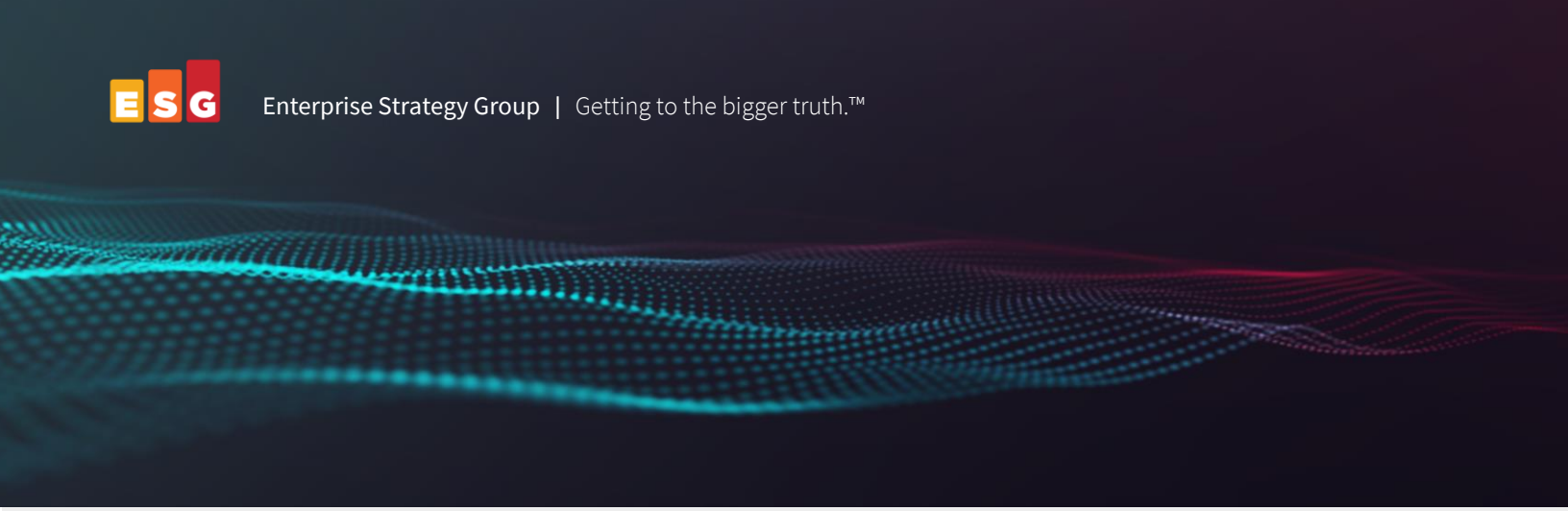


ESG WHITE PAPER

The Evolution of Cloud Access Security Brokers

Comprehensive, Integrated, Accurate Protection with Palo Alto Networks Next-Generation CASB

By John Grady, ESG Senior Analyst

November 2021

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

Contents

Executive Summary

In the years since the cloud access security broker (CASB) was first introduced, enterprise SaaS usage has risen dramatically. Most organizations now rely on the cloud for core business applications housing sensitive corporate data. This usage, coupled with the massive scale of smaller, potentially unsanctioned cloud applications, has made the CASB a critical component of enterprise security strategies.

With users more distributed than ever, cloud-based collaboration tools such as Slack, Zoom, Jira, and Confluence have also risen in prominence. Yet the decoupled, layered-on nature with which most organizations approached CASB initially now creates more problems than it solves. CASBs can provide broad functionality but require different deployment models to address different use cases. Organizations need to have visibility into all application usage, as well as inline threat prevention, access control, data security, and policy enforcement across all users, regardless of device or location.

The complexity of accomplishing this via additional agents, log collectors, and traffic redirection has reached a tipping point. As part of the evolution towards secure access service edge (SASE), security teams must begin considering how CASBs can better integrate with other network security control points to streamline deployment, provide more consistent management, and improve security effectiveness.

