


ACHIEVE DIGITAL ACCELERATION WITH ADAPTIVE CLOUD SECURITY

 **40%** of IT professionals cite cloud monitoring, security, and application development to be hybrid/multi-cloud challenges.¹

DIGITAL TRANSFORMATION: ALL ROADS LEAD TO THE CLOUD

A few months into the global pandemic, Microsoft CEO Satya Nadella stated that two years worth of cloud-driven digital transformation had occurred in just two months.² Nearly a year and a half later, Steve Van Kuiken, a global leader of McKinsey Technology, noted that most companies were reporting that they were seven years ahead of where they thought they would be prior to the pandemic, and that organizations were moving to the cloud 24 times faster than they thought.³ As many businesses quickly transitioned to a remote workforce during the early phase of the pandemic, they found that transitioning away from legacy infrastructure and migrating to the cloud was necessary to support business continuity and seamless online collaboration.

For many organizations, Covid-19 brought about fundamental changes in how business was done as they were forced to quickly pivot for the socially distanced era. Companies of all sizes and in all industries accelerated cloud adoption because of the need for flexible computing power, higher availability, better network speed, robust disaster recovery, lower cost for backup, and resiliency for business processes. The cloud

enables businesses to process, store, and manage data in a more efficient and scalable manner, which in turn allows for the transformation of their business models.



Many business have found that transitioning away from legacy infrastructure and migrating to the cloud was necessary to support business continuity and seamless online collaboration.

MANAGING OPERATIONAL CLOUD COMPLEXITY

Digitization has led to increased reliance on the cloud, but rapid migration resulted in some common challenges as well as operational complexities. Network monitoring and security tools designed for legacy infrastructure typically lack proper visibility into cloud environments, creating a visibility gap. In fact, 95% of organizations stated that lack of cloud visibility led to application performance issues.⁴ Without proper



oversight, accidental multi-cloud environments can be created, leading to additional overhead, security risk, and vendor sprawl. On average, organizations use over two public clouds and two private clouds, and cloud adoption continues to accelerate. Managing on-premises systems in addition to cloud presents difficulties; each added environment and application increases the complexity of sharing and protecting data effectively. Organizations must work to gain visibility and control over their cloud environments and applications.

THE IMPORTANCE OF CLOUD SECURITY

Cloud security is essential for realizing successful digital transformation. For instance, ninety percent of organizations increased their public cloud computing usage as a result of the global pandemic.⁵ Misconfigurations, inconsistent security, and security blind spots have resulted from this rush to the cloud. Companies now need to play catch up to address these issues, as well as the risk of malware, data breaches, and compliance violations. The top five areas that should be addressed when building and managing security in the cloud are:

1. Risk of data loss and/or compromise: Caused by user error/accidental deletion, overwriting data, or malicious action.
2. Regulatory compliance: Adhering to industry standards and legal regulations.
3. Resources/skills gap: Lack of skills needed to deploy and maintain cloud-based systems effectively.
4. Complexity: Due to a multitude of systems and services that become too numerous to operate in a reliable way.
5. Deployment/setup: Misconfigurations increase risk of cyberthreat exposure.

An attack on a cloud-based environment can result in data loss, operational downtime, and reputation damage. Successful cloud adoption necessitates effective management, monitoring emerging cyberthreats, and making coordinated security decisions. Unlike on-premises applications, which control access by restricting IP traffic, threat detection in the cloud must shift to the application content and context of the traffic itself. Continual and specific adjustments are required to keep security policies up-to-date, but with limited IT resources and the need for constant app management, these adjustments should be automated for the fastest, most intelligent results. As networks become more complex and distributed, security solutions must bring fragmented infrastructure and deployments under control.^{6,7}

SECURITY CHALLENGES FOR HYBRID AND MULTI-CLOUD MODELS

Security for cloud computing is based on the shared responsibility model, comprised of two components: security of the cloud and security in the cloud. The cloud provider manages the storage, network, and compute layers, while the customer is responsible for implementing controls to protect the application and data. Our experts have highlighted the specific challenges when it comes to securing each of the cloud models:

- Hybrid IT: A type of IT architecture that is a blend of infrastructure and applications located on-premises within a data center as well as one or more cloud-based services. This model allows organizations to maintain control of sensitive assets on site while also utilizing the benefits of the cloud, such as scalability and agility. Security needs to span across all environments and can become a challenge as



organizations become more hybrid and distributed.

