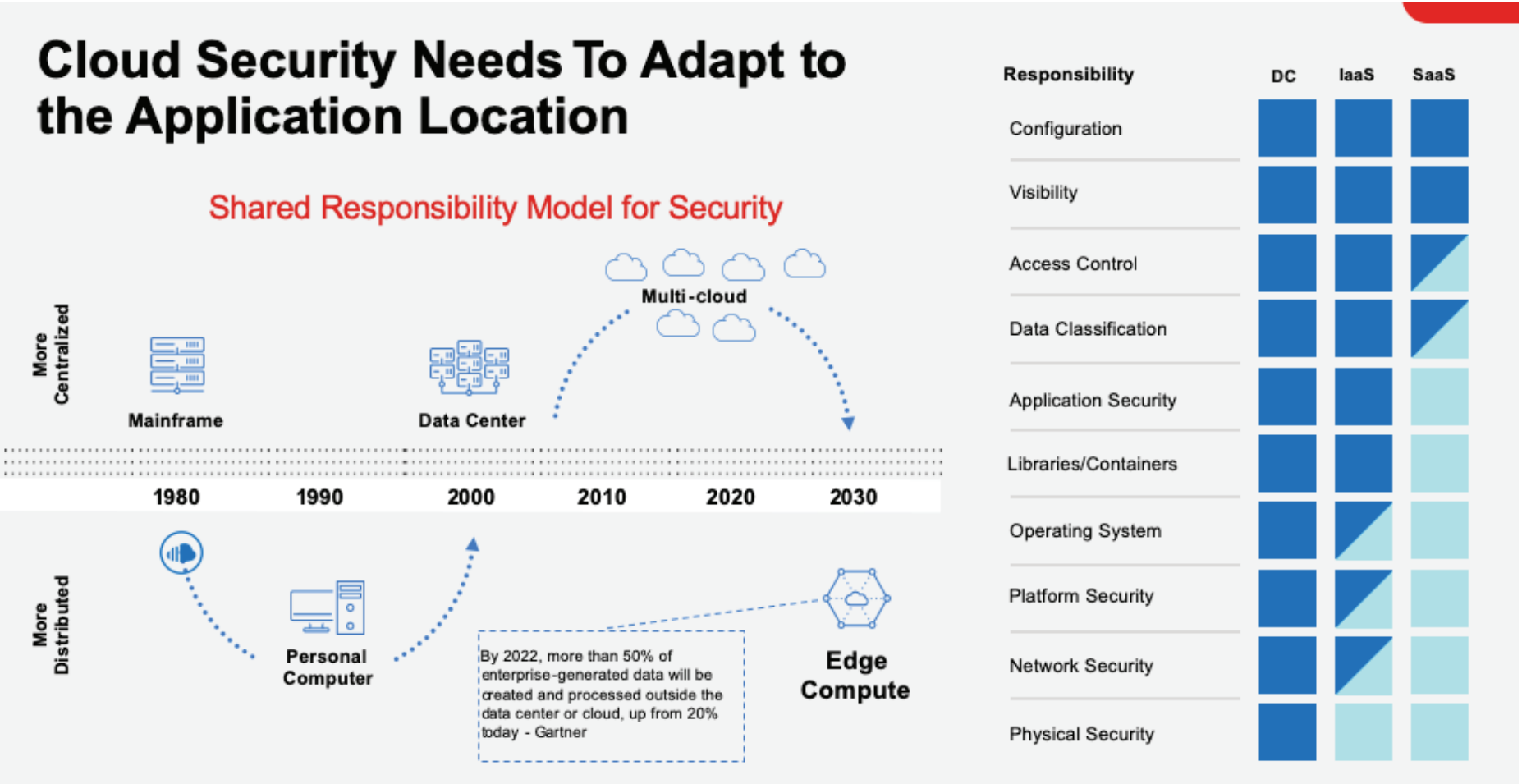
Mainframe

Workstation

Data center

Cloud

Hybrid and multi-cloud



Protecting applications is fluid, and adaptive cloud security solutions follow applications wherever they may be deployed, on whichever cloud or clouds they may be deployed on. Moreover, an adaptive cloud security platform empowers organizations to pursue and shift their cloud-enabled digital innovations strategy as they require, without having to sacrifice security, operational efficiency, or take on undue complexity. This is best accomplished as an integral part of a broad, integrated, and automated cybersecurity platform.

