

WHITE PAPER

Protecting Applications, Data, and Users with Next-Generation CASB

By John Grady, Enterprise Strategy Group Senior Analyst

December 2022

This Enterprise Strategy Group White Paper was commissioned by Palo Alto Networks and is distributed under license from TechTarget, Inc.

Contents

Executive Summary	3
Changing IT Environments Create Complexity and Increase the Attack Surface	3
Remote Work	4
The Explosion of SaaS Application Usage Creates Complexity	4
Attacks on Applications are Common	4
Point Tools Only Exacerbate the Issue	5
SASE as a Consolidation Point for Protecting Distributed Workers, Data, and Applications	6
Key Attributes for Next-Generation CASB as Part of SASE.....	6
Support Zero Trust Tenets	6
Protect the Application.....	6
Prevent Data Leakage	7
Block Sophisticated Threats.....	7
Palo Alto Networks' Next-Generation CASB.....	7
The Bigger Truth.....	8

Executive Summary

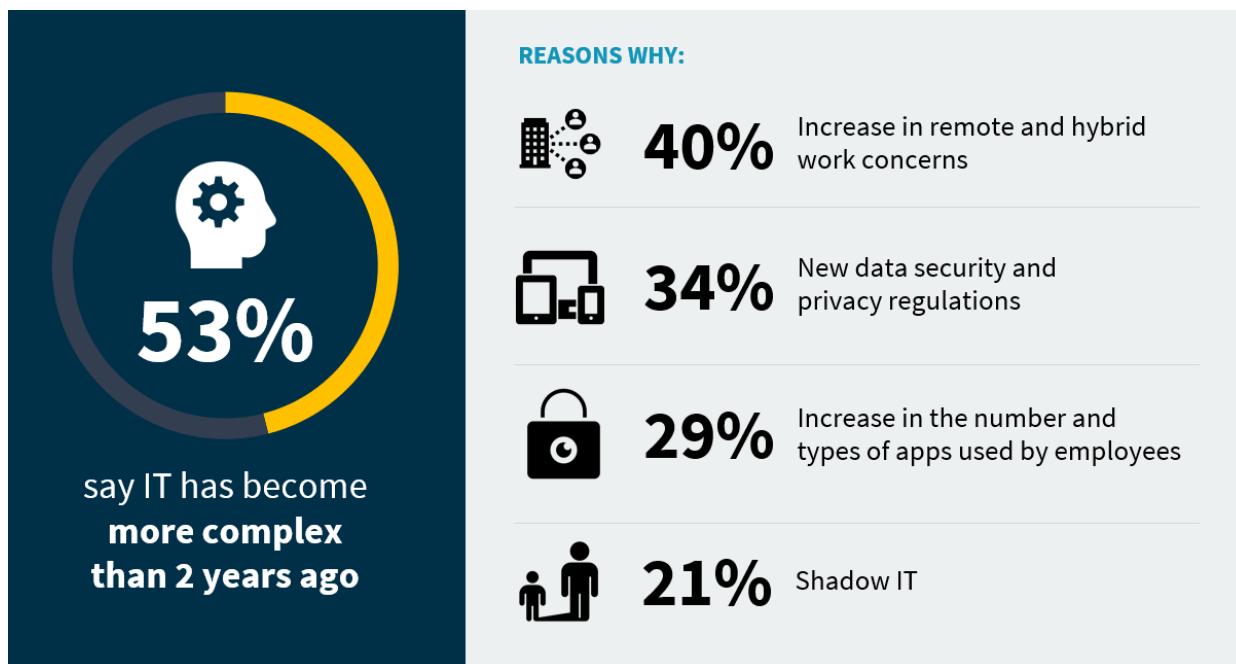
The rapid adoption of cloud and establishment of hybrid work have become the new pervasive trends as companies look to continue their digital transformations. Unfortunately, these changes make it difficult for security teams to efficiently and effectively maintain visibility, compliance, and security across the organization. In part to address these issues, secure access service edge (SASE) has emerged as a consolidation point for protecting distributed workers, data, and applications, with CASB as a focal point of the architecture.

