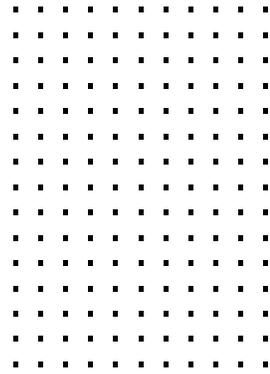


Top Four Considerations to Successfully and Securely Run Critical Applications in the Cloud



Today, nearly all organizations have adopted the cloud to modernize their operations, enable rapid innovation, and accelerate growth. The 2022 Cloud Security Report, a global survey of 823 cybersecurity professionals sponsored by Fortinet, reported that almost 40% of enterprises are running more than half of their workloads in the cloud. Moreover, that percentage is expected to increase to nearly 60% by 2024.¹ Many of these organizations have multiple disparate security solutions deployed, with few that integrate. And with each cloud environment, management complexity increases as each one presents a siloed risk posture and limited remediation capabilities.

Secure Your Critical Applications “Smarter, not Harder”

The same study also revealed a lack of security skills as the top challenge (61%, up from 57% last year) facing many organizations, followed by data protection (53%), understanding how different solutions fit together (51%), and loss of visibility and control (47%).²

Therefore, organizations need to evolve their security strategy and focus on improving operational efficiencies to manage cloud risks proactively. For securing workloads, this means choosing the right cloud-native platform that empowers organizations to effectively work “smarter, not harder” in securing their cloud deployments.

- Maximize the value and effectiveness of your solutions. Cloud-native, integrated security solutions are easier to deploy and manage, can keep pace with rapid changes to the cloud, and can scale quickly as your organization’s needs change. Consider implementing or consolidating solutions with these integrations to simplify your security architecture, achieve broad visibility across your applications and workloads, and help maximize your investments’ value.
- Focus on the most-critical risks to address. Consider integrated cloud-native solutions that can correlate and normalize security data from multiple security technologies and across cloud environments. These cloud-native solutions should also prioritize the most-critical risks to address, to help you focus on the risks that matter the most.
- Simplify security operations to accelerate response and manage the risks. Consider solutions that can monitor and enforce consistent policies and workflows from a single dashboard and can be enabled across multiple clouds to help help your security team minimize gaps in security coverage and improve productivity to secure your cloud footprint consistently.

When selecting a solution to manage your risks when running your critical applications in the cloud, consider the following key points:

Can the solutions integrate with other cloud-native security solutions and across all clouds?

Organizations securing their cloud resources often utilize the cloud service provider’s (CSP) broad range of security service offerings, which are easy to deploy and quick to implement. Given this, organizations should consider solutions that also integrate with the CSP’s cloud-native security services and technologies they have already invested in to minimize integration friction and maximize their value.

Moreover, organizations should look for solutions that offer the broadest integration across the major clouds. This empowers them to have a single platform to manage their workloads with consistent security and experience across all their clouds. A single platform means only learning and building expertise once, resulting in more predictable outcomes and more efficient cloud-security operations.



Can the solutions provide a prioritized view of the most-critical security risks to focus on?

Managing cloud risk is a dynamic process. It is not only about having broad visibility into all the potential new and evolving risks but also having insights into the most-critical risks that require mitigating, as well as accepting manageable risks.

The ideal solutions have integrations with other security tools and services to correlate and normalize security information generated by multiple security technologies and across cloud environments in real time while factoring in security posture, vulnerability, permissions, and threat signals to produce a normalized risk analysis.

Can the solutions simplify security operations and effectively manage the risks?

When it comes to simplifying security, solutions that leverage integrations with other security solutions and services should be easy to activate, cloud-agnostic, and not require expertise in extensive security technologies.

Solutions that enable consistent workflows are essential to help minimize gaps in security coverage across all major cloud environments, alleviating security teams from having to master the intricacies of each cloud platform and their respective security service.

Can the solutions work as part of a cybersecurity mesh platform?

As more applications and workloads are run in the cloud, organizations are faced with greater complexity with less visibility, resulting in blind spots managing both on-premises and cloud deployments. To address this, a cybersecurity mesh platform working in harmony with cloud-native integrations is critical. A cybersecurity platform offers broad, integrated, and automated capabilities to help organizations harmonize enterprise security with their cloud deployments. This powerful combination empowers organizations to benefit from centralized management and visibility, consistent policies, and automated response and operations across the entirety of their deployment. Ultimately, this further helps address cybersecurity skills and resource gaps that many organizations face as it allows organizations to respond faster and more efficiently to threats with the use of artificial intelligence and machine learning.

Conclusion

Fortinet helps secure the digital acceleration of cloud applications and workloads across cloud environments. We do this by providing a friction-free, cloud-native solution that is integrated across major cloud platforms and security technologies alongside the Fortinet Security Fabric. Fortinet helps organizations maximize the value from their cloud-native security investments, as well as investments with the Fortinet Security Fabric to drive greater benefits in operationalizing cloud security. Together, these, along with FortiGuard Threat Intelligence, provide a comprehensive cloud-native security solution that reduces complexity, achieves greater visibility to protect your applications and workloads, and delivers capabilities such as consistent workflows that are enabled across all cloud environments to help you manage and reduce your risk.

¹ [2022 Cloud Security Report](#).

² Ibid.