Challenges of Multi-cloud Models

Hybrid and multi-cloud deployments

Hybrid environments allow organizations to keep important data on-premises while also taking advantage of the benefits of the cloud. This allows them to maintain control over sensitive assets, while also taking full advantage of the scalability and agility the cloud has to offer. However, as organizations become more hybrid and distributed, their security needs to be able to span across all environments.

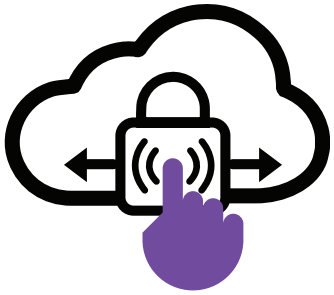
Hybrid cloud possibly presents the most challenging problem when determining the best security solution. With resources spanning both assets you control and either public cloud infrastructure or specific SaaS or data resources, visibility is paramount so the security team can see the entire picture. End-to-end management, segmentation, and securing external connections become the most-critical elements of a hybrid cloud security solution.

Multi-cloud environments generally fall short when it comes to providing visibility among solutions, often resulting from disjointed management tools that are provided by disparate vendors. And this lack of visibility can lead to numerous security issues, opening organizations up to more compromises and vulnerabilities and delaying response times, because none of the deployed security components can see or talk to one another.

Sharing the responsibility

As it is now, organizations with cloud ecosystems participate in the *shared responsibility model*. The shared security model consists of two key components: security **of** the cloud and security **in** the cloud. While organizations rely on cloud providers to protect the security "of" the cloud—the storage, network, and compute layers, they own the security "in" the cloud—that includes everything that is built, deployed, or stored in the public cloud. The challenge here is that each cloud environment has its own standards, requirements, and protocols. Security teams attempting to secure a multi-cloud environment need to not adopt these requirements when securing each cloud instance, but the solutions that they deploy must be flexible enough to support security functionality in a shared model, both within a specific cloud environment and between clouds.

This model can help relieve some of an organization's operational burdens, as the public provider operates, controls, and manages the components from the host operating system and virtualization layer down to the physical security of the facilities where the service operates. However, the organization still bears the responsibility of securing other multiple layers of their environments that need consistent, manual protection. What's left is a scattered, patchwork approach to cloud security that isn't sustainable or scalable, and it needs to evolve.



As organizations become more hybrid and distributed, their security needs to be able to span across all environments.

Web app and API protection

Many companies fail to adequately secure their cloud environments because they don't understand the shared responsibility model. Public cloud providers generally keep their systems safe, but, again, the cloud customers are fully responsible for protecting the applications they deploy and the data they store in their clouds.

Unlike on-premises applications, which can be protected by controlling access to specific Internet Protocol (IP) addresses, app traffic on the web doesn't have these security "choke points." In the cloud, threat detection needs to shift from the port the traffic flows through to the application content and context of the traffic itself. In order to provide this deeper level of insight, organizations need to make continual, granular adjustments to web-app security policies. This task done manually is not sustainable, with limited IT resources and the onus of constant app management. These adjustments need to be automated for the fastest, most intelligent results.

Many companies fail to adequately secure their cloud environments because they don’t understand the shared responsibility model.

Securing the Everywhere Enterprise

There are at least five security areas that need to be addressed when building and managing security in the cloud:

1. Risk of data loss/compromise
2. Regulatory compliance
3. Resources/skills gap
4. Complexity
5. Deployment/setup of cloud (e.g., misconfigurations)

Chief among these risks are misconfiguration-exploiting cyber threats. According to a 2020 Cloud Security Report, the highest ranking threat for 2021 was going to be misconfiguration, with 68% of companies citing this as their biggest concern.[3] The lack of visibility and communication between various point solutions invariably leads to greater exposure to risk. A successful attack on a cloud-based environment can possibly impact the entire company, interrupting or ceasing operations, causing the loss of crucial business data, and damaging the organization's brand reputation.

