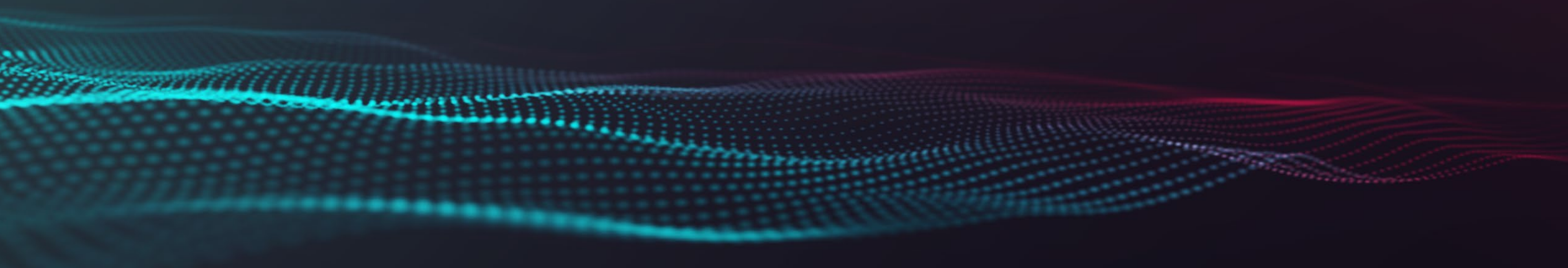
Enterprise Strategy Group | Getting to the bigger truth.™



ESG WHITE PAPER

Enhancing SaaS Security

Palo Alto Networks’ Next-Generation CASB with SaaS Security Posture Management

By John Grady, ESG Senior Analyst

September 2022

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

Contents

Executive Summary

The usage of SaaS applications continues to expand at a faster rate than security teams can keep pace with. As more applications are introduced and ownership becomes distributed across organizations the risk of misconfigurations grows, increasing the likelihood for security incidents to occur. As a result, organizations have become increasingly interested in SaaS Security Posture Management (SSPM) solutions to detect when SaaS applications are improperly configured. Unfortunately, security teams typically must decide between two less-than-ideal options. Some cloud access security brokers (CASBs) have begun to incorporate SSPM capabilities, but these may only cover a small number of settings for a limited number of applications and have a heavy focus on compliance rather than security. Conversely, pureplay SSPM tools can provide stronger functionality in some areas but require the addition of another point tool in the security stack, adding to already problematic tool sprawl. Additionally, because they are deployed as point tools, dedicated SSPM products can contribute to the tool sprawl so many security teams face today.

Given where they sit in relation to SaaS applications, CASBs provide a logical consolidation point for all the capabilities needed for complete SaaS security, including SSPM.

Given where they sit in relation to SaaS applications, CASBs provide a logical consolidation point for all the capabilities needed for complete SaaS security, including SSPM. However, functionality cannot be sacrificed for efficiency, and the criticality of ensuring SaaS applications are properly configured is no exception. Thus, in addition to offering robust SSPM, modern CASBs must provide strong security protection across both data and threats. Palo Alto Networks' Next-Generation CASB supports these requirements through its security-focused SSPM capabilities, coupled with comprehensive application coverage, DLP, and a history of analytics-led threat prevention.

The Explosion of SaaS Application Usage Creates Complexity

Enterprise use of applications continues to grow as companies look to engage with customers, connect with partners, and better enable employee productivity. Yet at the same time, applications are often cited both directly and indirectly as a leading cause of IT complexity.

Overall, 46% of organizations say their IT environment is more complex than it was two years ago (see Figure 1). One-third (33%) of organizations point to the increase in the number and types of applications used by employees as one of the reasons for that complexity.[1] 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 67% of research respondents say their organization uses at least 250 business applications. The sheer volume of this usage is 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 44% of organizations anticipating that more than 40% of their business applications will be public cloud-resident in that timeframe.

