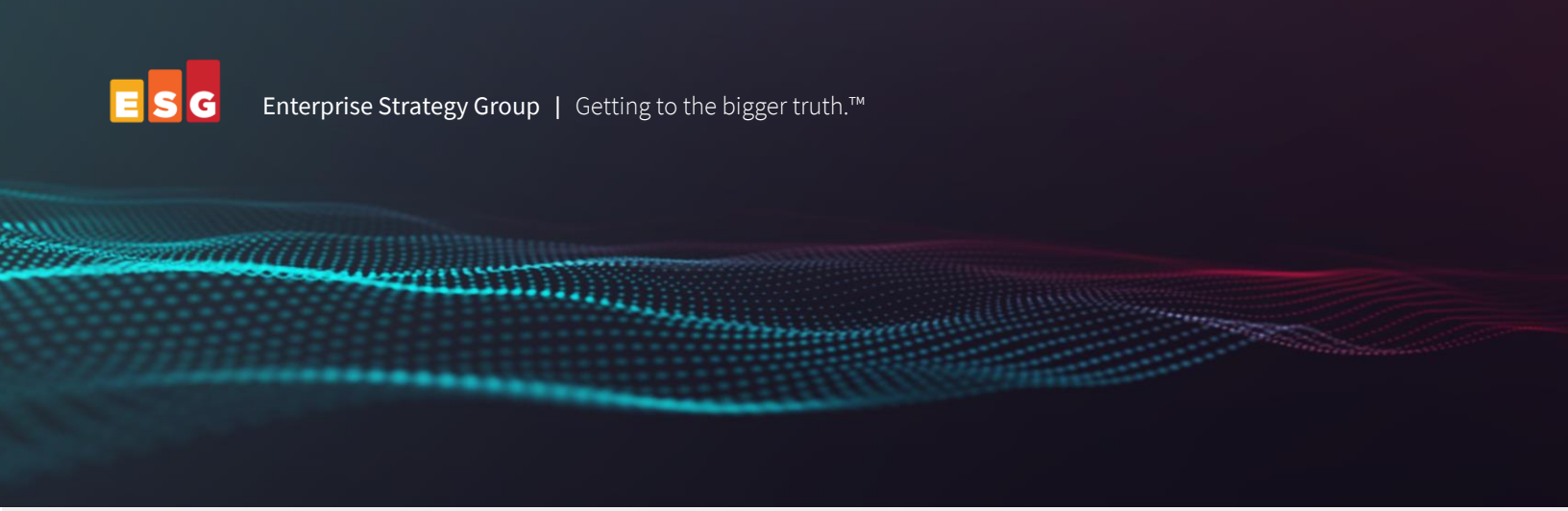


ESG WHITE PAPER

Revisiting a Software-based Approach to Network Security

How Virtual and Containerized Firewalls Can Support the Adoption of Hybrid, Multi-Cloud Environments

By John Grady, ESG Senior Analyst

March 2021

This ESG White Paper was commissioned by Palo Alto Networks and is distributed under license from ESG.

Contents

Executive Summary

The reality of the shift to the cloud is that it is not a singular movement. Most organizations use multiple cloud service providers and application architectures, while in most cases also maintaining on-premises data centers. Due to the fact that security is often a subsequent addition to these environments, many organizations now face a sprawl of network security tools and native cloud controls across the different aspects of their infrastructure.

The results of this fragmentation are typically increased complexity, reduced operational efficiency, and poor security effectiveness. To alleviate these issues, software-based, virtual, and containerized next-generation firewalls that can be deployed across a variety of cloud platforms and application architectures in order to provide consistent, effective protection against a myriad of advanced threats, as well as centralized management across the entire firewall infrastructure, are critical to secure the modern hybrid, multi-cloud enterprise.

Software-based, virtual, and containerized next-generation firewalls that can be deployed across a variety of cloud platforms and application architectures in order to provide consistent, effective protection against a myriad of advanced threats, as well as centralized management across the entire firewall infrastructure, are critical to secure the modern hybrid, multi-cloud enterprise.

