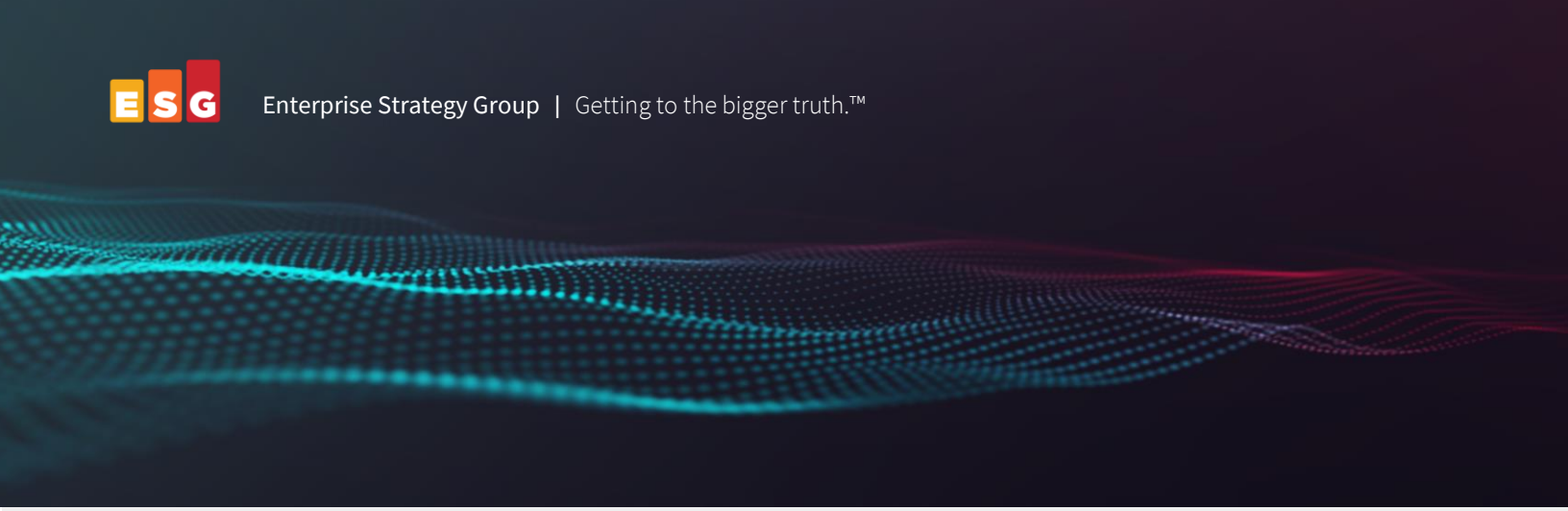


ESG WHITE PAPER

The Role of a Hybrid Approach on the Journey Towards Cloud-delivered Secure Web Gateway

By John Grady, ESG Senior Analyst

April 2021

This ESG White Paper was commissioned by Symantec, a Division of Broadcom, and is distributed under license from ESG.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Contents

Executive Summary 3

The Transition Towards the Hybrid Workplace 3

Work is What You Do, Not Where You Are 3

Challenges with Network Security Tools Complicate the Issue 4

Security Approaches Are Evolving But Will Not Be Rearchitected Overnight 5

Reasons for Maintaining an On-premises Secure Web Gateway 6

Managing an Incremental Shift to the Cloud 7

Addressing Regulatory Concerns 8

Preference for On-premises Solutions 8

Key Requirements for a Hybrid Approach to Secure Web Gateway 8

Centralized Management 9

Broad, Consistent Functionality 9

Flexibility 9

The Bigger Truth 9

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Executive Summary

The impact of the pandemic has obviously highlighted the shift to remote work and, as a result, the importance of cloud-delivered solutions to support enterprise agility, flexibility, and resilience. Yet as much as the pandemic has accelerated cloud adoption, the reality remains that many enterprises take a more incremental approach to cloud migration and will continue to transition on-premises applications and services to the cloud slowly over time.

