White Paper

Exploring Next-Generation CASB Concepts for Evolving Cloud Security Practices

Sponsored by: Palo Alto Networks

Christopher Rodriguez
July 2022

INTRODUCTION

The cloud has proven to be an invaluable technology in the digital transformation era, offering agility, scalability, and business value. SaaS in particular offers turnkey operations and innovative functionality that has driven business value and unlocked new use cases. Overall, the move to the cloud is changing how people approach work. IDC research shows that 41% of IT organizations are now reliant on cloud-managed, cloud-based services (source: IDC's *Future Enterprise Resiliency and Spending Survey,* February 2021, n = 1,191).

However, the cloud also presents a multitude of unique security considerations. Over the years, cloud providers and customers have answered tough questions, such as "who is responsible for certain security practices" and "what deployment models support which use cases." However, the nature of cloud adoption continues to evolve, thus changing business practices. Security practices and architecture must evolve to adapt as well, to stay ahead of threat actors.

SITUATION OVERVIEW

Profiling the Modern Cloud Environment

New Tools Take Precedence

IDC has identified a shift in the tools that businesses rely on to drive productivity. According to IDC's February 2021 *Future Enterprise Resiliency and Spending Survey* (n = 1,191), 30% of businesses have developed a preference for online-first collaboration.

As a result, there are more SaaS apps in use in enterprise IT environments than ever, and that number is only continuing to grow. IDC research shows that a third of organizations are dependent on 10+ distinct public SaaS environments (source: IDC's *Data Security Survey,* January 2020, n = 620). Another 7.6% are dependent on 25+ public SaaS environments, and some respondents relied on over 50 public SaaS environments.

While this research is based on a strict definition of "public SaaS environments," the trend is toward a proliferation of application functionality beyond mainstream public SaaS providers. Websites are replete with applications offering a wide array of new and innovative functionality. Accounting for this emerging segment of semi-SaaS environments, IT organizations must account for work activity spread across potentially thousands of sites.

IT Democratization Changes the Nature of Work

The move to the cloud, and SaaS in particular, has been steered significantly by workers. This is changing not only the location of where work happens but also how it happens. For instance, consider the shift toward collaboration apps such as Teams, Slack, or Zoom. The growing usage of these collaboration tools comes at the expense of email. About 76% of workers using team collaboration applications reduce email by over 20%, and some organizations by far more, according to *IDC's Annual Collaboration Study, 2020: The Benefits Emerge* (IDC #US43486518, March 2020).

Speed of Communications and Fluency of Data

The move to SaaS has also changed the data that is shared, how it is shared, and associated risks. Communications are now real time and asynchronous. Collaboration tools change the speed at which workers interact. These environments can lead to changes in communication as well. Positively, a real-time communications channel can lead to more insightful discussions and heightened productivity. It can also lead to a more casual tone, degradation of boundaries or norms, and relaxed awareness of policy and best practices.

Similarly, risk to data is changing as well. Data from these conversations is primarily unstructured. Data is no longer represented in simple text files or spreadsheets but is shared in conversation and images. Copy and paste, screenshots, or data divulged in conversation are all high-risk activities that can lead to data loss, whether intentionally or not.