Security teams must begin considering how CASBs can better integrate with other network security control points to streamline deployment, provide more consistent management, and improve security effectiveness.

Palo Alto Networks' Next-Generation CASB represents an updated approach to cloud access security brokers, designed to align with these changing enterprise needs. Through integrations with Palo Alto's cloud, software, and appliance-based next-generation firewalls and its cloud-delivered enterprise DLP, Next-Generation CASB provides a simpler and more cost-effective approach to CASB, while maintaining the broad application visibility and accurate threat and content inspection organizations require to secure the usage of cloud applications.

The Role of SaaS Security in the Modern Enterprise

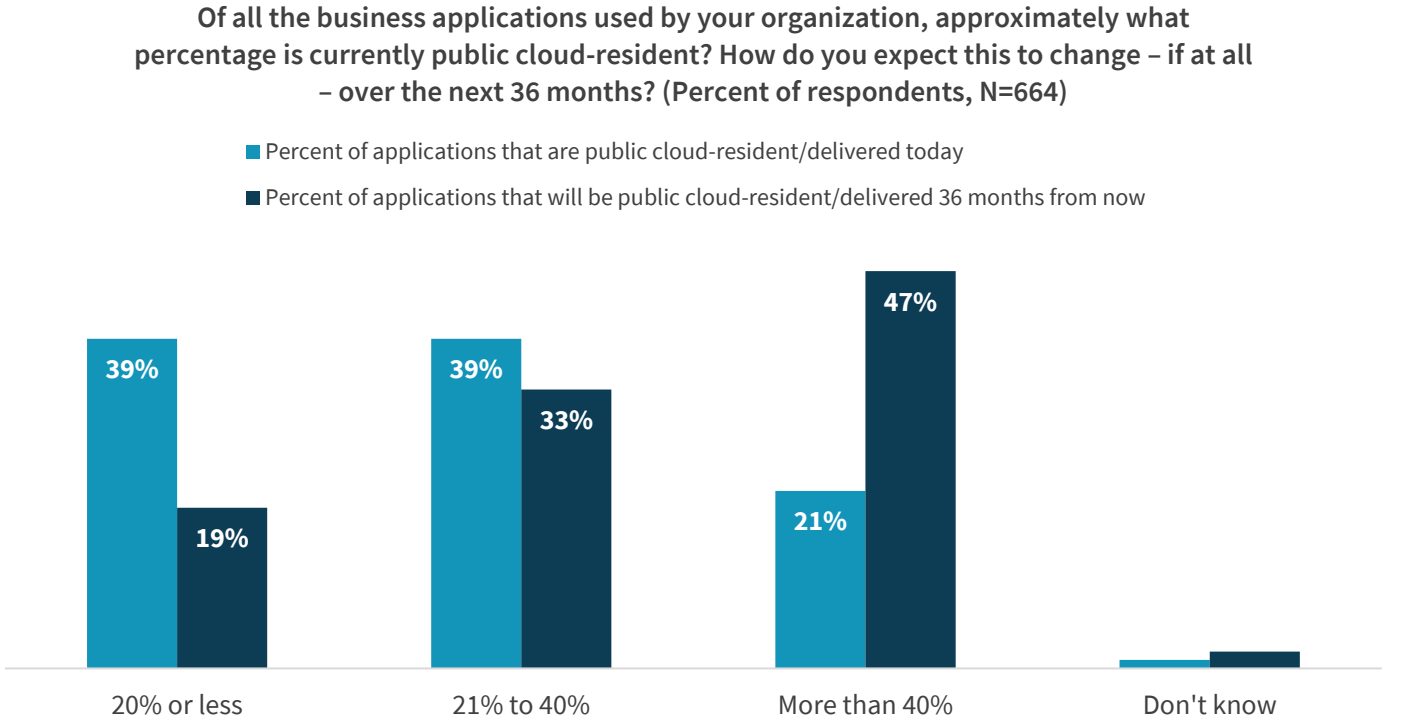
Cloud adoption has become nearly ubiquitous, with ESG research finding that 94% of organizations use public cloud services of some sort.[1] However, more important than adoption is the increase in the consumption of public cloud applications by these organizations.