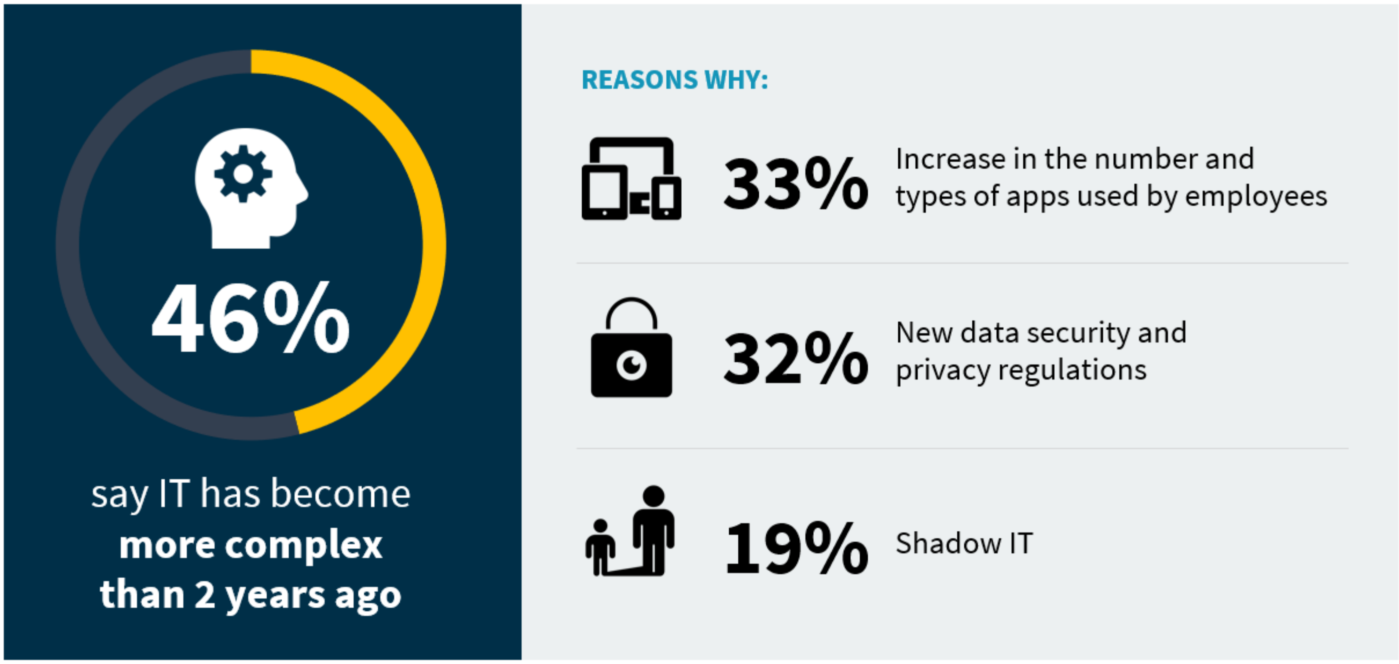
Additionally, 32% of ESG research respondents cite new data security and privacy regulations as a driver of IT complexity. The breadth of applications in use often makes it difficult for IT and security teams to ensure resources are properly configured, protected, and compliant. With hundreds of SaaS 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

[1] Source: ESG Complete Survey Results, *2022 Technology Spending Intentions Survey*, November 2021. All ESG research references and charts in this white paper have been taken from this complete survey results set, unless otherwise noted.

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 rate of change within these applications is constant, 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.

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, nearly one-fifth (19%) 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.

Figure 1. IT Complexity Is Increasing Due to Application Usage



Source: ESG, a division of TechTarget, Inc.

Attacks on Applications are Common

One of the most common attacks is the exploitation of an insecure configuration, which 26% of ESG research respondents indicated has occurred at their organization.

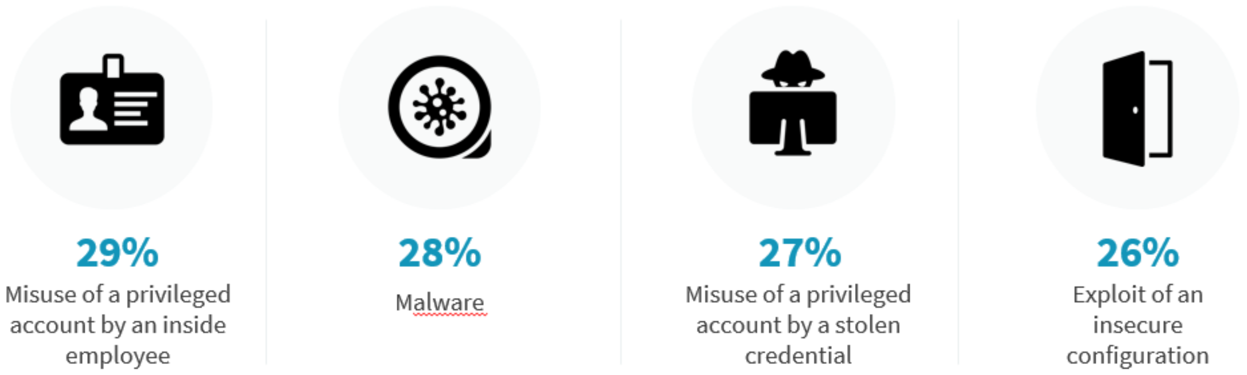
It should come as no surprise that security teams report a variety of attacks on SaaS applications. One of the most common attacks is the exploitation of an insecure configuration, which 26% of ESG research respondents indicated has occurred at their organization (see Figure 2).[2] SaaS services may 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

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

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.
- 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.
- 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.