- **Hybrid Cloud:** Combines private and public cloud usage so that companies can leverage the advantages of both. Confidential operations can run on a private cloud dedicated to a single organization. Larger applications of a less sensitive nature, or temporary workloads can run on a public cloud, which provides computing services to multiple organizations. Resources span both private cloud assets and public cloud infrastructure. In this cloud model, visibility becomes paramount as security teams must be able to see the entire picture. End-to-end management, segmentation, and secure external connections are the most critical security elements.
- **Multi-Cloud:** Refers to two or more cloud services of the same type (public or private) that are obtained from different vendors. A multi-cloud approach could involve either multiple public or private clouds. A hybrid multi-cloud environment occurs when an organization utilizes multiple public and private clouds. These types of environments typically lack visibility, which generally stems from utilizing disparate management tools provided by different vendors. This lack of visibility can lead to multiple security issues, which can expose organizations to more compromises and vulnerabilities. Response times are often delayed, because the deployed security components are unable to see or talk to each other.⁸

A UNIFIED PLATFORM APPROACH TO COVER ALL CLOUDS

Cloud environments are dynamic by design, and as such, the protection of applications must be fluid. Cloud security needs to adapt to application and data

location, which is best accomplished with a broad, integrated, and automated cybersecurity platform.

An adaptive cloud security solution secures all clouds, cloud networks, applications, and related transactions by protecting workloads both in on-premises data centers as well as in any cloud environment, including private, public, hybrid, and multi-cloud models. This platform approach provides organizations with a consolidated view of their security posture by leveraging a single console for policy management, regardless of cloud infrastructure.

No matter where they reside, all 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 and timely fashion. Adaptive cloud security solutions allow IT teams to securely scale or relocate applications and related transactions, and provide flexibility so that companies may adapt their digital innovation strategy as needed without sacrificing simplicity, security, and operational efficiency. An adaptive cloud security solution delivers consistent policies across the network, and can reduce cost and operational burdens by implementing automated and integrated solutions.

When choosing a cloud security platform, organizations should look for a solution with management framework designed to enable seamless interoperability, full visibility, and real-time communications. An integrated, unified cybersecurity platform approach protects the extended digital attack surface, and works seamlessly with all cloud platforms as well as third-party apps and solutions, providing ease of use and management control. Security solutions should offer broad integration with application programming interfaces (APIs) and third-party apps, and should have



automation enabled as well as artificial intelligence (AI) and machine learning (ML). AI and ML supply real-time data analysis and audit data protection techniques to detect unknown threats and forecast future attacks. This helps IT teams to manage and secure each element in their complex cloud environments, especially with the ongoing cloud skills gap.

A cloud security solution must also integrate a single view and centralized management across all systems operating both on-premises and in the cloud. This single-pane-of-glass management approach can track data flows across the entire network in a format that makes information relevant and actionable, which provides visibility and enables all aspects of the platform ecosystem to function cohesively.^{9,10}

FORTINET SECURE HYBRID CLOUD SOLUTION

The Fortinet Security Fabric addresses the challenges of hybrid and multi-cloud environments by natively integrating with major cloud providers, centrally enforcing consistent security policies, and establishing high-speed and secure connectivity. Security is enhanced through the leveraging of anonymized threat intelligence provided by Fortinet Security Fabric customers around the world.

Fortinet Security Fabric improves protection against known and unknown attacks through third-party integration, and automates actionable responses across hybrid environments. The meshed security network delivers broad visibility across the entire digital attack surface, both on-premises and in multiple clouds, and enables automated, centralized management of the entire security infrastructure

from a single pane of glass. Gartner predicts that by 2024, organizations adopting a cybersecurity mesh architecture will reduce the financial impact of individual security incidents by an average of 90%.¹¹ The virtual and physical components of the Fortinet Security Fabric work together to centrally protect the resulting dynamic infrastructure and secure critical data from the customer to the cloud and back.^{12,13}