Most enterprises are well beyond taking a limited approach by shifting a less-sensitive application or two to the cloud, and rather are using the public cloud for numerous, mission-critical applications.

Most enterprises are well beyond taking a limited approach by shifting a less-sensitive application or two to the cloud, and rather are using the public cloud for numerous, mission-critical applications. This trend is only expected to increase over the next three years, with 47% of organizations expecting more than 40% of their business applications to be public cloud-resident by that time (see Figure 1).[2]

[1] Source: ESG Research Report, *2021 Technology Spending Intentions Survey*, January 2021.
[2] Ibid.

Figure 1. Percentage of Public Cloud Applications, Today versus 36 Months from Now



Source: Enterprise Strategy Group

Core Capabilities of CASB

The need for visibility and control over applications has been apparent for over a decade and has led to the advent of the next-generation firewall (NGFW). While industry-standard now, the shift from predicating policies on port, protocol, and IP address to specific applications and users represented a transformative change at the time and provided network security teams better visibility into the composition of network traffic. Over the years, the number and types of enterprise SaaS applications have grown from just a handful, such as email and CRM, to a diverse universe supporting marketing, human resources, finance, IT, and nearly every other aspect of the business. Further, the use of cloud-based collaboration tools such as Slack, Zoom, Teams, Jira, and Confluence has exploded, as remote work has become commonplace. In many cases, both internal and external entities using either managed or unmanaged devices may be accessing these applications or sharing data through them.

Yet the increase in the number of sanctioned corporate SaaS applications is only one part of a broader story. The self-service nature of the public cloud continues to empower employees to use numerous unsanctioned applications outside the purview of the IT department. As a result, ensuring consistent data security and compliance with mandates such as the Payment Card Industry Data Security Standard (PCI), the Health Insurance Portability and Accountability Act (HIPAA), and the General Data Protection Regulation (GDPR) has become increasing complex.

Cloud access security brokers (CASB) have been on the market for nearly ten years, specifically to protect and govern the usage of SaaS applications and address many of these issues. With the consumption of cloud applications continuing to increase, their criticality has only been heightened. These tools typically provide functionality to address four major use cases:

- Visibility. CASBs must identify and inventory all the applications enterprise users access, whether sanctioned by the IT department or not, and assess the level of risk these resources pose to the organization to help inform policy

decisions. ESG research has found that 32% of organizations cite the increasing use of cloud applications as a leading driver of cybersecurity complexity.[3]

- Threat Protection. CASBs should protect users and corporate data from malicious activity, especially when using unsanctioned applications, and ensure that threats do not compromise sanctioned application environments. Nearly half of ESG research respondents (45%) cite the increasing threat landscape as one of the biggest drivers of network security complexity.[4]

- Data Security. CASBs need to identify the types of data flowing to and residing in SaaS applications and apply corporate policies to ensure sensitive data is properly protected. Yet ESG research has found that 26% of organizations indicate that the need to incorporate data-centric policies and security controls has made network security management and operations more difficult.[5] This is primarily due to the siloed nature of the different tools used for data security across the environment.

- Compliance. CASBs help organizations map their assets in the cloud back to the regulator mandates to which they are subject. This is important, as 18% of ESG research respondents say difficulty in remaining compliant efficiently has made cybersecurity more difficult.[6]

A Layered Approach to CASB Has Increased Complexity

Like most emerging technologies, CASB has been layered into existing environments. While this has improved visibility and application control, the fact that it is architected and managed independently from other security tools has a downstream effect on the security analysts and practitioners who must synchronize their risks, policies, and goals across a separate layer of the stack.