The Solution: A Unified Platform Approach To Cover All Clouds

Securing all clouds, cloud networks, applications, and platforms is the security architecture approach that can benefit all organizations, regardless of industry. Adaptive cloud security platforms make this possible, protecting workloads and business applications both in on-premises data centers as well as in any cloud environment—private, public, multi-cloud, and hybrid models. This platform approach provides organizations with a consolidated view of their security posture, leveraging a single console for policy management regardless of which cloud infrastructure they have.

Organizations should look for a cloud security platform that is built organically around a common operating system and management framework designed to enable seamless interoperability, full visibility, and real-time communications, as well as automated granular control across the entire infrastructure. An integrated, unified cybersecurity platform approach with a rich ecosystem built-in to protect the extended digital attack surface provides broad integration and implementation with application programming interfaces (APIs) and third-party apps, automation enabled by artificial intelligence (AI) and machine learning (ML), and the single-pane-of-glass visibility needed for all of the solutions to function cohesively.

Broad integration and easy implementation

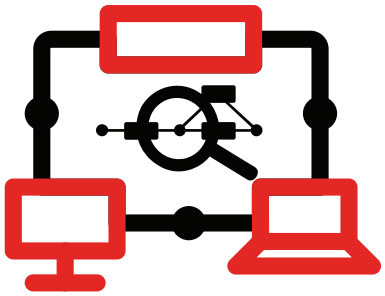
Lack of security solutions integration makes it impossible for organizations to use the flexible network environments they need to compete effectively. A unified security platform needs to work seamlessly with all cloud platforms as well as third-party apps and solutions for easy setup, visibility, and management control. Security solutions need to support a distributed security model where the exact same security solutions can be deployed in any environment, either with open APIs or integrations, or both.

Automation

AI and ML can detect and prevent anomalous and malicious behaviors early in the attack cycle. Lean IT teams often lack the time and resources needed to manage and secure each element in their complex cloud environments, especially with the ongoing cloud skills gap. In a recent Gartner survey of infrastructure and operations leaders, 58% of respondents identified "insufficient skills and resources" as their biggest challenge when it comes to meeting cloud adoption and optimization goals.[4] Organizations need more automated and integrated solutions to ease cost and operations burdens.

Visibility

All of the various security solutions deployed across the network need to be able to see one another and work together as a single system to detect and respond to threats in a coordinated, timely fashion, regardless of where they reside. With resources spread across both physical and virtual systems, security professionals can't coordinate among dashboards for visibility, or operate without central, real-time analytics for threat intelligence. A cloud security solution must integrate a single view across all systems operating in the cloud and on-premises with centralized management. This single-pane management approach can track data flows across the entire network in a format that makes that information relevant and actionable.



Lack of security solutions integration makes it impossible for organizations to use the flexible network environments they need to compete effectively.

Conclusion: Fortify and Enhance Your Cloud Security Platform

The security tools that come standard on public cloud services are inadequate when it comes to protecting dynamic, hybrid, and multi-cloud environments. Misconfigurations are inevitable, and the resulting security gaps can inflict damage on an entire organization. While these risks may not be fully visible and felt in the early stages of software development, organizations cannot wait until they are. By integrating cloud-native security with adaptive cloud security solutions, organizations can close cloud security gaps while alleviating security management burdens. Ideally, organizations should choose a cloud security solution that is tightly integrated with an overarching cybersecurity platform to further simplify network, security, and cloud operations. The broad range of advanced security technologies, seamlessly integrated functionality, and AI-driven capabilities of an adaptive cloud security solution can fortify and enhance an enterprise security platform, with broad integration, easy setup and implementation, included automation functionalities, and vast visibility.

[1] Caroline Castrillon, "This Is the Future Of Remote Work In 2021," Forbes, December 27, 2020.

[2] "Flexera 2021 State of the Cloud Report," Flexera, 2021.

[3] "The Biggest Cloud Security Challenges in 2021," Check Point, accessed April 26, 2021.

[4] Raj Bala and Ross Winser, "The Cloud Infrastructure and Platform Services Skills I&O Teams Require for the Future," Gartner, September 2, 2020.

www.fortinet.com

May 1, 2021 12:33 AM

ebook-adaptive-cloud-security

945671-0-0-EN