Enterprise Environments Continue to Grow in Complexity

According to a recent ESG survey of senior IT professionals from a wide range of industries, including manufacturing, financial services, healthcare, communications and media, retail, government, and business services, more than three-quarters of organizations believe that IT complexity has increased over the past two years. Respondents cited a variety of reasons they believe this is the case, including changing work patterns due to the COVID-19 pandemic, privacy regulations, the threat landscape, and other outside factors. Yet many organizations point not to these external factors, but to the very tools they employ to support the business as the biggest reasons for IT complexity. Specifically, 29% indicated that the need to use both on-premises data centers and public cloud providers was a leading driver of IT complexity.[1]

Cloud Adoption is Ubiquitous and Sprawling

Cloud usage has only continued to increase over time, with the percentage of organizations reporting the usage of infrastructure-as-a-service (IaaS) reaching 78% in 2021, up from 42% in 2017. However, along with the more pervasive usage of IaaS is an increase in the number of cloud service providers used by enterprise organizations. Nearly four-fifths (78%) of organizations using IaaS report doing so across at least two cloud service providers (CSPs).

Many organizations have prioritized the use of multiple CSPs, and view doing so as a strategic imperative.

In some cases, the progression towards multiple CSPs is a result of natural sprawl over time and the by-product of the self-service nature of cloud. Yet many organizations strategically decide to use more than one CSP to delineate development or test environments from those running production applications, to ensure availability across different geographies, for disaster recovery purposes, or simply to avoid vendor lock-in. Whatever the reason, just over half (51%) of the organizations using multiple CSPs indicated that they do so in a meaningful way, as opposed to relying on a primary CSP and only using a secondary

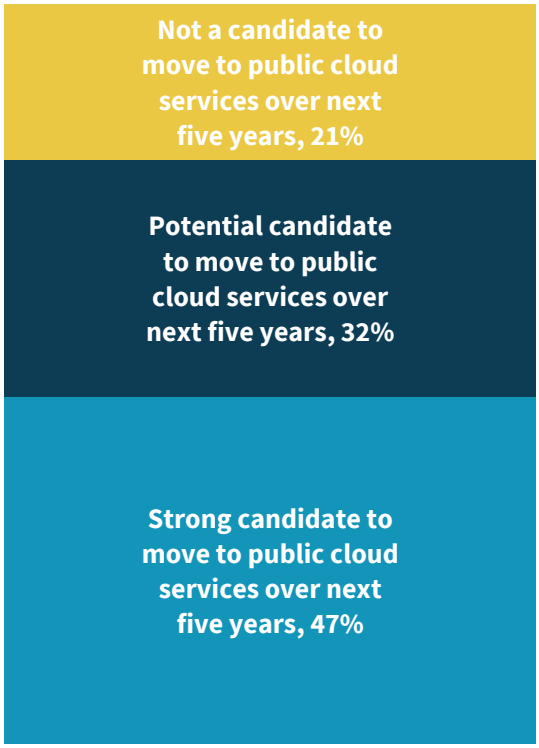
[1] Source: ESG Research Report, *2021 Technology Spending Intentions Survey*, January 2021. All ESG research references and charts in this white paper have been taken from this research report, unless otherwise noted.

provider for smaller, discrete purposes. This indicates that many organizations have prioritized the use of multiple CSPs and view doing so as a strategic imperative.

Yet it is important to remember that while most organizations accelerate their march to the cloud and expect many of the workloads currently run in on-premises data centers to be candidates for cloud migrations over the next 5 years, a number of applications and workloads will remain on-premises (see Figure 1). In other words, many organizations will continue to support hybrid cloud environments.

Figure 1. Likelihood Workloads Will Move to the Public Cloud

Think about all of the applications and workloads that your organization currently runs in your on-premises data centers. What percentage of these workloads are/aren't candidates to move to public cloud services over the next five years? (Mean, N=664)



Source: Enterprise Strategy Group

Heterogenous Architectures Are Expanding

75% of ESG research respondents said they were currently using containers for production applications.