The cybersecurity space is no different in this respect, and as far as the secure web gateway market has come with regards to the shift to cloud, the fact remains that on-premises tools have not disappeared and are unlikely to any time soon. Whether due to compliance concerns, network complexity, or simply preference, many organizations will continue to manage on-premises secure web gateways as part of a hybrid approach, while progressing to the cloud over time.

Whether due to compliance concerns, network complexity, or simply preference, many organizations will continue to manage on-premises secure web gateways as part of a hybrid approach, while progressing to the cloud over time.

The Transition Towards the Hybrid Workplace

The pandemic has forced most companies to reassess their IT strategies to better support a work-from-home model. Many organizations have accelerated their investments in cloud services, collaboration tools, and secure remote access solutions to ensure users are able to continue to be productive outside of corporate locations. Yet as transformative as these shifts have been for many, there remains an expectation that the post-pandemic professional world will revert to something similar to what it was in January 2020.

Work is What You Do, Not Where You Are

Without a doubt, the biggest shift over the last 12 months has been the explosion in the percentage of employees working from home. Prior to the pandemic, there were notable examples of companies mandating office attendance and limiting the ability to work from home, even within the IT industry itself.

72% of IT decision makers say their organizations are becoming more pro work-from-home over the course of the pandemic, indicating a more lasting embrace rather than grudging acceptance of this change.

Yet for most of 2020, companies had little choice but to embrace remote work and build out an infrastructure to support that priority. As one might expect, this has led many to update their views on remote work overall. In fact, ESG research has found that 72% of IT decision makers say their organizations are becoming more pro work-from-home over the course of the pandemic, indicating a more lasting embrace rather than grudging acceptance of this change.[1]

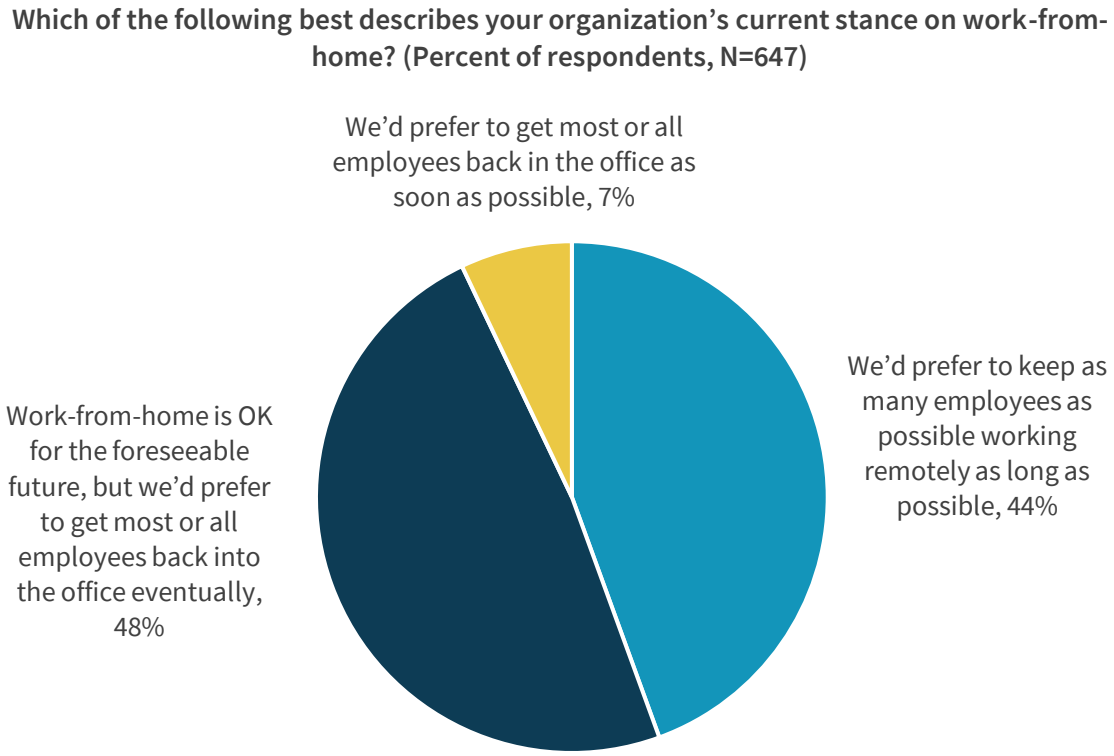
Even with that being the case, many organizations are already back to supporting some level of office activity, and this will likely continue to increase. Specifically, ESG research has found that nearly half (48%) of organizations would prefer to get most or all employees back into the office at some point in the future (see Figure 1).[2] While this will not necessarily mean that employees will be required to work from corporate offices 5 days per week, the fact that most organizations will