The fact that CASB is architected and managed independently from other security tools has a downstream effect on the security analysts and practitioners who must synchronize their risks, policies, and goals across a separate layer of the stack.

Further, depending on the use case in question, CASBs must be deployed differently in the environment. For inline control and visibility, a reverse or forward proxy deployment is required. However, there are limitations to each option. Because they are deployed in front of known applications, reverse proxies lack visibility into unsanctioned applications. While forward proxies provide visibility into many applications whether sanctioned or not, this model requires traffic to be routed from users through the CASB before reaching the application. Proxy auto-configuration (PAC) files or agents on the endpoint can redirect application traffic to the CASB, but these options are only available if the device is managed. Proxy chaining services together or redirecting DNS requests to cloud services through the CASB are also options but require more extensive network routing changes. An additional issue with the proxy model is that visibility is limited to web-based protocols. Applications such as BitTorrent, Tor, FTP, Private VPN, and others can bypass the proxy and can be used by attackers to exfiltrate data.

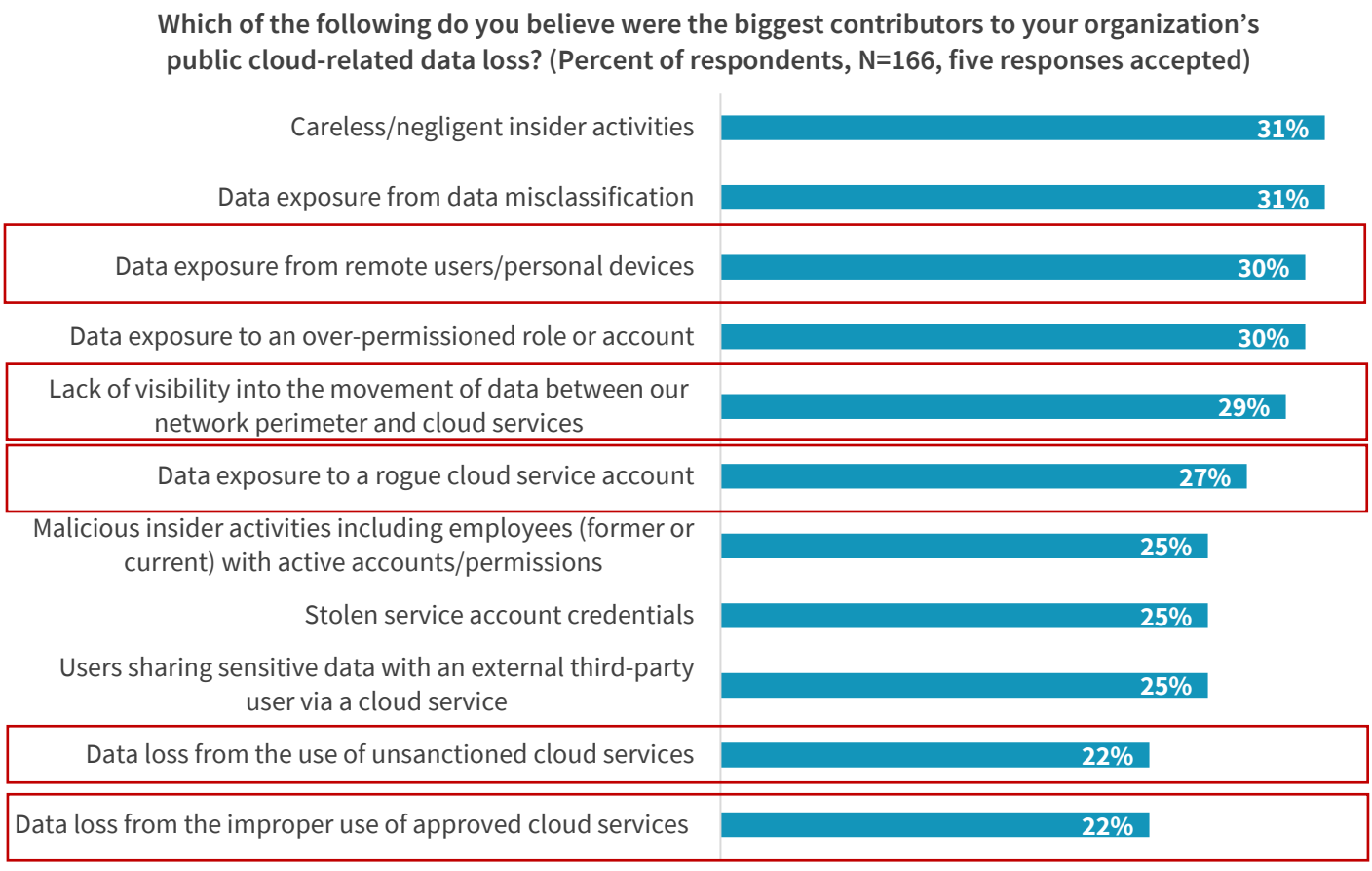
Alternatively, for sanctioned enterprise applications, CASBs can also sit out-of-band and use log collection and API integrations. API integrations allow granular control over application features and enforce data security policy within the application itself, but only for sanctioned applications. Conversely, while log collection from firewalls and secure web