In order to be an effective component of SASE, CASB must evolve to better support zero-trust initiatives, protect applications by detecting and remediating misconfigurations, prevent data leakage and abuse by insiders, and block sophisticated attacks as they occur. Palo Alto Networks offers a Next-Generation CASB as part of its [Prisma Access solution](#), and enables organizations to secure all their SaaS access, SaaS applications, and data and prevent threats.

Changing IT Environments Create Complexity and Increase the Attack Surface

IT and security teams have a lot on their plate. The nature of work has changed, with many employees now working in a remote or hybrid manner. The speed of change in the enterprise has accelerated as organizations undertake digital transformation initiatives to become more operationally efficient and develop new business models. Key to this transformation is the use of applications, and SaaS applications in particular, in business processes to improve productivity. All these changes have led to increased complexity, with TechTarget’s Enterprise Strategy Group (ESG) research finding that 53% of organizations say their IT environment is more complex than it was two years ago (see Figure 1).¹

Figure 1. IT Complexity Is Increasing



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

¹ Source: Enterprise Strategy Group Research Report, [2023 Technology Spending Intentions Survey](#), November 2022. All Enterprise Strategy Group research references and charts in this white paper have been taken from this research report, unless otherwise noted.

Remote Work

Forty percent of organizations indicated that their IT environment's increased complexity is due to the increase in remote and hybrid work concerns. Until recently, ensuring that remote employees had access to the tools they need to be productive and were protected from cyber risks was the exception rather than the rule. Now, remote and hybrid work is the dominant model for many organizations. This can limit visibility into the resources employees are using, the data they are accessing, and the threats targeting them. Organizations shifting to hybrid models opens additional concerns around consistency, both for users in terms of experience and administrators in terms of policy management and enforcement.

The Explosion of SaaS Application Usage Creates Complexity

One-third (34%) of Enterprise Strategy Group (ESG) research respondents cited new data security and privacy regulations as a driver of IT complexity. The breadth of applications in use often makes it difficult for IT and security teams to ensure resources are properly configured, protected, and compliant.

With hundreds of SaaS applications, each with a unique mix of settings and administrative consoles, it is extraordinarily difficult to ensure that all apps are properly configured all the time. The processes to do so are typically manual and keeping track of how every application is configured in a spreadsheet is not scalable to the hundreds of applications most

enterprises consume. Further, the feature and security updates for these applications are constant and ongoing, meaning that even if a security team manages to thoroughly audit each of their applications, they must immediately start over again, making this laborious process a continuous exercise.

The breadth of applications in use often makes it difficult for IT and security teams to ensure resources are properly configured, protected, and compliant.

Additionally, 29% of organizations point to the increase in the number and types of applications used by employees as one of the reasons for their IT environment's complexity. Over time, application usage has expanded from general productivity

applications, such as Microsoft Office, to a variety of departmental and role-specific applications supporting sales, marketing, human resources, finance, and other functions. In fact, ESG has found that 70% of research respondents say their organization uses at least 250 business applications.² The sheer volume of this usage is

70% of research respondents say their organization uses at least 250 business applications.

difficult for IT and security teams to keep pace with under the best of circumstances, and this has been exacerbated by the cloud. This trend is only expected to increase over the next three years, with 48% of organizations anticipating that more than 40% of their business applications will be public cloud-resident in that timeframe.³

Cloud applications, and enterprise SaaS applications in particular, offer many benefits, including speed of deployment, resiliency, and scalability. Yet, the resulting democratization of IT gives business users more influence and often more direct control over the applications in their department. As a result, one-fifth (21%) indicated that shadow IT is an issue that leads to increased complexity since it is not uncommon for individuals to purchase SaaS subscriptions via credit card, circumventing the standard procurement process that would typically give IT insights into their activities.

Attacks on Applications are Common

It should come as no surprise that security teams report a variety of attacks on SaaS applications. One of the most common attacks is the exploitation of an insecure configuration, which 26% of Enterprise Strategy Group (ESG) research

² Source: Enterprise Strategy Group Complete Survey Results, [2023 Technology Spending Intentions Survey](#), November 2022.