[1] Source: ESG Master Survey Results, *2021 Technology Spending Intentions Survey*, December 2020.
[2] Ibid.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

continue to utilize office environments means they will need the associated network and security infrastructure to support these locations.

Figure 1. Over Half of Organizations Will Look to Resume Office Activities



Source: Enterprise Strategy Group

Challenges with Network Security Tools Complicate the Issue

Exacerbating the work-from-home trend and anticipated hybrid workplace model many will use once the pandemic subsides are the challenges organizations cite with regards to network security tools used in their environments. These include:[3]

- Inconsistent management across physical and cloud or virtual environments (44%). Whether managing different form factors of the same tool, or different tools securing different parts of the environment, the operational inefficiencies and potential for human error when replicating policy across management consoles make a siloed approach ineffective.
- Performance issues that negatively impact user experience (42%). As important as security is, it cannot come at the expense of the user experience or employee productivity. Solutions must be able to provide effective threat prevention while simultaneously enabling users to effectively do their jobs with no interruption or latency.
- Too many disparate tools (36%). Most organizations have dozens of tools across a similar number of vendors. This leads to inefficiencies and additional costs from a product management and procurement perspective. Negotiating

[3] Source: ESG Master Survey Results, *Network Security Trends*, March 2020.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

and navigating multiple contracts, managing different update cycles, and ensuring staff are properly trained across different tools are some of the issues driving many to look for consolidation wherever possible.

- Difficulty implementing (33%). Enterprise environments have become so complex and interconnected that deploying a new tool is not always straightforward. Ensuring the proper configurations, policies, and access controls are in place is often time consuming and laborious.

- Lack of scalability (25%). Today's IT environment is so dynamic that solutions may have difficulty keeping pace with the near constant rate of change required to meet the changing needs of the organization. While the example of scaling up support for employees working from home is top of mind after the last year, the reality is that, moving forward, organizations will need to think about flexing services up or down to meet the changing needs and shape of the business.

Security Approaches Are Evolving But Will Not Be Rearchitected Overnight

In part to address these challenges, the pendulum has been swinging towards cloud-delivered and software-as-a-service (SaaS) oriented security for a number of years. The pandemic certainly highlighted some of the benefits afforded by this type of approach for supporting a distributed workforce. Nowhere is the trend towards cloud clearer than with regards to secure access service edge (SASE). The concept of a cloud-centric solution converging a variety of security tools has generated a significant amount of interest over the last 18 months, with organizations anticipating improved security, better user satisfaction, centralized management, and more agility to rollout security services and updates faster.

