Enterprise Strategy Group | Getting to the bigger truth.™

BUSINESS JUSTIFICATION BRIEF

Fortnet on Google Cloud:

Ensuring Consistent Defense-in-depth across On-premises and Cloud-native Workloads

Author: Alex Arcilla, Senior IT Validation Analyst

JUNE 2021

Challenges of Maintaining Security Across Hybrid Cloud and Multi-cloud Environments

As organizations increase their use of public cloud, they continue to reap the benefits of business agility, flexibility, and scalability. Yet, consistently maintaining an organization's security posture across its on-premises and public cloud environments can be difficult and cumbersome. This is especially challenging as traffic moves across core and edge networks and the public cloud.

Implementing numerous and disparate point solutions from multiple vendors addresses a variety of attack vectors but these solutions are difficult to integrate and automate easily and are thus unable to provide consistent defense-in-depth and visibility across organizations' hybrid cloud and multi-cloud environments. Simply put, the adoption of public cloud services has outpaced the maturity of cybersecurity programs to provide the consistency and visibility organizations require to detect and mitigate threats and breaches.

As ESG research has uncovered, respondents have major concerns with securing cloud-native applications running in hybrid clouds and multi-cloud environments, and many are already experiencing security breaches as a result.[1]

ESG data analytics research illuminates the struggle. According to ESG research:

88%
Report having experienced an attack on their cloud-native applications and infrastructure over the past 12 months.

88%
Believe their cybersecurity programs need to evolve to secure their cloud-native applications and use of public cloud infrastructure.

73%
Report that the lack of access to the physical network and dynamic nature of cloud-native applications and elastic infrastructure create visibility blind spots.

Consistent Security and Visibility with Fortinet and Google Cloud

To provide comprehensive defense-in-depth for hybrid clouds, organizations need tools unified by a single underlying security platform so that organizations can apply consistent security policies across all workloads to stay ahead of a rapidly evolving threat landscape. Leveraging Fortinet's Adaptive Cloud Security portfolio in conjunction with security controls provided with Google Cloud helps organizations to enact security policies consistently across on-premises and cloud-native applications.

At the heart of the Fortinet portfolio is the Fortinet Security Fabric that delivers an integrated and automated platform for connecting and protecting workloads deployed within hybrid clouds. This platform approach converges numerous networking and security technologies, enabling organizations to implement a single, simplified, and consistent policy and management framework. With Fortinet's Security Fabric, security gaps can be closed by addressing multiple attack vectors while gaining the broad visibility necessary, across on-premises and Google Cloud deployments, to automatically detect, mitigate, and prevent any potential damage posed by threats and breaches.

Fortinet's Adaptive Cloud Security solutions are deeply integrated with Google Cloud to secure both data in the cloud and a customer's cloud infrastructure. Because security has driven Google's design and development of Google Cloud, security is prevalent in every Google Cloud service. Google has developed a suite of integrated security controls that simplify securing an organization's cloud-resident data and operate in complex hybrid multi-cloud environments. By leveraging Fortinet on Google Cloud, organizations can secure their data in the cloud and the dynamic network boundaries existing within hybrid clouds and multi-cloud environments, enabling simplified and secure cloud on-ramp.

Source: [1] ESG Research Report, *The Maturation of Cloud-native Security*, May 2021.

Why Fortinet?

- Manage risk effectively with broad visibility of the dynamic attack surface.
- Decrease management costs and complexity with integrated solution.
- Reduce operational time and expenses with automated self-healing networks.

The Fortinet Security Fabric offers a security portfolio to mitigate numerous attack vectors via an integrated and automated platform. Fortinet closes security gaps with an end-to-end solution that delivers:

- **Zero trust access**, verifying who and what is on your network to decide on their level of access across networks, endpoints, and the public cloud.
- **Security-driven networking**, integrating an organization's network infrastructure and security architecture so that the hybrid cloud's perimeter can scale and change without compromising security operations.
- **Adaptive cloud security**, securing networks within and across clouds, and enabling effective usage of resources with auto-scaling, dynamic load-balancing, and end-to-end visibility for cloud-native applications.

ESG Business Justification

Leveraging Fortinet on Google Cloud enables organizations to implement an integrated and automated defense-in-depth posture, decreasing the cost and complexity associated with managing multiple cybersecurity products across dynamic attack surfaces throughout IT environments encompassing Google Cloud, the data center, and the edge.

With its single-pane control and management enabled, Fortinet on Google Cloud enables organizations to obtain end-to-end visibility across hybrid clouds, reducing time and costs spent on security monitoring.

To further close security gaps, Google's security culture and powerful technologies (e.g., DLP, IAM, VPC Service Controls, protection from data exfiltration, and access transparency) mitigate the cybersecurity risks associated with cloud-resident data and cloud-native applications.

For organizations that expand their IT environments into multiple public clouds, Fortinet enables the same consistent defense-in-depth strategy with the visibility needed to monitor and control against a single set of security policies.

Why Google Cloud?

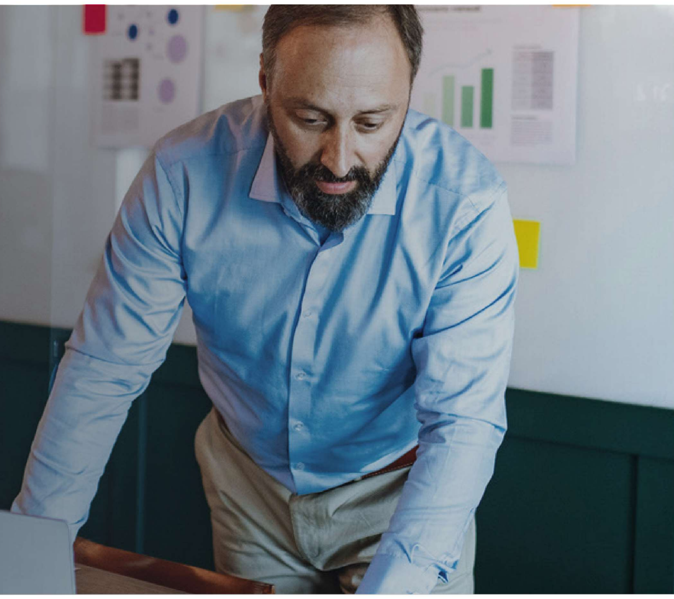
- Google Cloud secures underlying cloud infrastructure to further close security gaps with cloud-native applications.
- Google increases security and reduces management complexity for the growing number of cloud-native IaaS, analytics, AI, and ML workloads deployed in Google Cloud.
- Through Google's Risk Reduction Program, customers can obtain cybersecurity insurance via Google's partnerships with Allianz Global Corporate and Specialty (AGCS) and Munich Re.

The Bigger Truth

When asked about their preferred types of controls to secure cloud-native applications, 73% of ESG survey respondents cited their desire to have a consolidated set of controls based on an integrated platform with coverage across public cloud and on-premises environments in the next two years.[2] With the Fortinet portfolio, unified by the Fortinet Security Fabric, organizations can achieve this consolidation to provide a consistent defense-in-depth security model across hybrid clouds.

The business justification for using Fortinet on Google Cloud is clear. With Fortinet Security Fabric and Google Cloud's security architecture, organizations can enact security policies consistently across workloads deployed within on-premises edge and core networks and within Google Cloud. To reduce overall risk and maintain business agility, ESG strongly believes that Fortinet and Google Cloud are better together in closing cybersecurity gaps for hybrid and cloud-native applications.

Learn More



ESG a division of TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

Source: [2]ESG Research Report, *The Maturation of Cloud-native Security,* May 2021.