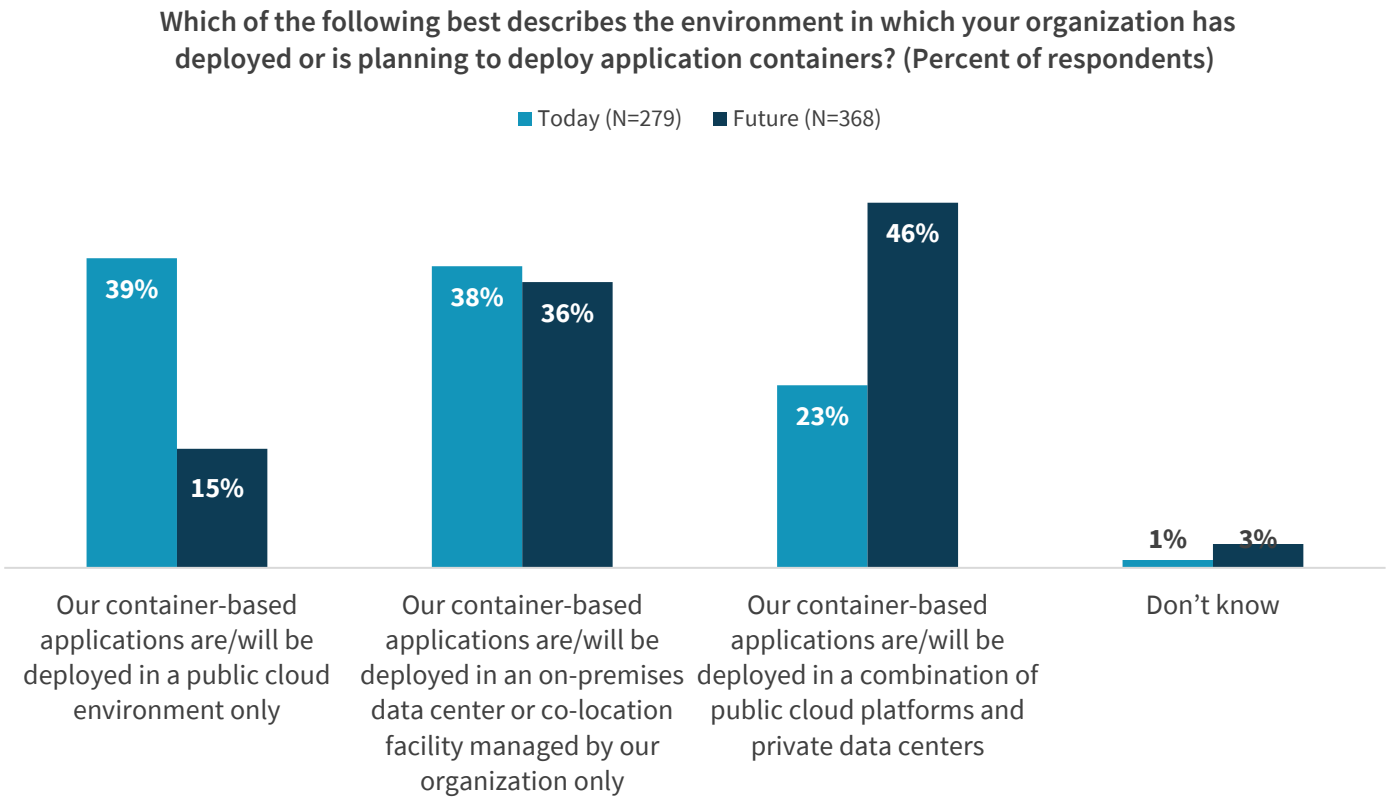
In addition to shifting resources to the cloud, many organizations are accelerating their reliance on microservices-based application architectures through the use of containers. When paired with DevOps methodologies, these approaches enable organizations to be more agile in their application development processes. Further, many organizations have moved beyond the experimentation phase with regards to containers. In fact, 75% of ESG research respondents said they were currently using containers for production applications, as opposed to for dev/test or staging purposes.[2]

However, while container-based architectures may be cloud-native, that does not mean they will always be public cloud resident. In fact, nearly half (46%) of organizations anticipated deploying container-based applications across both public

[2] Source: ESG Master Survey Results, *Leveraging DevSecOps to Secure Cloud-native Applications,* December 2019.

cloud platforms and private data centers (see Figure 2).[3] This further illustrates the hybrid cloud model many organizations will continue to follow, even with regards to modern application architectures. Ultimately, the blending of different CPSs, infrastructures types, and locations further adds complexity from a security perspective.

Figure 2. Location of Container-based Applications



Source: Enterprise Strategy Group

Security Teams Struggle to Keep Pace

Cybersecurity continues to be a strategic imperative for most organizations, and there is no shortage of spending specifically allocated to secure these hybrid, multi-cloud environments. In fact, 59% of organizations expect to increase their spending on cloud infrastructure security over the course of 2021, more than any other security segment.

59% of organizations expect to increase their spending on cloud infrastructure security over the course of 2021.