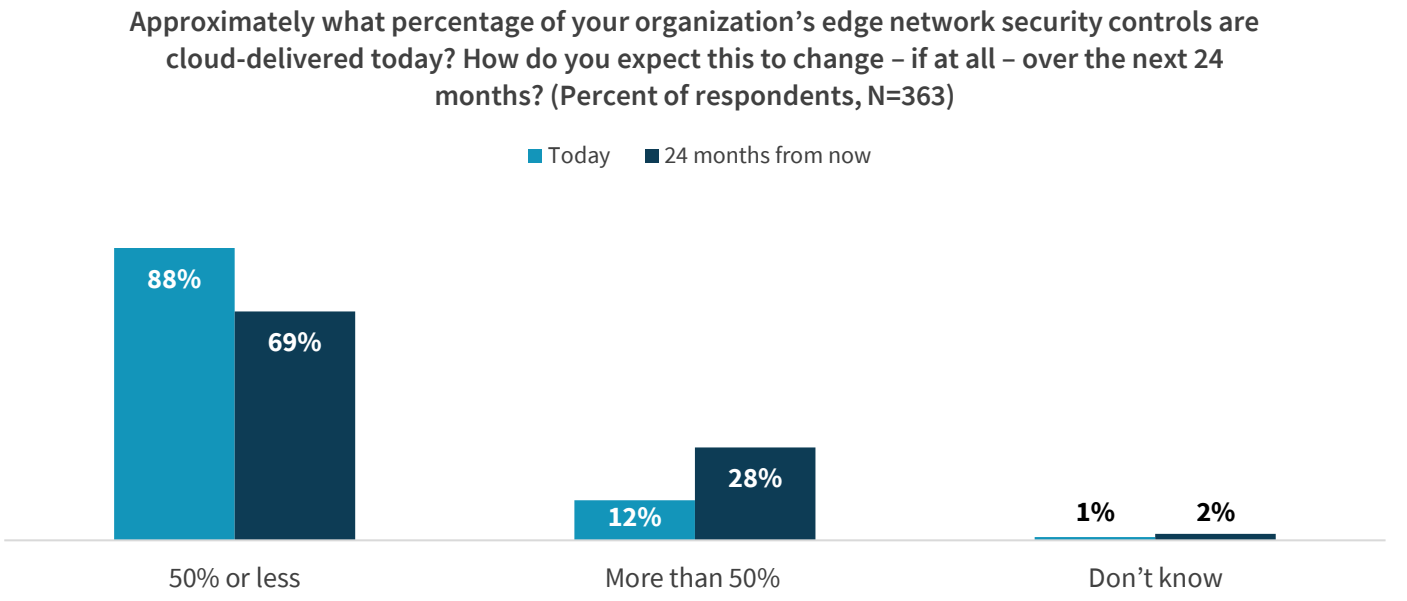
While the percentage of cloud-delivered perimeter network security solutions is expected to increase notably, the reality is that on-premises solutions will not disappear any time soon.

Yet while the percentage of cloud-delivered perimeter network security solutions is expected to increase notably, the reality is that on-premises solutions will not disappear any time soon. In fact, ESG research has found that even while the percentage of organizations expecting more than half of their perimeter network security controls to be cloud-delivered in the next 2 years will markedly increase from today (i.e., 12% to 28%), the majority (69%) still anticipate that half or fewer of their tools will be cloud-delivered (see Figure 2).[4] This staged shift to the cloud is further evidenced by the fact that, with regards to SASE specifically, there is still a strong appeal for hybrid options to enable organizations to transition over time to a fully cloud-delivered model. ESG has found that 33% of research respondents rank support for hybrid architectures as a top-3 attribute of SASE.[5]

[4] Source: ESG Master Survey Results, *Transitioning Network Security Controls to the Cloud*, July 2020.
[5] Ibid.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 2. The Percentage of Cloud-delivered Perimeter Network Security Tools