The Current State of CASB

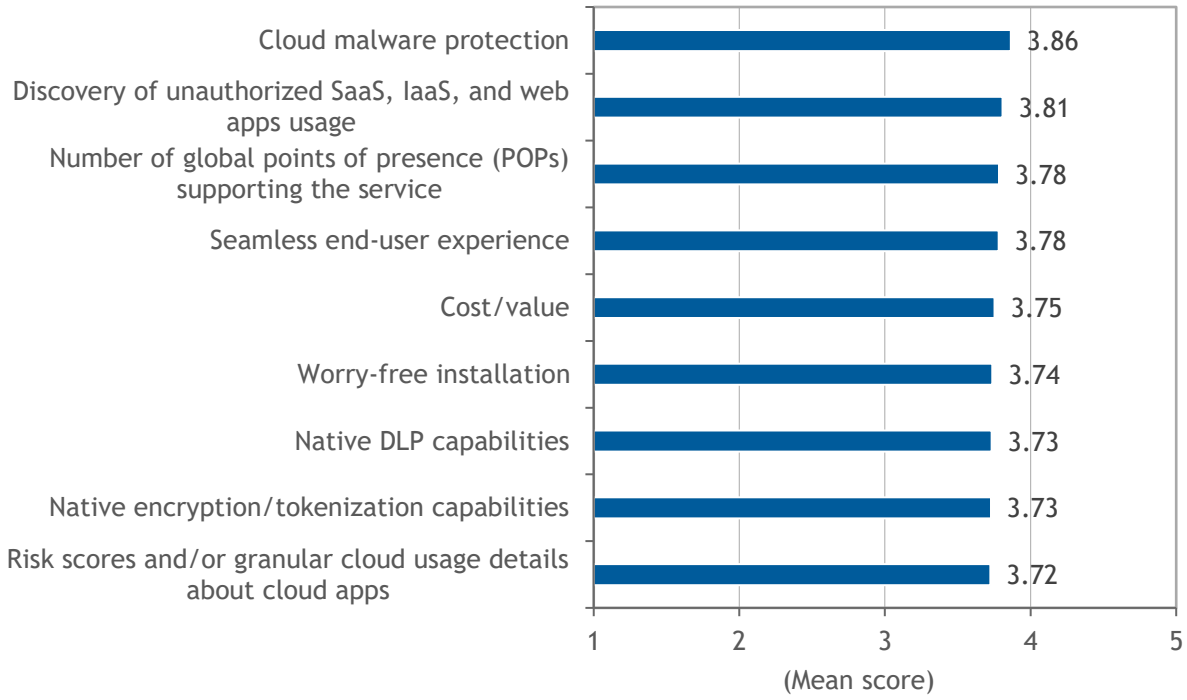
CASB Capabilities and Complexity

Cloud access security broker (CASB) has emerged as the solution of choice for protecting cloud services and related data. CASB addresses several security requirements, and buyer expectations have shifted over the years, but a hierarchy of needs has emerged. "Discovery of unauthorized SaaS/IaaS/web app usage" is an early use case that remains popular, rating as the second most important function of CASB. However, over the years, CASB has become increasingly focused on threat prevention, with IT buyers rating "cloud malware protection" as the top benefit of CASB. Data loss prevention (DLP), encryption/tokenization, misconfiguration detection, SaaS configurations, and risk scoring are other key functions of CASB. Figure 1 shows the top use cases for CASB.

FIGURE 1

Top Features of Current CASB Solutions

Q. Please rate the importance of the following features and attributes of your present cloud security gateway provider on a scale of 1-5, where 1 = not at all important and 5 = critical.



n = 620

Source: IDC's *Data Security Survey,* January 2020

Changing business practices and security requirements have forced an evolution in CASB solutions. Currently, the preference is for multimode protection that capitalizes on the benefits of both inline and out-of-band CASB deployments. Multimode CASB leverages inline inspection and API integrations to balance broad, "active" protection of data in transit with extensive capabilities for protection of data at rest. Overall, confusion about CASB capabilities and options has dissipated over the years, but complexity of legacy CASB has presented a hurdle to full security maturity. CASB vendors have developed further integrations in their solutions to ensure consistent base-level protection with deep functionality for specific SaaS environments as needed.

SaaS Requires Unique Protections, But Not Silos

Adoption of cloud services changes the need and ability for enterprises to implement security. Business leaders must keep in mind that the cloud provider does not inherently address all security requirements. In the early stages of cloud adoption, IT organizations focused on extending existing security controls to the cloud. Over time, more appropriate tools have gained broad adoption such as CASB or CSPM. In addition, SaaS adoption requires businesses to continue security practices such as data protection and identity management rather than infrastructure protection.

Despite its unique requirements, cloud is only one aspect of the broader enterprise IT ecosystem. Telemetry must be collected across all threat vectors for analysis and detection of indicators of compromise. Management and reporting must be centralized to ensure consistent policies. Essentially, risk management must be applied via holistic, complete, and integrated security platforms.

