White Paper

Elastic Cloud Gateways: The Evolution of Secure Cloud Access

Securing Enterprise Perimeters through a Cloud-native, Data-centric Approach

By Doug Cahill, ESG Senior Analyst; John Grady, ESG Analyst

September 2019

This ESG White Paper was commissioned by Netskope and is distributed under license from ESG.

Contents

Executive Summary

Enterprise security groups today face a daunting task. While their core responsibility of protecting corporate data and resources remains unchanged, they are asked to do so while enabling line-of-business teams and individual employees to drive growth through innovation and transformation via the cloud. Security teams today must secure an exponentially increasing number of perimeters across their network by accounting for managed and unmanaged cloud applications, protecting data that is moving off-premises and accessed by partners and other third parties at an accelerated rate, and controlling user access that increasingly comes from outside of the main campus across a multitude of devices.

These challenges are not new, but the approach to securing this modern environment has been slow to progress. In fact, the most common method has been to secure these new perimeters through the legacy perimeter. However, this approach is costly and lacks the necessary visibility to maintain a strong security posture. Layering on additional point tools to address specific parts of the overall problem introduces inconsistency and can reduce overall security efficacy.

Ultimately, IT organizations require a new architecture to secure the multiple perimeters enterprises are charged to protect. Elastic cloud gateways (ECGs) represent a network security architecture for the cloud era. ECGs are built on a globally distributed, cloud-delivered and cloud-native, microservices-based architecture that arbitrates access and inspects content across the entirety of an organization's cloud and web ecosystem.

Ultimately, IT organizations require a new architecture to secure the multiple perimeters enterprises are charged to protect. Elastic cloud gateways (ECGs) represent a network security architecture for the cloud era.

The Multiple Perimeters of the Modern Enterprise

The continuing explosion of cloud usage and increased knowledge worker mobility born out of digital transformation is forcing enterprises to rethink their approach to access and security. The modern enterprise is application- and data-centric, with the underlying infrastructure becoming somewhat of an afterthought. As applications, data, and users have sprawled beyond the confines of the perimeter, maintaining both a high quality of service and a consistently strong security posture has become increasingly difficult. Clearly, the corporate perimeter is no longer a singularly defined location. Instead, enterprises must account for multiple edges encompassing cloud, data, and human perimeters.

The Cloud Perimeter

The adoption of cloud has continued to increase steadily, with nearly every organization having shifted at least some part of their business off-premises. In fact, an increasing number of companies now follow a "cloud-first" policy where new applications are deployed using public cloud services *unless* a compelling case is made to maintain them on-premises. ESG research indicates that the use of a cloud-first policy grew from 29% of organizations to 39% between 2018 and 2019.

Of the 58% of organizations currently utilizing IaaS platforms, just over half use three or more cloud service providers.

Introducing more complexity to this cloud perimeter is the fact that organizations are increasingly likely to utilize multiple cloud platforms. According to ESG research, 67% of organizations report at least 20% of their applications are SaaS delivered (see Figure 1). Additionally, of the 58% of organizations currently utilizing IaaS platforms, just over half use three or more infrastructure cloud service providers.[1] These percentages may even be conservative when considering the impact of shadow IT and the long tail of unmanaged SaaS applications. In an enterprise