Source: Enterprise Strategy Group

Reasons for Maintaining an On-premises Secure Web Gateway

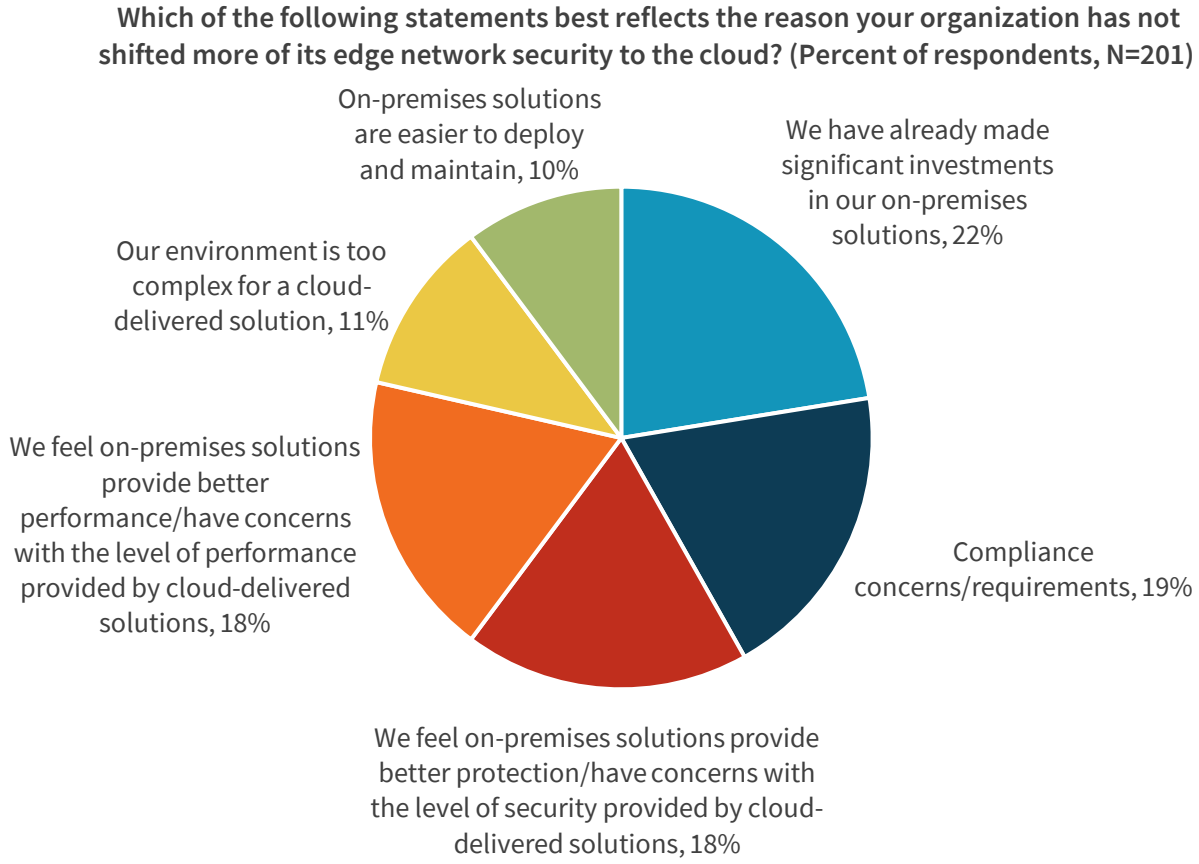
The secure web gateway (SWG) market was one of the first in the network security space to begin to transition to a SaaS model. Supporting branch office and local internet breakouts was the first use case, but that has expanded over time to include remote users and, for some, even company-wide SaaS deployments. Yet nearly a decade after the first versions of cloud-delivered SWGs were introduced, ESG research has found that 95% of enterprise organizations continue to use an on-premises, appliance-based solution as part of their access control and management network security strategy.[6]

In the context of the daily routine of many knowledge workers, secure web gateways represent the tip of the spear of an organization's threat prevention capabilities. Enforcing corporate policy with regards to web usage, preventing malware downloads, enforcing data loss prevention policies, and providing a level of control over application usage are all supported by SWG solutions. With that criticality as the backdrop, there are a few key reasons organizations may incrementally move to the cloud while continuing to manage an on-premises approach (see Figure 3).[7]