[3] Source: ESG Master Survey Results, *The State of Zero Trust Security Strategies*, May 2020.
[4] Source: ESG Master Survey Results, *Network Security Trends*, March 2020.
[5] Source: ESG Master Survey Results, *Transitioning Network Security Controls to the Cloud*, July 2020.
[6] Source: ESG Master Survey Results, *The State of Zero Trust Security Strategies*, May 2020.

gateways (SWG) provides visibility into application traffic, real-time threat prevention and policy enforcement is not possible in this model. Over the years, some CASBs have adopted a multi-mode approach to address all use cases and support deployment flexibility for customers. However, the complexity of mapping these deployment modes to use cases and management policies across inline and out-of-band modes can become burdensome.

An additional element of confusion has arisen from the overlap of CASB and data security. Encryption and tokenization-focused use cases have become less common over time as native application data protection has improved. At the same time, as more and more enterprise data has become cloud-resident, CASBs have increasingly been positioned as DLP tools. While they certainly are a component of DLP, a significant percentage of enterprise data remains on-premises and flows through user devices. This is borne out when one considers the broad causes of enterprise data loss (see Figure 2).[7] This means that a DLP approach too heavily weighted toward any one control point can lead to reduced effectiveness. Trying to create consistent policies across the different tools that deliver their own data loss prevention across cloud applications, the network, and endpoints is inefficient and can be prone to human error.

Figure 2. Top 11 Causes of Public Cloud Data Loss



Source: Enterprise Strategy Group

[7] ESG Master Survey Results, *Trends in IAM: Cloud-driven Identities*, December 2020.

Top Requirements for a Modern CASB

To address the ever-growing and clearly business-critical nature of SaaS usage, while at the same time reducing complexity, a simplified, integrated approach to CASB is preferred. Specifically, three core requirements are needed:

- Deep visibility, intelligence, and security across the thousands of available cloud services and collaboration tools.
- End-to-end DLP coverage to ensure consistent security across the cloud, network, and endpoints.
- Tight integrations with other network security tools to position CASB as the security anchor point for the transition to (SASE).

Visibility

The initial use case for CASB was visibility into unsanctioned applications. Yet while this has become more difficult as the number of available applications has exponentially risen over the years, it has become more important for exactly the same reason. CASBs must be able to accurately recognize and inventory applications in real time as they become available—something traditional CASBs have struggled to keep pace with. Most importantly, providing a detailed risk assessment for these applications helps administrators make informed decisions with regard to employee access. The scale of today's SaaS usage requires a degree of automation to this discovery and assessment to keep up with the constant rate of change. Yet at the same time, some level of customization is necessary for more or less risk-tolerant organizations to manage employee access according to their preferences.