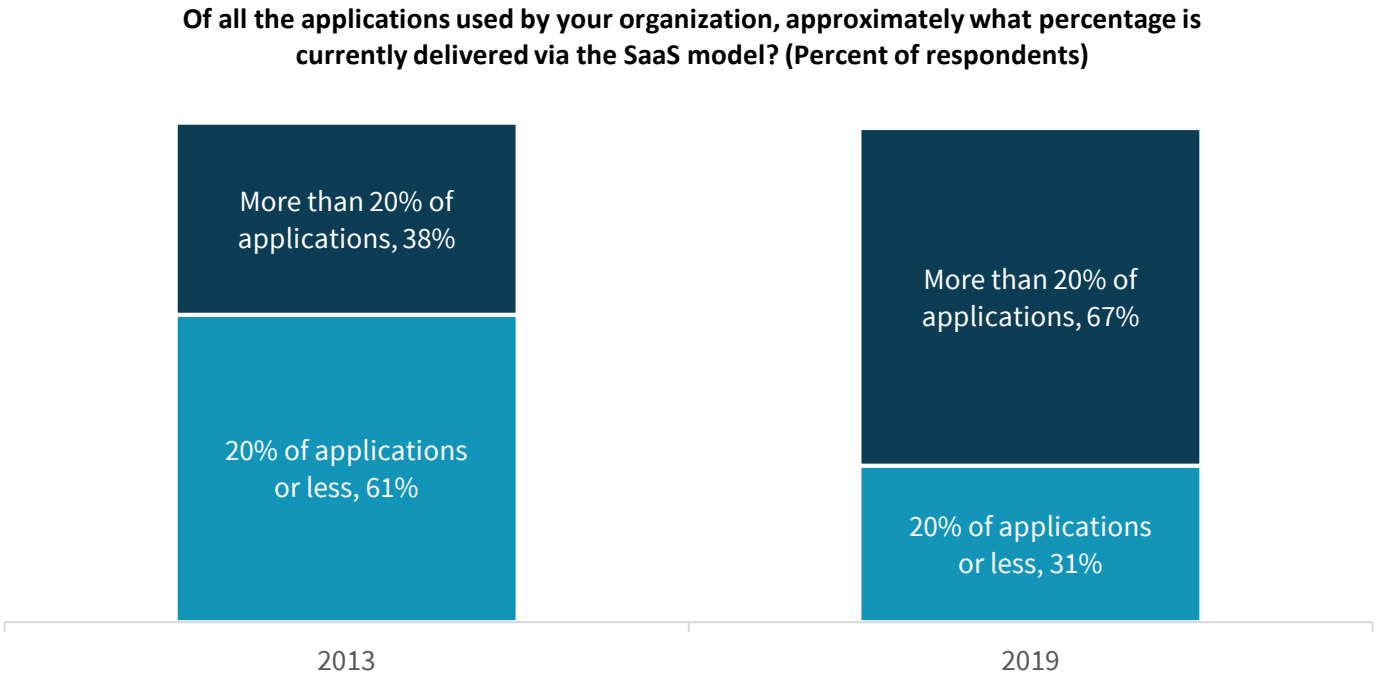
[1] Source: ESG Master Survey Results, *2019 Technology Spending Intentions Survey*, March 2019.

with a mature approach to leveraging cloud technologies, it would not be uncommon to find hundreds or even over a thousand cloud services in use across the spectrum of both corporate-managed and unmanaged applications. For example:

- O365 and Salesforce as corporate-managed email and CRM SaaS applications.
- AWS and Azure as corporate-managed IaaS platforms.
- Developers and lines of business led use of Github, Jira, Jenkins, and many others.
- Individual use of Gmail, Evernote, Dropbox, and similar applications.

It becomes incredibly difficult if not impossible for security teams to maintain consistent controls and policy across this type of environment using existing security tools.