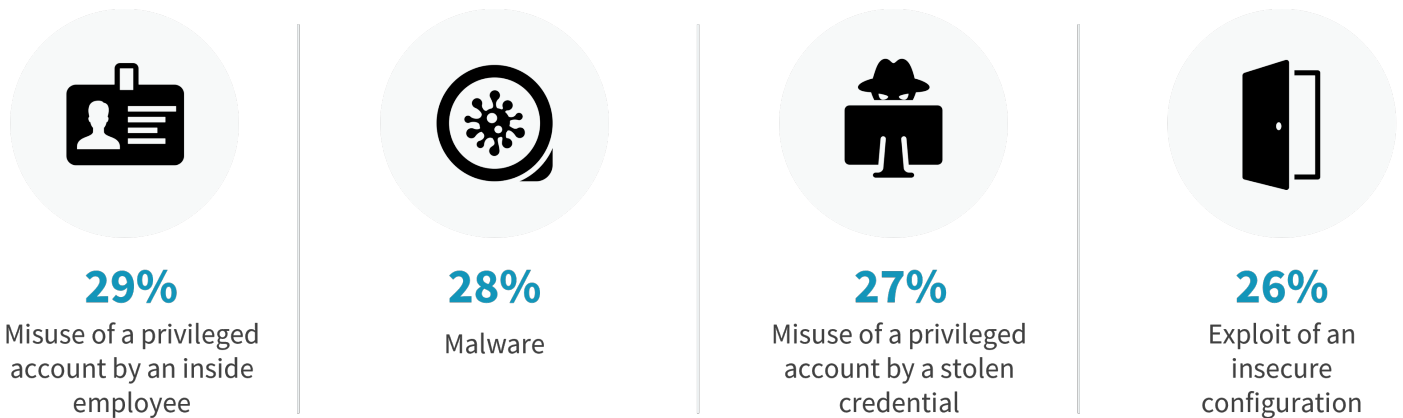
³ Ibid.

respondents indicated has occurred at their organization (see Figure 2).⁴ SaaS services may be misconfigured from the beginning or experience configuration drift away from established baselines over time. Weak or default password usage, excessive permissions, and authorization for users that are out of date can all occur and ultimately result in sensitive data being left exposed. Difficulty maintaining real-time, consistent visibility into SaaS settings across all of the different applications in use, as well as the number of roles and departments that can access those settings, can make the likelihood of misconfigurations even greater.

Other common SaaS attacks include:

- **Misuse of a privileged account by an inside employee (29%).** The potential for fraud and abuse, either willfully or through negligence, is of particular concern when it comes to privileged accounts. Because of the wide range of applications in use, hundreds of administrative accounts across all the SaaS applications may be used in the enterprise, not all of which may be known to the security team.
- **Malware (28%).** Attackers clearly understand the value SaaS applications offer as an attack target. SaaS applications often house a wealth of sensitive data that attackers may find attractive. Additionally, SaaS applications have increasingly been the target of ransomware attacks. Alternatively, attackers may target SaaS applications with malware as they attempt to propagate an attack and move across the environment.
- **Misuse of a privileged account via stolen credentials (27%).** As part of a broader campaign, attackers may use stolen credentials from administrative accounts as they move through the target environment.

Figure 2. Common Application Attacks Experienced



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Point Tools Only Exacerbate the Issue

As is often the case with cybersecurity, as new issues and threat vectors are uncovered, point products are developed to solve the issue. This is especially true with regard to how security teams protect their remote and hybrid employees and secure access to the applications these users need to do their jobs. Most enterprises use a variety of tools such as VPN for remote access, secure web gateway for threat prevention, data loss prevention to block unauthorized data usage, CASB to control SaaS usage, and SaaS security posture management (SSPM) to protect SaaS applications. This creates an enormous amount of tool sprawl, which adds to complexity, reduces efficiency, and can lead to ineffective security. This is

⁴ Source: Enterprise Strategy Group Survey Results, [Leveraging DevSecOps to Secure Cloud-native Applications](#), December 2019.

a significant problem across the industry, with 22% of security professionals indicating that managing the complexity of too many disconnected point tools is among the biggest cybersecurity challenges at their organization.⁵

SASE as a Consolidation Point for Protecting Distributed Workers, Data, and Applications

Taken together, these issues have resulted in a significant trend toward convergence and consolidation across the industry to help improve efficiency and achieve better security results. Secure access service edge (SASE) is a perfect example of this trend. SASE converges previously siloed network and security capabilities into a cloud-centric architecture, providing centralized management and distributed enforcement across the entire environment. Capabilities typically include SWG, CASB, zero trust network access (ZTNA), data loss prevention (DLP), and SD-WAN.