In addition to inventorying and assigning risk to SaaS applications accessed by employees, modern CASBs must provide strong threat prevention. As the scale of web usage has tipped from traditional websites to SaaS applications, attackers have adjusted their tactics accordingly and can leverage cloud-based resources to serve malware in an attempt to compromise corporate assets. As a result, CASBs must offer the same level of protection users have traditionally benefited from through secure web gateways, next-generation firewalls, and other threat prevention tools.

End-to-end Data Loss Prevention

There is a pressing need for more consistent visibility into and control over corporate data across the entire environment. ESG research has found that 70% of respondents agreed that their organization's implementation of a single set of data loss prevention policies spanning on-premises and cloud-resident data was in need of improvement.[8] With more data now cloud-resident, DLP should be cloud-first but not cloud-only.

A central aspect of moving from a siloed to a unified DLP approach is the ability to federate policies across enforcement points, with CASB as the central piece of a large solution set.

This requires strong cloud enforcement capabilities and centralized policy management through the cloud but with distributed control points. Consistency means mapping roles to data classes to ensure that users with certain roles have the same level of access and usage policies by classes of data, irrespective of location. Further, policy enforcement must be distributed at the control points for data in motion and at rest, which requires enforcement in the cloud, at egress points, and at the edge. As many organizations have shifted from email to collaboration tools, it has become critical that CASBs not only provide visibility into these tools, but also the different avenues of sharing information through them. This means that in addition to scanning files, DLP engines should understand when sensitive data is shared via screenshot, plain text,

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

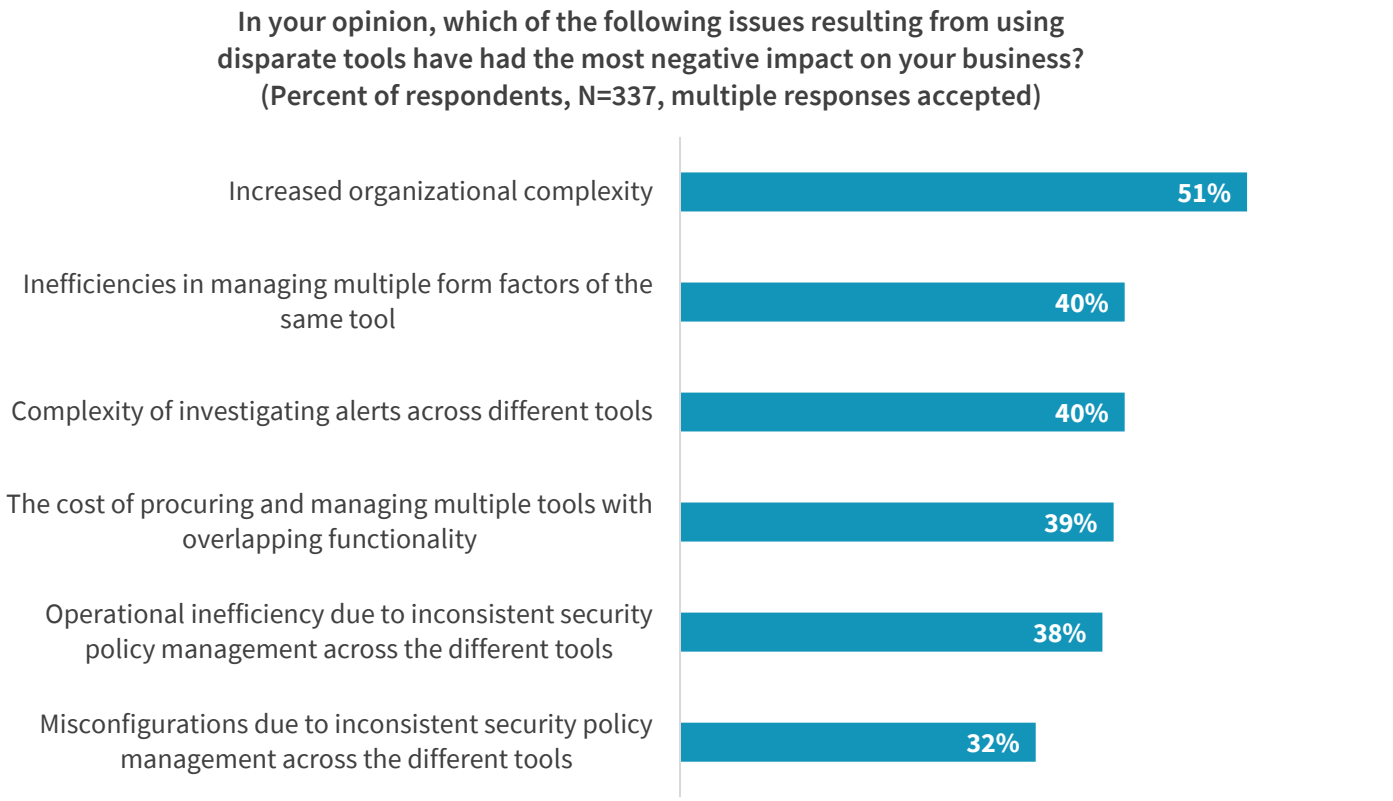
or across multiple posts. As a result, a central aspect of moving from a siloed to a unified DLP approach is the ability to federate policies across enforcement points, with CASB as the central piece of a large solution set.