Figure 1. The Breadth of SaaS Usage Continues to Increase



Source: Enterprise Strategy Group

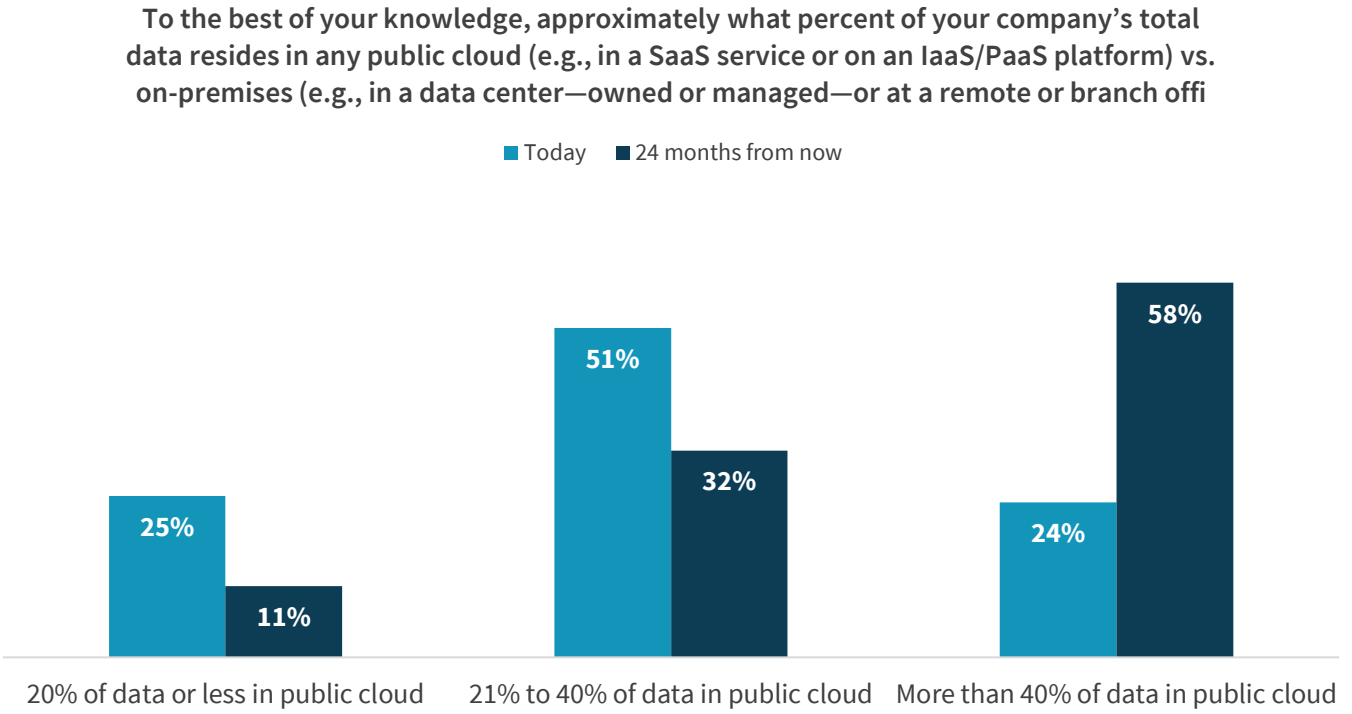
The Data Perimeter

More corporate data is now cloud-resident, including sensitive data being distributed across an enterprise cloud environment. ESG research shows that today, 24% of organizations say at least 40% of their organization's data is in the public cloud. In two years, 58% expect at least 40% of their data to be in the public cloud (see Figure 2).[2] With what is left of the perimeter becoming more amorphous and flexible, data must become the protection point, meaning that security controls need to be data-centric.

With what is left of the perimeter becoming more amorphous and flexible, data must become the protection point.

[2] Source: ESG Master Survey Results, *Trends in Cloud Data Security*, January 2019.

Figure 2. Data Continues to Move to the Cloud



Source: Enterprise Strategy Group

This fact has played a large role in the policy creation moving beyond the security organization as business objectives are increasingly weighed by the data center, networking, compliance, application, and line-of-business leaders in developing security policy. As the group of security stakeholders expands to directly include non-security personnel, there must be a common language to ensure the organizational alignment. The only way this can occur is if data is the central tenet of the discussion, and a core focus of the overall security strategy.

The Human Perimeter

In addition to the adoption of cloud and the flow of data beyond the campus network, mobility continues to challenge the traditional network architecture. Historically through the use of VPN clients and MPLS or other dedicated broadband technologies, all corporate traffic was hair-pinned back through the campus network, allowing security policies to be centrally enforced. This made sense when mobile workers were few and enterprise resources were centralized behind a defined network perimeter.

The distributed nature of the modern enterprise makes this legacy approach unfeasible. Knowledge workers travel and work outside of the office on a more frequent basis. At the same time, remote and branch office locations are accessing the public internet for corporate applications as much if not more than the enterprise data center. Further, an expanded ecosystem of partners, suppliers, and contractors has access to cloud-resident data, shifting the perimeter even farther from campus edge. ESG has found that 67% of organizations have some combination of business partners, supply chain partners, customers, suppliers, or resellers with access to their cloud-resident data.[3]

[3] ibid.

The Challenges of Securing the New Perimeters via the Old Perimeter

Unfortunately, these changes to the nature of the corporate perimeter have occurred over a span of years and the adoption curve of technology does not typically lend itself to wholesale replacement of legacy solutions. Rather, new products are slowly layered into the existing architecture, and IT and security teams do their best to make all the pieces work together. However, many organizations are well beyond the trial stage and are utilizing the cloud for business-critical applications and processes. Practitioners clearly recognize the need for cloud security solutions and expect to prioritize investment in this area with 36% of organizations pointing to cloud security as an area where they plan to make significant investments, the highest percentage of any cybersecurity segment.[4]

> Security practitioners are limited to the solutions that are currently available and in many cases are forced to utilize add-on investments to legacy cybersecurity solutions.