[6] Source: ESG Master Survey Results, *Network Security Trends*, March 2020.
[7] Source: ESG Master Survey Results, *Transitioning Network Security Controls to the Cloud*, July 2020.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 3. Reasons for Using On-premises Security Tools



Source: Enterprise Strategy Group

Managing an Incremental Shift to the Cloud

Many cloud migration projects occur over multiple years. The scale of enterprise infrastructure and applications simply does not allow for the shift to occur all at once. As a result, organizations must assess the performance of existing on-premises applications and services and weigh the criticality of shifting them to a cloud platform.

Organizations must assess the performance of existing on-premises applications and services and weigh the criticality of shifting them to a cloud platform.

Those that are performing well may be deprioritized as candidates for cloud migration in the short or moderate term. If the solution performs as required under the current deployment model, focusing cloud migration strategies on less effective parts of the environment can yield more positive impacts.

Additionally, the "lift and shift" scenario does not always play out as easily as it sounds, especially for larger enterprises. No security tool operates in a silo. Secure web gateways are no exception and often integrate with other solutions from the same or third-party vendors to support advanced threat protection, data loss prevention, DNS, CASB, or other capabilities. Reconstructing these integrations, as well as routing and policy models, may serve as an additional barrier to cloud migration. Finally, advanced tools such as network detection and response (NDR) and full packet capture (PCAP) may also be customized to run within the existing architecture and be difficult to meet enterprise needs in the cloud.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Addressing Regulatory Concerns

The introduction of expansive regulations such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) have forced organizations to weigh and balance security requirements with employee privacy, especially as it relates to the decryption and inspection of network traffic. In some geographies and industries, performing this type of inspection in the cloud, potentially in datacenters outside the country of origin, can either run afoul of the regulations themselves or increase the complexity of ensuring the proper safeguards and mitigations are in place to protect personal data. As a result, some organizations continue to deploy security tools on-premises to meet data residency requirements and limit complexity.

Preference for On-premises Solutions

Finally, some organizations simply prefer on-premises approaches. ESG research has found that 18% believe on-premises tools provide better protection compared to SaaS.[8] The flexible customization and architecture design options on-premises tools provide, which are not always available with cloud-delivered solutions, is a likely reason for this.

This may seem counterintuitive at first, as one of the main value propositions of the cloud is always-on updates. However, effective on-premises solutions will leverage cloud-enabled back-end resources to collect telemetry and apply intelligence to ensure the most up-to-date protections are applied to inspected traffic.

Effective on-premises solutions will leverage cloud-enabled back-end resources to collect telemetry and apply intelligence to ensure the most up-to-date protections are applied to inspected traffic.

Similarly, 18% believe on-premises solutions provide better performance compared to cloud alternatives.[9] This is critical with regards to maintaining a consistent user experience. Again, the cloud narrative is predicated on putting protections closer to the user. This makes perfect sense in a remote worker or remote office scenario where the alternative is backhauling traffic to the corporate datacenter. However, when in a main office location, using an on-premises stack is unlikely to result in increased latency when compared to a cloud solution, though the specific results depend upon the capacity of the on-premises solution, the location of the office as compared to the cloud resources the user is accessing, and the infrastructure of the cloud provider (PoPs, peering footprint, etc).

Key Requirements for a Hybrid Approach to Secure Web Gateway

As noted, nearly all enterprises indicate they use an on-premises secure web gateway. However, a similar percentage of respondents (93%) also report using cloud-delivered SWGs as part of their access control and management network security strategy.[10] This significant overlap highlights the prevalence of a hybrid approach in the market in order to protect employees across different locations, support a variety of use cases, and ensure regulatory compliance where applicable.