SASE is often discussed in the context of protecting users. In fact, when asked what are or will be their organization's initial SASE use cases, respondents cited several initiatives, including remote user security (47%), supporting zero trust initiatives (45%), enabling hybrid work environments (43%), modernizing secure application access (40%), and incorporating more data-centric security policies (38%).⁶

SASE architectures provide a logical consolidation point for all of the capabilities needed for complete SaaS security.

With all this in mind, SASE architectures provide a logical consolidation point for all of the capabilities needed for complete SaaS security through next-generation CASB. CASB

can provide visibility into both sanctioned and shadow SaaS application usage and support security for data at rest through API connections, as well as data in motion via inline scanning. By incorporating configuration management capabilities as well, SASE can provide a holistic approach to protecting applications, users, and data.

Key Attributes for Next-Generation CASB as Part of SASE

CASBs provide a logical consolidation point for all the capabilities needed for complete SaaS security. CASBs can provide visibility into both sanctioned and shadow SaaS application usage and support security for data at rest through API connections, as well as data in motion via inline scanning. However, to fully address the challenges discussed earlier, modern CASB solutions must support four critical areas.

Support Zero Trust Tenets

As discussed, zero trust is a key driver of many SASE initiatives, so by necessity, next-generation CASB must support zero trust tenets. This includes enforcing least privilege policies and remaining inline to continually inspect even after the connection is made. NG-CASB solutions must be able to assess the risk of a session based on the user, device, network, data, and other characteristics and take action if and when the trustworthiness of the entity changes. This also includes inspecting all content and user activity to ensure threats from malicious insiders are detected and blocked.

Protect the Application

SaaS Security Posture Management (SSPM) tools have been developed to help organizations ensure configurations remain aligned with industry standards and company policy. As mentioned, many breaches of SaaS applications are the result of misconfigurations. CASBs must be able to not only understand the range of enterprise SaaS applications in use, but also determine the risk the applications pose, assess the configurations of the applications, and determine when configuration drift occurs. While some CASBs provide this functionality for a handful of applications, enterprises need coverage across as

⁵ Source: Enterprise Strategy Group Complete Survey Results, [ESG/ISSA Cybersecurity Process and Technology Survey](#), June 2022.

⁶ Source: Enterprise Strategy Group Complete Survey Results, [2021 SASE Trends: Plans Coalesce but Convergence Will Be Phased](#), December 2021.

many major applications as possible for SSPM to meaningfully move the needle and provide deep visibility and coverage for the applications they do support. For example, some SSPM tools compare SaaS configurations solely to compliance benchmarks. While this is important to assure alignment with industry regulations and best practices, this approach may miss more subtle misconfigurations that can pose security issues. By looking at a broader range of settings and doing so through a security lens, the odds of detecting meaningful misconfigurations can be improved.

Further, when issues are detected, a streamlined remediation workflow is critical. Application owners are often spread across different roles within IT as well as the lines of business. Because these owners control the day-to-day management of their applications, security teams often do not have visibility into the configurations and are not able to make recommendations. This can lead to a lag time of days or even weeks between when an issue is detected and when it is finally remediated. Especially for critical issues, system-led remediation can help close security gaps much more quickly, without creating additional work for security teams or application owners.

System-led remediation can help close security gaps much more quickly, without creating additional work for security teams or application owners.

Finally, the interconnectedness of SaaS applications with third-party extensions and other connected applications continues to increase and poses additional risks that security teams may have difficulty recognizing or addressing. As this trend continues, it will be increasingly important to provide centralized visibility over the entire SaaS application ecosystem and configuration settings. This, coupled with the general application visibility a CASB already provides, will help security teams more effectively identify stealthy threats that might otherwise go undetected.

Prevent Data Leakage

Cloud access security brokers should also incorporate strong data security capabilities that go beyond checkbox compliance use cases. Many CASBs currently focus on recognizing data that is subject to regulatory requirements such as social security numbers, credit card data, and other personally identifiable information. But SaaS apps can house sensitive internal data as well that falls outside the scope of these capabilities. Further, it is increasingly common for sensitive information to be shared in real time via chat and other collaborative applications. To address this, modern CASBs should seamlessly integrate data visibility across a variety of channels and data types to protect passwords, API keys, and other corporate secrets.