However, security professionals are limited to the solutions that are currently available and in many cases are forced to utilize add-on investments to legacy cybersecurity solutions despite a fundamental shift in the broader architecture. An enterprise may utilize VPN solutions to backhaul traffic through the on-premises security stack for scanning. Alternatively, they may employ some level of virtual or cloud-based firewall and secure web gateway solution to inspect traffic directly routed to the cloud. From a data protection perspective, expanding the enterprise DLP solution into the cloud may provide some additional protections. However, while these approaches provide some level of security, they create additional challenges relative to performance, consistency, visibility, and economics.

The Backhauling Performance Penalty

Cost and performance impacts are associated with using a legacy security approach to control access to cloud resources. This is especially the case with a hub and spoke model in which all network traffic from branch offices and remote workers is backhauled to the main campus, typically via VPN connections. This approach may seem to at least help organizations maintain a high level of visibility and control over employee cloud usage.

> Unfortunately, when user experience suffers, employees will find a workaround, typically at the expense of security.

However, in practice this is rarely the case. The circuitous routing of traffic to the campus when it is ultimately destined for the public cloud can negatively impact performance. Unfortunately, when user experience suffers, employees will find a workaround, typically at the expense of security. Additionally, as more corporate traffic is destined for the public cloud and users increasingly access corporate resources from off-network mobile devices, it is not cost-effective to maintain the access backbone to support this model. Taking a direct-to-internet approach makes more sense in this environment, but requires integrated tools to maintain a strong security posture, and cloud-delivered secure web gateway capabilities to provide security controls closer to the user.

Inconsistent Policies and Misaligned Economics

Whether utilizing a hub and spoke approach or implementing a mix of virtual and cloud-based perimeter defenses as a first step to enabling a direct-to-internet model, static security tools have trouble keeping pace with the dynamic nature of the cloud and introduce management inefficiencies and inconsistent policies. Businesses want to enable user- and line-of-business-led applications to drive growth and promote innovation. However, security teams typically operate under a siloed approach with multiple security tools and disparate management consoles, and ultimately suffer point tool fatigue.

[4] Source: ESG Master Survey Results, *2019 Technology Spending Intentions Survey*, March 2019.

In fact, 43% of organizations say that maintaining security consistency across on-premises and public cloud environments is a top security challenge.[5]

To enable growth and innovation via the cloud while also mitigating risk, the security architecture must shift from siloed to unified to integrate controls for the cloud, data, and human perimeters as well as centralize management for consistent policy. Further, security consumption should be more closely married to cloud consumption to better align the economics. This means not only moving from a CapEx to an OpEx approach but also shifting to a consumption-based model that allows organizations to have the correct level of performance and protection as they need it, without over-provisioning.

To enable growth and innovation via the cloud while also mitigating risk, the security architecture must shift from siloed to unified to integrate controls for the cloud, data, and human perimeters as well as centralize management for consistent policy.

Incomplete Visibility

Traditional network perimeter tools (e.g., secure web gateways) were not designed to granularly inspect and control cloud traffic. While many solutions are application-aware to an extent, their main focus is stopping threats and coarsely blocking inappropriate or clearly malicious web traffic. With so much enterprise traffic now comprised of SaaS applications, a deeper understanding of those resources is required in order to be "risk-aware." For example, organizations need to distinguish between the enterprise-managed version of Dropbox and an unmanaged personal instance in order to correctly enforce policy. As cloud providers expand their ecosystems to include thousands of plug-in applications (e.g., Salesforce AppExchange), the ability to differentiate between the sub-applications and enforce policy at that level becomes foundational. Because SaaS traffic is so heavily comprised of API calls, JSON language and other non-HTTP communications, the SWG and other traditional tools are not able to decode the sessions and thus have limited visibility.

Further, marrying content inspection capabilities to this visibility is the only way to craft holistic data-centric policies that account for the risk profile of the application in question. Without these integrations, security teams face an uphill battle to gain visibility and control over the entirety of their organization's network traffic, which can lead to gaps in coverage.

Securing Today's Perimeters with Elastic Cloud Gateways

The tools for controlling and securing web access have evolved as usage has changed. Initially, URL filtering and bandwidth control represented the core functionality to block certain classes of website and maintain quality of service for critical corporate resources. Over time, threat prevention capabilities were added to address a more advanced and dynamic threat landscape. More recently, this functionality shifted to the cloud in an attempt to support the remote office and direct-to-internet use cases.