CASB as an Anchor Point of SASE

The trend of consolidation has become a focus across much of the cybersecurity landscape. While defense-in-depth has been the preferred approach for many years, the pendulum is swinging toward integrated platforms to address the difficulties caused by having to manage a variety of disparate point tools. Siloed tools can result in a number of negative issues (see Figure 3).[9] These can best be summarized as:

- Operational inefficiencies. The manual mapping of policies across multiple tools, many of which can have overlapping functionality, is not only inefficient but prone to error. Similarly, the coordination required by different teams (i.e., network security, data security, cloud security) is made more complex by the use of many disparate tools.
- Increased costs. Both direct and indirect costs are typically higher when organizations use siloed tools. Rather than spreading solution costs across many different vendors, a converged approach can lead to a more strategic and cost-effective relationship with fewer vendors. Additionally, security teams can focus their training and certifications on a more targeted set of solutions.
- Weakened security. Ultimately, visibility and threat protection can be inconsistent across siloed tools, leading to investigation complexity when issues do arise.

Figure 3. Issues Arising from Using Many Disparate Tools



Source: Enterprise Strategy Group

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

By merging CASB back into the broader, foundational security architecture, management and policies can become integrated with other network security controls, relieving security analysts and practitioners of the burden of managing a layered CASB.

While SASE includes a variety of capabilities from SD-WAN to zero trust network access (ZTNA) to remote browser isolation, the convergence of CASB with traditional perimeter tools such as secure web gateway and next-generation firewall is often a first step on the longer path toward a full SASE architecture. In fact, 75% of ESG survey respondents indicated that CASB is a required or important component of a SASE architecture.[10] The shift to SASE comes in recognition that network security is no longer on-premises only but must provide distributed enforcement everywhere. By merging CASB back into the broader, foundational security architecture, management and policies can become integrated with other network security controls, relieving security analysts and practitioners of the burden of managing a layered CASB.

Introducing Palo Alto Networks' Next-Generation CASB

Palo Alto Networks' Next-Generation CASB seeks to deliver deep application visibility, simpler and more efficient management, and granular content and threat inspection.