However, regardless of the amount spent, simply purchasing tools does not in and of itself improve security, especially if those tools are not well suited for the broader enterprise environment they are put in place to protect. With regards to cloud-native applications, organizations report a variety of security challenges when it comes to securing these environments (see Figure 3). These include:

- Inconsistency across different locations (43%). Unsurprisingly, the most common challenge organizations cite with regards to securing cloud-native applications is maintaining security consistency across the different locations and platforms inherent in hybrid multi-cloud environments. Typically, the on-premises data center and its associated

[3] Source: ESG Master Survey Results, *Leveraging DevSecOps to Secure Cloud-native Applications,* December 2019.

security solutions are well established, with new tools being added as an organization's cloud footprint expands. These tools are often managed in silos, meaning configurations, policies, and protections must be replicated (typically manually) across each different location. In addition to the fact that the functional capabilities often differ across these tools, the opportunity for human error increases substantially.

- Increased cost and complexity (35%). The complexity that comes from using multiple security tools has been discussed. However, both direct and indirect costs result from having to use multiple tools. Rather than developing a deeper relationship with a limited number of vendors and seeing procurement benefits based on that, spending is spread across multiple vendors with fewer economies of scale. Operationally, managing similar but different tools in parallel across different locations is inefficient and can be time-intensive. Additionally, the training and certification requirements across these different toolsets can add significant indirect costs.

- The dynamic threat landscape (35%). Attackers continue to evolve their methods to stay ahead of defenders, but seemingly nowhere is this truer than with regards to cloud. In cloud environments, attacks exploiting insecure configurations, known or unknown vulnerabilities, insecure APIs, and malware are all common. Many of these issues were prevalent on-premises as well. However, the speed and scale at which organizations operate in the cloud can make understanding, tracing, and protecting these potential avenues of attack much more complex. Further, the interconnectivity between cloud and on-premises environments can allow threats to easily move across the environment and evade detection.

- Limited visibility (33%). Cloud environments are obviously very different than on-premises data centers. Not owning the end-to-end infrastructure provides a different level of visibility, which many organizations struggle to adapt to. Modern cybersecurity is predicated on having deep visibility and being able to apply advanced analytics and detection mechanisms to network traffic. The blind spots and inefficiencies resulting from securing a hybrid, multi-cloud environment with a collection of different point tools makes it more difficult to sift through the significant amounts of noise to pinpoint connections that are likely to be malicious.

- Organizational issues (33%). In addition to the challenges posed by tools, the shift to more DevOps-focused methodologies, sometimes resulting in decentralized security responsibilities, continues to be an obstacle. Alignment across groups (security, infrastructure, and developers) is required so that developer and cloud teams understand security requirements and priorities and security teams adopt more agile processes and work to more effectively enable the business. That said, tools are important in this instance as well—security solutions that plug into development processes and continuous integration and continuous delivery (CI/CD) pipelines and tools to provide more dynamic deployment and automation can help address these organizational challenges.

Figure 3. Challenges of Securing Cloud-native Applications

Source: Enterprise Strategy Group

Modern, Hybrid Cloud Environments Require a Software-based, Platform Centric Network Security Approach

Despite the broader technology industry transition to cloud, the network security market, and firewalls specifically, have remained more rooted in appliance-centric architectures. There remain use-cases for which an appliance-based architecture may be the most logical:

- Data center ingress/egress inspection where performance is critical.
- Campus perimeters supporting broad security functionality.
- Branch locations when cloud-delivered security may not be desirable for one reason or another.

However, for modern, cloud-centric environments, a software-based approach is preferrable. That said, simply virtualizing an appliance-based solution does not address the fundamentally different nature of cloud-native approaches and may not offer the capabilities to support the numerous platforms and architectures used in these types of environments.

Native cloud tools from CSPs may be designed specifically for cloud environments. However, these tools can only support a single CSP's platform, contributing to the tool sprawl responsible for many of the security challenges discussed earlier, especially among the many organizations using multiple providers. Further, CSPs may have varying levels of focus on security, leading to gaps in capabilities and efficacy. As a result, network security solutions targeted towards securing hybrid multi-cloud environments should include the following capabilities.