However, this incremental evolution does not holistically address the fundamental shift to cloud, as delivering security in the cloud is not the same as delivering security for the cloud. A new approach focusing on data, applications, and performance is required. This approach must evolve beyond simply securing web and internet access to protecting data everywhere it goes, whether it is created and stored in the cloud, or transmitted to unmanaged cloud applications and personal devices. It also requires a deep understanding of the thousands of cloud applications that enterprises use to facilitate the implementation of granular, risk-based controls based on user, action, and context to safely enable cloud usage. Lastly, this new approach must scale via a globally distributed platform to deliver distributed enforcement of

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

security controls regardless of the location of users, applications, or data and allow even the largest enterprises to forgo the traditional trade-off between security and performance.

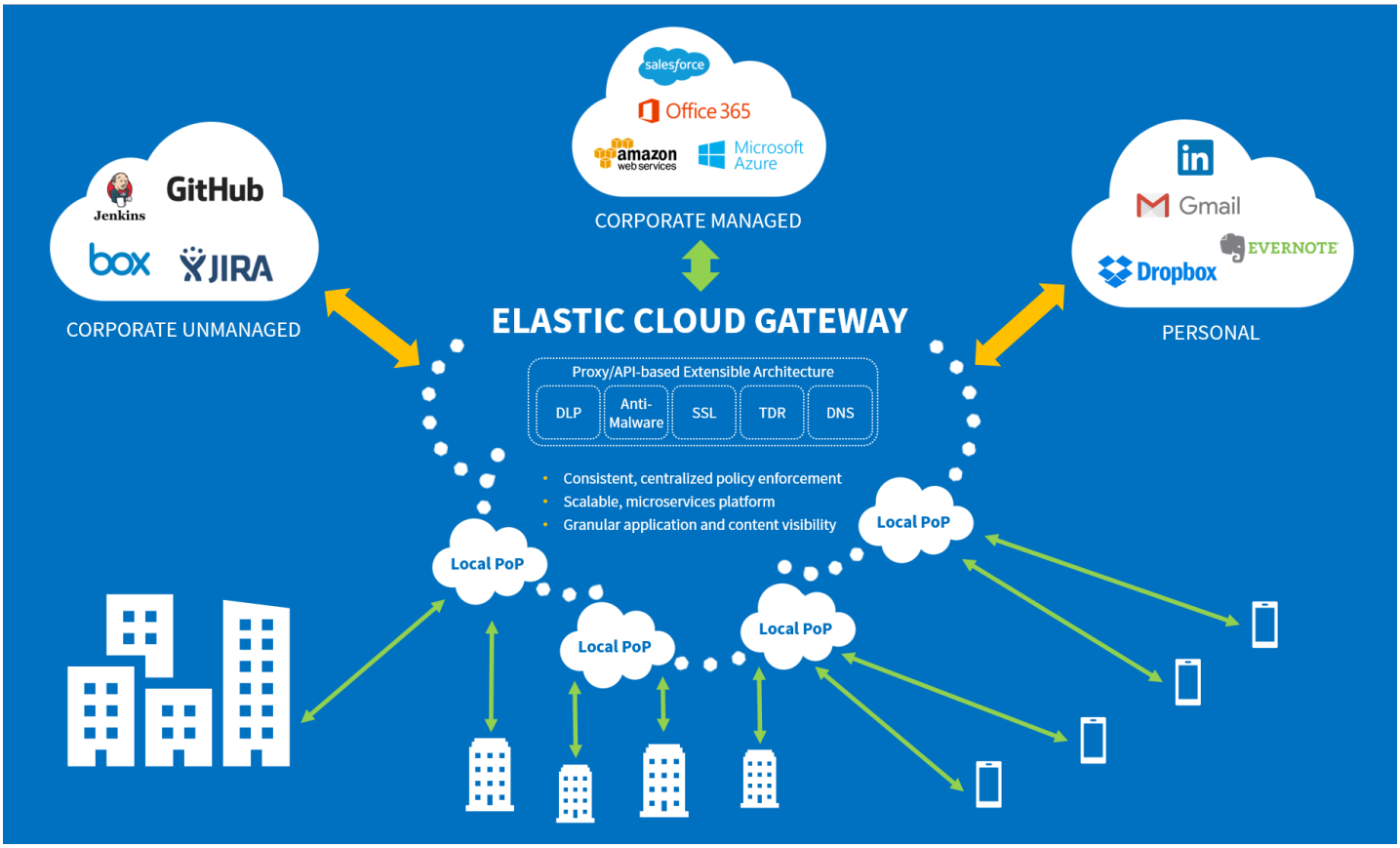
> To solve for these issues, elastic cloud gateways represent a network security architecture for the cloud era.