Palo Alto Networks has introduced its Next-Generation CASB as an integrated solution to address the core cloud application challenges most organizations face today. The solution is natively integrated with Palo Alto Networks' next-generation firewall, enterprise data loss prevention, and Prisma Access for ease of deployment and broader DLP coverage. Palo Alto Networks anticipates both significant deployment time savings, as well as a lower total cost of ownership by running a leaner security architecture through this model. While full functionality is enabled through the use of the broader portfolio, not all tools are required for organizations to use Next-Generation CASB. The offering seeks to deliver deep application visibility, simpler and more efficient management, and granular content and threat inspection.

Comprehensive with Cloud-scale

Palo Alto Networks' Next-Generation CASB supports both inline and API deployment models. Inline scanning currently recognizes tens of thousands of applications and automatically adds new ones as they are seen by crowdsourcing the Palo Alto Networks customer base. The directory provides detailed application reports, as well as a risk score based on more than 40 application elements such as application type, SOC 2 compliance, privacy policies, and more. API integrations are currently available for many of the most common enterprise applications to support granular in-application control as well as streamlined compliance reporting for GDPR, HIPAA, PCA, and other mandates. This includes popular collaboration applications such as Slack, Jira, and Zendesk.

Simple and Cost-effective

The solution uses a unified management console and common interface across API and inline CASB deployments, as well as DLP policy creation. Through this unified console, rules can be more consistently applied to individuals and roles across both sanctioned and unsanctioned applications, reducing the potential for misconfigurations. Out-of-the box rules, automated worklfows, and ML-based automation provide ease of use to help customers get started quickly, but the solution also allows for broad customization. For example, application risk scores are tunable, allowing more risk-averse organizations to be more conservative with unsanctioned application usage. This can be adjusted based on specific factors such as the application group, data type, user role, and more. Additionally, Palo Alto Networks offers a single, unified cloud

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

console for managing Prisma Access, enterprise DLP, and Next-Generation CASB. This converged approach serves as an entry point to SASE by providing a consistent experience for users and ease of use for administrators.

Deep Content and Threat Inspection

Next-Generation CASB leverages Palo Alto Networks' broad visibility into threats through its Wildfire threat analysis capabilities and Unit 42 threat research group. Based on this intelligence, updates are pushed to the CASB as threats are identified while also utilizing machine learning to identify unknown threats in real time, all of which improves threat prevention for Next-Generation CASB use cases.

Content inspection for DLP control is supported by three types of rulesets: asset, user activity, and security controls. Asset rules rely on match criteria to identify sensitive data and support follow-on actions such as notifying the file owner, quarantining the file, removing public links to make the file unsharable, and more. User activity rules can be used to limit actions such as copy, move, and share across a single application or all applications, based on the data and individual in question. Security controls also provide auditing for security administrators, with role-based access control to ensure sensitive data is not compromised by first responders during investigation and remediation activities. The DLP engine uses more than 1,000 data identifiers combined with exact data match (EDM), optical character recognition (OCR), real-time machine learning, and natural language processing (NLP) through control points across the cloud and on-premises environments. This approach ensures sensitive data is consistently protected across all locations and applications, whether shared via file, screenshot, or collaborative chat.

The Bigger Truth

Unsurprisingly, the threat landscape continues to be the biggest cybersecurity challenge most organizations face. However, complexity is a significant and growing concern. The increasingly distributed nature of enterprise environments through cloud usage and, more recently, remote work, has challenged traditional security approaches. While the emergence of broader security transformations such as SASE can be directly tied to these changes, the reality remains that such a significant architectural shift takes time to plan and implement.

Organizations have prioritized cloud investments during the pandemic to improve flexibility and agility, and this will likely continue. As a result, a logical first step on the SASE journey is to begin assessing how to tie CASB back more closely into the network security stack in order to reduce complexity and improve the effectiveness of securing cloud application usage. Palo Alto Networks' Next-Generation CASB accomplishes this by focusing on tight integrations with existing network security tools and building on the strong security foundation the company has built over the last sixteen years. As a result, organizations should expect a simpler, cost-effective, comprehensive, and next-generation approach to CASB with Palo Alto Networks.

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