Coverage Across Multiple Locations and Platforms

To support modern on-premises data center requirements, virtual firewalls must integrate seamlessly with on-premises data center and private cloud infrastructure and software-defined networking solutions. This enables security teams to efficiently enforce granular segmentation, inspect permitted traffic between applications and services for threats, and ensure that security automatically and consistently scales with the environment. Additionally, support for all leading cloud service providers to deliver threat prevention at the perimeter of the environment is no longer an additional benefit but a requirement to meet the needs of cloud-first organizations.

Finally, and perhaps least often considered, is integration with and support for Kubernetes to protect container-based environments. Organizations often must choose between using traditional firewalls residing outside the container environment (necessitating traffic hairpinning and resulting in reduced visibility); using basic segmentation that lacks threat prevention or traffic inspection; or worse, ignoring the issue all together. Further, security teams often lack visibility into the range of applications running in Kubernetes. Containerized firewall solutions that deploy within Kubernetes or hosted environments such as Amazon Elastic Kubernetes Service (EKS), Google Kubernetes Engine (GKE), and Azure Kubernetes Service (AKS), can give security teams the visibility they require to provide consistent security across all the locations in which containers reside, while natively integrating with the tools DevOps teams regularly use.

Centralized Management

Even if a solution has coverage across different locations and platforms, the benefits in protecting heterogenous environments are reduced if the management across those locations remains siloed. The ability to write policy once and replicate across different parts of the environment through a single pane of glass improves efficiency and reduces the opportunity for human error. Integrating with DevOps tools ensures that security controls are properly configured prior to the push to production.

The ability to write policy once and replicate across different parts of the environment through a single pane of glass improves efficiency and reduces the opportunity for human error.

But further, automation capabilities supported by machine learning can provide policy recommendations and catch misconfigurations in real time and have become a critical requirement to keep pace with dynamic cloud environments. Finally, role-based access control (RBAC) is important to ensure that administrators only have management rights for aspects of the infrastructure for which they are responsible. For example, cloud operations teams may need access to logs or reports to troubleshoot, while configuration ownership remains with the network security team.

Highly Effective Threat Prevention

Despite the shift towards platform-based approaches, the ability to prevent and detect threats remains by far the top purchasing criteria, as cited by 41% of ESG research respondents. By comparison, the second most cited consideration was cost (12%).[4] In the context of software firewalls, this starts with full next-generation firewall (NGFW), layer 7 visibility and is

[4] Source: ESG Master Survey Results, *Enterprise-class Cybersecurity Vendor Sentiment*, March 2020

extended through a subscription-based platform model. This approach provides increased flexibility and scalability to consume a broader range of security services over time in order to protect against more varied threat vectors and attack types as they emerge.

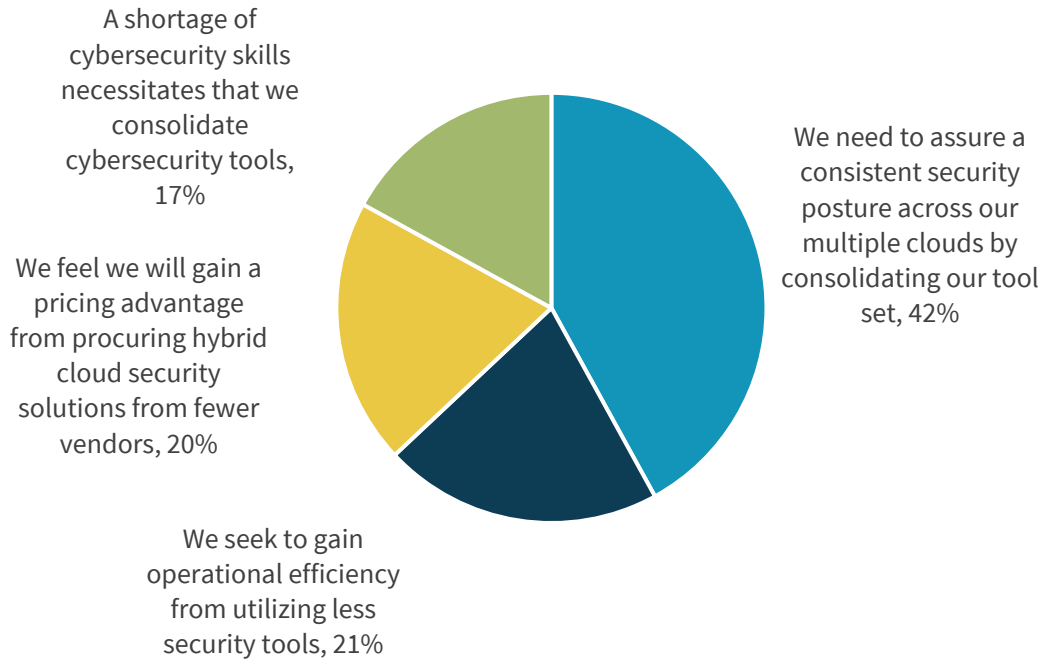
Native cloud offerings from cloud service providers may be limited to stateful firewall inspection and port blocking. In the same way that NGFW products replaced traditional firewalls at the perimeter, it has become clear that cloud environments require highly effective threat protection, supported by machine learning and analytics, to accurately detect and block advanced attacks, including zero-day exploits that have never been encountered before. This should include intrusion prevention capabilities to ensure compliance, advanced malware protection to prevent ransomware and zero-day attacks, URL filtering to protect outbound traffic to developer resources and other internet-based assets and repositories, DNS security to identify and block command and control traffic, and data loss prevention (DLP) to prevent data exfiltration and help maintain compliance.