To solve for these issues, elastic cloud gateways (ECGs) represent a network security architecture for the cloud era. ECGs are multi-channel, multi-mode, cloud-delivered security gateways built on a globally distributed, cloud-native microservices platform. These solutions automatically scale to provide end-user access and threat prevention to a range of cloud services, with tightly integrated data loss prevention (DLP) capabilities. The centralized control plane and scalable data plane of ECGs arbitrate access and inspect content across the entirety of an organization's cloud ecosystem.

Convergence via Multi-channel Functionality

At its core, the ECG architecture integrates secure web gateway (SWG), cloud access security broker (CASB), DLP, and access control functionality (see Figure 3). This multi-channel capability enables ECGs to secure all web and cloud application usage for complete visibility across the spectrum of internet traffic. A recent Netskope study revealed that while 85% of enterprise web traffic goes to cloud services, 15% remains traditional web browsing.[6] The integration of multiple technologies and functions serves to simplify management, drive consistent policy, and improve efficacy.

Figure 3. Elastic Cloud Gateway Architecture



Source: Enterprise Strategy Group

[6] Source: *Netskope Cloud Report*, August 2019.

Further, with the ECG representing a significant control point on the network and including SWG functionality, it becomes a logical location for integrated threat prevention capabilities. In addition to targeting enterprise resources in the cloud, threat actors now commonly leverage cloud resources as part of their attack infrastructure. Attackers may house command and control servers on, or exfiltrate data to, legitimate cloud infrastructure platforms. Alternatively, modern phishing campaigns often utilize links to well-known cloud applications which in actuality host malicious payloads, in order to confuse users. In one recent example, attackers spoofed an email from the CEO of an energy company using a rogue account, which shared a malicious Google Doc with employees. They were prompted to enter their credentials, which were then forwarded to the attackers. Traditional defenses are often circumvented by these types of attacks because they cannot integrate a granular understanding of the applications in use across the enterprise, including all users and the related context and risk, with strong threat detection capabilities.

Scalable Cloud-native Architecture

The fact that elastic cloud gateways are cloud-native directly addresses many of the drawbacks associated with the legacy approaches previously described. A microservices-based architecture allows for elasticity in which the ECG infrastructure automatically scales up or down based on usage demand. This model serves two purposes:

The fact that elastic cloud gateways are cloud-native directly addresses many of the drawbacks associated with legacy approaches.

- It enables deep content inspection for DLP, threat detection, and prevention capabilities and even SSL decryption/re-encryption at line-speed.
- It directly aligns the purchase of security controls to cloud usage by employing a consumption-based subscription model.

Consumption-based subscriptions have been in place from a workload protection perspective for some time but have yet to be implemented on the access side. Whether based on active users, traffic levels, or number of cloud platforms accessed, some consumption metric is needed.

In addition to services scaling, ECGs rely on a globally distributed platform with widespread points of presence to deliver consistent performance for users, regardless of location. Without locally accessible POPs, the architecture essentially reverts to a hub and spoke approach, only in the cloud. Further, this globally distributed approach addresses data residency and compliance concerns across disparate geographies.

Multi-mode Implementation

The multi-mode facet of elastic cloud gateways is based on the architecture of cloud access security brokers. As such, ECGs can be deployed out of band by leveraging APIs for managed cloud application inspection. This method supports ease of use and introspective analysis to apply policy to data that has already been sent to a cloud application. ECGs can also be deployed inline as a forward or reverse proxy for inspection of unmanaged applications and web traffic with better threat protection and user experience. The fact that ECGs are multi-mode and can leverage the native APIs of cloud applications is one of the attributes that fundamentally distinguishes ECGs from secure web gateways.

Operational, Efficacy, and Economic Benefits

The essential value proposition of elastic cloud gateways is that they converge multiple point tools to drive consistent policy, create operational efficiencies, and reduce the attack surface. Chasing bad behavior from a security practitioner perspective is a Sisyphean task. ECGs shift the security model from siloed to unified, which improves consistency and

ultimately enables a more positive security model. The centralized management improves efficacy by closing holes across disparate product sets and helps address the acute security skills shortage many organizations deal with daily.