However, implementing a successful hybrid secure web gateway approach requires much more than simply mixing and matching on-premises and cloud-delivered tools. A hybrid solution must seamlessly integrate the different appliance, virtual, cloud-delivered, and SaaS components of which it is comprised. Further, to ensure consistent protection across the entire enterprise, scale with the organization as its needs change, and better enable security teams to be effective and efficient, hybrid solutions (and the on-premises component specifically) should include the following attributes:

[8] Source: ESG Master Survey Results, *Transitioning Network Security Controls to the Cloud*, July 2020.
[9] Ibid.
[10] Source: ESG Master Survey Results, *Network Security Trends*, March 2020.

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Centralized Management

Modern secure web gateways must provide a centralized management experience for administrators regardless of how the solution is deployed. Policy language and construct must be universal and intuitive to ensure the correct protections are in place regardless of where a user may be located. By streamlining the number of consoles administrators must be trained and proficient on, while reducing duplicative management tasks, organizations can gain operational efficiencies and free security personnel to work on more proactive assignments.

Additionally, centralized reporting across both on-premises and cloud tools supports more robust analytics practices to uncover threats and other issues more efficiently. Rather than having to manually correlate information from different tools, an aggregated view enables security teams to efficiently analyze the data and improve incident response.

Broad, Consistent Functionality

Similarly, the level of protection must be consistent across on-premises and cloud instances This requires feature parity to ensure threats can be accurately identified and blocked regardless of where the user is. Modern secure web gateways should have a strong proxy architecture as a foundation, supported by web filtering, SSL decryption, advanced malware protection, data loss prevention, and cloud access security broker features. Advanced capabilities such as sandboxing and web browser isolation are increasingly required to protect organizations from zero-day threats. These capabilities (whether from a single or multiple vendors) must be consistently available across all parts of the solution, regardless of location. Additionally, the timing of updates must be comparable across both on-premises and cloud deployments.

Flexibility

The described management and functional requirements can be supported by cloud-enabled on-premises tools. In this model, the on-premises tool is reinforced by cloud capabilities, which could include pulling in real-time threat intelligence from a global network of users or offloading compute-intensive functions such as isolation and emulation. Even the centralized management aspects described above can be supported through a cloud user interface.

In a cloud-enabled model, the on-premises tool is reinforced by cloud capabilities, which could include pulling in real-time threat intelligence from a global network of users or offloading compute-intensive functions such as isolation and emulation.

From a packaging and pricing perspective, the ability to transition on-premises controls to the cloud seamlessly when organizational needs change provides investment protection and a clear roadmap to shift towards a more cloud-centric hybrid approach over time. This is facilitated through subscription-based, user-focused pricing supported across on-premises hardware, virtual appliance, private cloud, or SaaS deployments. In this model, organizations would purchase hardware for use in traditional, on-premises deployments. However, the security services running on the appliances would be subscriptions that are transferrable to virtual machine or SaaS deployments. This approach reduces CapEx by shifting the associated services to an OpEx model, and more closely aligns to cloud consumption, providing longer-term cost certainty. All these aspects help provide enterprises with a more flexible, and ultimately effective, secure web gateway experience.

The Bigger Truth

The world is rarely one of absolutes, and the IT space is no different. Every company is unique, and the complexity of modern enterprise networks leads to a variety of different needs across the environment. The shift to cloud is often

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.

discussed in general terms and with an unspoken presumption that everyone is doing it the same way and that it is happening all at once.

Yet, there is nuance behind the transition to cloud and the reality is that many organizations continue to support a variety of applications and services on-premises. This is not to say that on-premises solutions can remain static. Rather, by incorporating cloud attributes such as centralized management and subscription pricing, and by augmenting functionality with cloud-enabled capabilities, on-premises tools can provide the flexibility required as part of a hybrid approach and support an incremental transition to cloud over time.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

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

© 2021 by The Enterprise Strategy Group, Inc. All Rights Reserved.