Figure 2. Common Application Attacks Experienced



Source: ESG, a division of TechTarget, Inc.

SaaS Security Should Not Be Fragmented

SSPM tools have been developed to help organizations ensure configurations remain aligned with industry standards and company policy. Yet, even with this being the case, many teams continue to struggle. ESG research has found that 30% of organizations say that meeting prescribed best practices for the configuration of cloud services and workloads is a challenge.[3] More importantly, while tying configuration baselines to compliance standards and best practices may reduce some aspects of the threat surface, it does not offer comprehensive assessment across all settings to ensure a secure foundation for the application.

[3] Source: ESG Research Report, *Leveraging DevSecOps to Secure Cloud-native Applications,* March 2020.

Additionally, these tools typically fail to address threat prevention or data security, which remain significant issues for many organizations. Data security in the cloud is of particular concern because of the difficulty in maintaining consistent visibility across so many applications and locations. Supporting this point, ESG research has found that 33% of organizations said they have lost cloud-resident data, while an additional 28% believe they have but cannot be sure.[4]

33% of organizations said they have lost cloud-resident data, while an additional 28% believe they have but cannot be sure

As is often the case with cybersecurity, as new issues and threat vectors are uncovered, point products are developed to solve the issue, meaning many organizations are forced to deploy multiple tools for comprehensive SaaS security. This is 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] This has resulted in a significant trend toward convergence and consolidation across the industry to help improve efficiency and achieve better security results, which is something that SaaS security would benefit from as well.

Posture Management, Data Security, and Threat Prevention are Critical for Modern CASB

CASBs provide a logical consolidation point for all of 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 three critical areas.

SaaS Security Posture Management

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 many major applications as possible for SSPM to meaningfully move the needle and 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.

CASBs provide a logical consolidation point for all the capabilities needed for complete SaaS security.

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 line-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.

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

[4] Source: ESG Research Report, *The State of Data Privacy and Compliance,* March 2022.
[5] Source: ESG Complete Survey Results, *ESG/ISSA Cybersecurity Process and Technology Survey*, June 2022.

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.

Data Loss Prevention

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.

Threat Prevention

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, are 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 Offers a Holistic Approach to Securing SaaS with Next-Generation CASB

Palo Alto Networks has expanded its Next-Generation CASB to include SaaS Security Posture Management. With the addition of SSPM, Palo Alto Networks' Next-Generation CASB is able to detect misconfigurations in sanctioned SaaS applications. Additionally, Next-Generation CASB is part of Palo Alto Networks' broader Prisma Access SASE solution, helping security and IT teams simplify operations and streamline policy workflow management. The solution provides three key values for organizations seeking to prioritize SaaS security. These are:

- Comprehensive application coverage. 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.

- Security beyond compliance. Rather than focus 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 discover. This is different than the compliance-first approach other tools take, which might only assess some settings and structure the posture assessment around compliance categories rather than security concerns.

- A prevention-first focus. Finally, Palo 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%. Additionally:

- 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.

- 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

Ensuring corporate resources are properly configured has always been an uphill battle for security and IT teams. Unfortunately, the shift to the cloud has made the task more Sisyphean than ever: there are more SaaS applications than ever to keep track of and more settings and configurations to assess. In addition, distributed application ownership leads to a constant rate of change and unending cycle of detection and remediation of configurations. Complicating the issue, these misconfigurations can often lead to attacks on SaaS applications and breaches, resulting in data loss.

CASB tools have a unique position in the security stack, combining both out-of-band security for the data within SaaS applications through API integrations, with inline policy enforcement and control over data-in-motion for real-time protection. As a result, this represents a logical point to incorporate SSPM functionality for comprehensive protection of SaaS applications. However, these capabilities must be on par with purpose-built tools and provide broad coverage across a wide number of enterprise SaaS applications, deep visibility into the settings within each application beyond compliance benchmarks, and, ideally, help bridge the gap between security teams and application owners. The addition of SaaS Security Posture Management augments Palo Alto Networks' Next Generation CASB capabilities, which include analytics-led threat prevention and cloud-centric DLP, to enable organizations to move beyond compliance and automatically harden and protect a wide range of SaaS applications against data breaches.

ESG a division of TechTarget

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