CASBs should seamlessly integrate data visibility across a variety of channels and data types to protect passwords, API keys, and other corporate secrets.

Block Sophisticated Threats

Finally, CASBs should be able to tie together a deep understanding of applications and visibility into data, with inline threat prevention capabilities to stop attacks as they occur. As noted, malware generally, and ransomware specifically, is increasingly targeting SaaS applications. Identifying these attacks in real time should be a priority when assessing CASB solutions. Additionally, the use of analytics to identify when valid user credentials are used for suspicious or malicious activity, whether by insiders or compromised accounts, can help close two of the common SaaS application attack scenarios discussed earlier.

Palo Alto Networks' Next-Generation CASB

Palo Alto Networks offers a Next-Generation CASB as part of its SASE solution, Prisma Access. In addition to NG-CASB, Prisma Access offers SWG, ZTNA, and FWaaS capabilities. This convergence helps security and IT teams simplify operations

and streamline policy workflow management. NG-CASB enables organizations to secure all their SaaS access, SaaS applications, and data and prevent threats.

- **Secure SaaS access.** NG-CASB operates inline and securely connects all users and all apps with fine-grained access controls. Once access to an app is granted, trust is continually monitored to identify changes in device posture, user behavior, application behavior, and more.
- **Secure SaaS applications.** With the addition of SSPM, Palo Alto Networks' Next-Generation CASB is able to detect misconfigurations in sanctioned SaaS applications. Next-Generation CASB identifies both web and non-web applications, using ML-based identification and inline control for 40,000 enterprise and Shadow IT SaaS applications. From an SSPM perspective, the solution provides automated posture assessments for over 35 enterprise SaaS applications, with a goal of supporting over 100 applications by the end of the year. Rather than focusing solely on CIS or NIST benchmarks, Palo Alto Networks' SSPM compares configurations with comprehensive security best practices to assess a broader set of configurations than traditional tools. SSPM organizes all settings into a common framework using Palo Alto Networks' Posture Security Policy Engine to make it easier for security administrators to understand how configurations map to security issues and the relative risk of the misconfigurations discovered. This is different than the compliance-first approach other tools take, which might include only assessing some settings and structuring the posture assessment around compliance categories rather than security concerns. Finally, Palo Alto Networks' Next-Generation CASB emphasizes a prevention-first approach. SSPM provides both guided and automatic remediation as well as the ability to lock sensitive application configurations in place to prevent drift, which Palo Alto Networks claims reduces remediation times by 90%.
- **Secure data.** Through integrations with Enterprise DLP, Next-Generation CASB helps organizations prevent secrets and passwords from being improperly shared through real-time collaboration applications via the use of advanced data security capabilities, including natural language processing (NLP), image detection, and optical character recognition (OCR). These data security capabilities are available across a large catalog of enterprise SaaS applications through 27 API connectors. The combination of Enterprise DLP and user and entity behavior analytics (UEBA) provides detection of insider threats and compromised accounts using advanced behavioral analytics to identify suspicious login activity, unusual data access patterns, and other attempts to steal sensitive data within enterprise SaaS applications.
- **Prevent threats.** Next-Generation CASB also leverages Palo Alto Networks' broad visibility into threats through its WildFire threat analysis tool and Unit 42 threat research group. Based on this intelligence, updates are pushed to the CASB as threats are identified while also using machine learning to identify unknown threats in real time, all of which improve threat prevention for Next-Generation CASB use cases.

The Bigger Truth


CASBs may be one of the more underappreciated tools in the security stack. The combination of inline control with deep, API-based application integrations provides a unique level of visibility and control over applications, data, and users. With organizations housing more and more sensitive data in SaaS applications, it only follows that planning for SASE should prioritize tools that offer holistic SaaS security. By aggregating zero trust support, SaaS security, analytics-led threat prevention, and cloud-centric DLP in a SASE architecture, Palo Alto Networks' Next Generation CASB enables organizations to move beyond compliance and automatically harden and protect a wide range of SaaS applications against data breaches.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, 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 TechTarget, 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 Client Relations at cr@esg-global.com.



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

 www.esg-global.com

 contact@esg-global.com

 508.482.0188