Consistency and Cost Savings Are Expected from a Consolidated Approach

Organizations that plan to converge security capabilities across their cloud-native environments anticipate not only better security, but both direct and indirect cost savings (see Figure 4). Specifically, 21% expect to gain operational efficiencies. This could come through more consistent management across locations, streamlined policy creation, and even reduced training and certification requirements. Further, 20% believe sourcing solutions from fewer vendors will result in reduced product costs.[5]

Figure 4. Drivers for a Platform-based Approach

What is the primary reason your organization plans to consolidate controls by employing suites and platforms from a smaller number of vendors? (Percent of respondents, N=187)



Source: Enterprise Strategy Group

[5] Source: ESG Master Survey Results, *Leveraging DevSecOps to Secure Cloud-native Applications,* December 2019.

Palo Alto Networks' Comprehensive Approach for Hybrid Cloud Environments

Palo Alto Networks is well known for leading the market transition from traditional to next-generation firewalls. But in addition to providing protection for campus and branch offices, the vendor has a long history securing data center environments. Further, it continues to innovate across its portfolio to address changing data center and cloud requirements. In addition to cloud-native capabilities such as cloud security posture management, cloud workload protection, and cloud access security broker, Palo Alto Networks has transitioned its network security portfolio to a more cloud-centric focus with its virtual and containerized software firewall products. These virtual and containerized firewalls are managed through the Panorama management console, which provides centralized policy management, visibility, and response across both appliance and software-based Palo Alto firewalls.

VM-Series Firewall

VM-series firewalls provide the same ML-based NGFW protection as PA-series appliance-based firewalls but in a software form factor. Integrations with infrastructure providers such as VMware, Cisco, Nutanix, and Red Hat support data center and private cloud environments for use cases such as advanced network segmentation with threat prevention, virtual desktop infrastructure security, and achieving compliance in highly regulated environments. Additionally, VM-series firewalls are available across all major public cloud services providers (AWS, Azure, Google, IBM, Oracle, and Alibaba) to provide advanced network segmentation with threat prevention both between and within VPCs and VNETs to secure the cloud perimeter.

CN-Series Firewalls

CN-series firewalls are deployed natively in Kubernetes as two containers, one each for the data plane and management plane. This ensures the protection not only of inbound and outbound traffic, but east/west flows as well. Firewalls are deployed natively through Kubernetes, ensuring consistent, streamlined provisioning as part of the DevOps workflow. While deployment is integrated into the CI/CD pipeline, policy can be managed through Panorama, just as with hardware and virtual Palo Alto Networks firewalls.

The Bigger Truth

More than twenty years ago, Bruce Schneier said "complexity is the worst enemy of security." That was prior to the introduction of cloud computing generally, let alone the hybrid, multi-cloud reality most organizations now navigate daily. As new infrastructure models and threat vectors emerge and add to enterprise complexity, the tendency is to add new security controls to address those dynamics and close gaps in the enterprise's security posture. This approach, while necessary, can reach a tipping point where the proliferation of new controls causes more problems than it solves. The network security of hybrid multi-cloud environments has reached this milestone. However, by shifting to a consolidated software-firewall approach that consistently addresses the variety of cloud platforms and architectures in use today, organizations can begin to reduce that complexity.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com

contact@esg-global.com

508.482.0188