Extensible, API-driven Open Architecture

Elastic cloud gateways are based on an extensible framework, which allows for additional functionality to be incorporated over time. The open nature of the architecture supports third-party integrations via APIs. Examples of extended ECG functionality include:

- Software-defined perimeter (SDP) to protect applications and control access by securely brokering only the right level of privilege to the right individuals, regardless of location.
- DNS protection and additional threat prevention capabilities to detect and block malicious traffic.
- Network security functionality to provide unified visibility and control over enterprise traffic across multiple protocols.

Netskope's Security Cloud Delivers Elastic Cloud Gateway Capabilities

Netskope's cloud-native, multi-channel, and multi-mode architecture, globally distributed network, and deep data inspection capabilities deliver elastic cloud gateway functionality and provide network security for the cloud era. With CASB inline and API-mode roots dating back to 2013, Netskope's platform is built to provide organizations deeper visibility and control across their cloud infrastructure.

Multi-channel Coverage across Web Properties and Cloud Applications

Netskope was one of the pioneers in the CASB market. Its solution governs usage based on identity, micro-application, data, and activity while enforcing risk-based and activity-based fine-grained policy control. It focuses on data protection by securing data at rest across corporate managed cloud applications and data in flight across both corporate managed and unmanaged cloud applications. Additionally, anti-malware, threat intelligence, and anomaly detection applied to either encrypted or unencrypted traffic provide threat prevention capabilities.

More recently, the addition of secure web gateway functionality enables Netskope to present customers with a more unified approach to security by enabling a shift to a secure direct-to-internet access model for remote users and branch offices. This approach offers multi-layered threat prevention including advanced scanning and sandboxing as well as TLS decryption to eliminate blind spots. Further, the acquisition and subsequent integration of Sift into the Security Cloud has expanded Netskope's IaaS capabilities to include deeper data protection and threat detection functionality.

A Content-aware, Multi-mode Implementation

Netskope's Security Cloud is based on a cloud-native, microservices architecture. Its solution supports multi-mode implementation for real-time and near-real-time inspection. Proxy, API, and agent-based deployments allow organizations to tailor the deployment to their specific use case: discovery of unsanctioned applications, governance, data security, or threat protection.

Netskope's rich DLP policy engine leverages the multi-mode implementation to control data in flight to and at rest in all cloud services. The engine leverages metadata extraction, fingerprinting, exact match, proximity analysis, and other techniques in addition to supporting broad file type and data identification. Scalability of this content inspection is enabled by the cloud-native platform. According to Netskope, more than 36,000 applications have been scored against Netskope's Cloud Confidence Index (CCI), enabling deep application visibility and granular policy controls to be enforced. This includes

the ability to differentiate between corporate and personal versions of Dropbox, separate instances of Marketo, and various Salesforce plug-ins, among other examples.

Edge-based Deployment for Local Access

Netskope's NewEdge platform is expected to include more than 50 POPs by the end of 2019, providing local access to globally distributed users. Its cloud-native architecture and NewEdge backbone enables the feature set to scale as customers require. It also allows Netskope to perform compute-intensive functions like TLS decryption, data loss prevention, content inspection, and malware prevention inline at speed while maintaining user experience regardless of location.

The Bigger Truth

Enterprise security groups continue to suffer from an acute skills shortage, with 53% of organizations reporting it as a problem.[7] At the same time, they are asked to enable business innovation and productivity by supporting cloud services in a secure way. Yet, while there has been a fundamental rearchitecting of the compute paradigm and the underlying infrastructure, security controls have advanced more incrementally.

Deeper integrations across the various point tools in use today and a cloud-delivered, microservices-based approach would be a welcome development for security practitioners. It would enable organizations to significantly mitigate their business risk while fully embracing digital transformation. For security teams, reducing policy inconsistencies, streamlining management, improving performance, and increasing efficacy would go a long way to offset the shortage of cybersecurity skills.

Elastic cloud gateways represent the next stage in what has been a slow and incremental evolution of the network security stack. As web (and more recently cloud) usage has changed, the level of visibility and control required to ensure secure access has become more granular. That granularity coupled with the increasingly advanced attack surface and explosion of corporate data going to and from the cloud urgently requires a scalable cloud-native approach to network security.

[7] Source: ESG Master Survey Results, *2019 Technology Spending Intentions Survey*, March 2019.

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

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188