KEY FORTINET ELEMENTS THAT PROTECT AND ENABLE HYBRID AND MULTI-CLOUDS:¹⁴

- FortiGate next-generation firewalls (NGFWs) provide secure connectivity, network segmentation, and application security for hybrid cloud-based deployments. They help ensure centralized, consistent security policy enforcement. Connection occurs through a high-speed virtual private network (VPN) tunnel, which protects data without compromising performance. In tests, Fortinet NGFWs blocked 100% of evasions and achieved minimal performance degradation when inspecting encrypted traffic (as compared to competitive solutions). This is crucial as 95% of all network traffic is now encrypted.¹⁵
- FortiGate VMs are virtualized instances of FortiGate NGFWs. FortiGate VMs can securely communicate and share consistent policies with FortiGate NGFWs of any form factor that are provisioned in an on-premises data center.
- FortiManager provides single-pane-of-glass management across the entire extended enterprise including Fortinet NGFWs, switches, wireless infrastructure, and endpoints. FortiManager makes security management for enterprises easier,



enabling security professionals to create and modify policies and objects with a consolidated, drag and drop editor. In addition, devices can be managed in a Security Fabric group as if they were a single device, ensuring that security policies are enforced consistently across all environments. Finally, security professionals can simplify and track changes, and make them auditable through integration with IT service management (ITSM) applications, such as ServiceNow.

- FortiAnalyzer enables organizations to analyze, report, and archive security events, network traffic, web content, and messaging data. A comprehensive suite of easily customized reports simplifies the measurement and documentation of compliance.

CONCLUSION

The global pandemic caused digital transformation to accelerate at an extraordinary rate and fast-tracked migration to the cloud. An adaptive cloud security solution allows your organization to simplify operations, streamline and fortify security, and provides deep visibility across workloads. By leveraging adaptive cloud security tools that evolve as the cloud does, your organization can effectively protect data, devices, and applications within complex hybrid and multi-cloud environments.

Fortinet helps customers with secure digital acceleration into, within, and across clouds using security solutions that are natively integrated across major cloud platforms with the Fortinet Security Fabric, which extends across all hybrid and multi-cloud configurations.



TALK TO WEI TODAY

No matter where you are on your journey to the cloud, WEI can assist your organization with implementing the right adaptive cloud security solution. Contact us to kickstart your cloud security journey.



Sources:

1. Foundry Research commissioned by WEI, December 2021
2. Microsoft 365 Blog, 2 years of digital transformation in 2 months: <https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/30/2-years-digital-transformation-2-months/>
3. Washington Post Transcript, Accelerating Cloud-Driven Transformation with Nasrin Rezai & Steve Van Kuiken: <https://www.washingtonpost.com/washington-post-live/2021/09/27/transcript-accelerating-cloud-driven-transformation-with-nasrin-rezai-steve-van-kuiken/>
4. Keysight Technologies, The State of Cloud Monitoring Report: https://www.keysight.com/us/en/resources.html?srtby=MOST_RELEVANT&q=cloud+monitoring&qlc=en
5. ESG, Beyond Cloud Adoption - How to Embrace the Cloud for Security and Business Benefits: <https://www.devo.com/wp-content/uploads/sites/1/2021/06/ESG-eBook-Beyond-Cloud-Adoption-2021-Final.pdf>
6. Fortinet, Adaptive Cloud Security – Fortify and Enhance Your Cloud Security Platform: <https://www.fortinet.com/content/dam/fortinet/assets/ebook/ebook-adaptive-cloud-security.pdf>
7. Fortinet, Fortinet Security Fabric – The Industry’s Highest-performing Cybersecurity Mesh Platform: <https://www.fortinet.com/blog/business-and-technology/fortinet-security-fabric-the-industrys-highest-performing-cybersecurity-mesh-platform>
- 8,9. Fortinet, Adaptive Cloud Security – Fortify and Enhance Your Cloud Security Platform: <https://www.fortinet.com/content/dam/fortinet/assets/ebook/ebook-adaptive-cloud-security.pdf>
10. Spiceworks, Adaptive Cloud Security – What It means for Modern Enterprise Networks: <https://www.spiceworks.com/it-security/cloud-security/guest-article/adaptive-cloud-security-what-it-means-for-modern-enterprise-networks/>
11. Gartner, Top Strategic Technology Trends for 2022 – Cybersecurity Mesh: <https://www.gartner.com/en/doc/756665-cybersecurity-mesh>
- 12,13. Fortinet, Fortinet Security Fabric – The Industry’s Highest-performing Cybersecurity Mesh Platform: <https://www.fortinet.com/blog/business-and-technology/fortinet-security-fabric-the-industrys-highest-performing-cybersecurity-mesh-platform>
14. Fortinet Solution Brief, Fortinet Secure Hybrid Cloud: <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-secure-hybrid-cloud.pdf>
15. Google Transparency Report, HTTPS encryption on the web: <https://transparencyreport.google.com/https/overview?hl=en>

ABOUT WEI



WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. *Because we go further.*

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 30 years.



 info@wei.com

 www.wei.com

 43 Northwestern Drive | Salem, NH 03079

 800.296.7837