Customers have traditionally faced trade-offs in functionality between comprehensive network security platforms and specialized solutions. As a result, enterprises with specialized requirements or interested in particular features, or application support, have focused on point product security strategies. Overall, these trade-offs are becoming untenable, and holistic security platforms are gaining interest. While convergence is a basic value of these integrated platforms, the true benefit of integration is to catch more elusive threats.

FUTURE OUTLOOK

Aligning CASB to the Unique Requirements of Modern Cloud Practices

Automation Becomes Table Stakes

By necessity, CASB solutions provide protection that is both broad and deep. Enterprise IT administrators must account for "democratization of IT" where users select the cloud and web applications they would prefer to use for work. These cloud applications enable workers to create, access, manipulate, and share data from the ease of their browser.

Manual processes for detecting and classifying applications are no longer viable as the threat surface is continually expanding. Cloud and web applications number in the tens of thousands and increase each year, with no signs of slowing. When asked what their organization's greatest challenges to establishing organization trust today is, respondents listed "lack of advanced tech such as automation" (21%) and "lack of visibility into applications and data assets" (20.8%) as the top 2 challenges (source: IDC's *Future of Trust Survey,* February 2021, n = 507).

These security functions (i.e., automation and visibility) are closely related. Rote, manual researching and classification of public SaaS applications is not a tenable approach for assessing cloud risk. Machine learning is required for the foundational security function of discovering and inventorying the cloud applications in an IT environment.

While visibility and policy enforcement remain essential CASB functions, security needs are expanding to include detection of indicators of compromise, insider threats, account takeover, and other high-severity risks. Automation and orchestration capabilities are key to detecting and mitigating these advanced threats.

The Importance of "Intent" to Risk Management

Security has evolved from simple binary decisions to a deeper understanding of risk. Simple binary determinations about content (malicious/benign) or access decisions (permit/deny) are essential at a base level. However, a deeper level of insight into user intent is required to identify insider threats and compromised accounts. These users are typically authorized and authenticated, and certain activities may be part of a job function. Detection of a malicious insider or compromised account may require a combination of signals (e.g., time of day, recipient, data type, and presence of external stimulus) that is not possible with outcome-only triggers.

This threat vector is a growing area of concern, as 18.7% of organizations expressed "potential insider threats" as a key challenge to establishing organizational trust (source: IDC's *Future of Trust,* February 2021, n = 507). On the other hand, understanding intent enables identification of violations that are unintentional and require corrective responses instead of punitive actions. Most users are well meaning and make simple mistakes that require education and reminders, not punishment. Therefore, it is not only the impact of a given action that determines risk but rather the combination of action and intent.

Extend Defenses to "Layer 8"

End users are the first and last line of defense. Workers have been more productive since the pandemic and adoption of work-from-home models. According to IDC's 2020 *Future Enterprise Resiliency and Spending Survey* (n = 800), 55.5% of organizations experienced a percentage increase in productivity of up to 25%, while another 38.3% achieved up to 50% increases in productivity resulting from investments in digital transformation. These productivity gains require workers to work faster and more efficiently. Unfortunately, increased speed raises the potential for accidental data leakage.

Attackers have identified this vulnerability and are increasingly leveraging social engineering techniques to coerce an unauthorized action from an authorized user. While many of these attacks reached users through unsolicited email messages, other vectors such as social media, poisoned links, and phishing sites provide many new paths to deliver targeted, crafted attacks to unsuspecting end users.

End users require continuous coaching and real-time feedback to learn from security missteps and reduce risky behavior. Protecting end users in the cloud environments of their preference ultimately enables them to be more productive. As such, CASB provides protection of productivity. However, detection must be accurate, and corrective actions must be surgically precise, and invisible to end users when possible. CASB solutions that hamper legitimate activity force business leaders to make risky decisions in the name of enabling productivity.

Evolving from Data Security to Information Protection

The shared responsibility model for cloud security reduces customers' need or ability to control infrastructure. SaaS in particular removes the requirement for customers to secure physical data systems, as well as servers, hypervisors, and networks. However, this model leaves data security in the customers' hands at a time when sensitive data is more distributed and vulnerable than ever across multiple SaaS environments.

For CASB solutions, this means data loss prevention functionality is becoming table stakes. When asked to "rate the following features of your present DLP solution (1 = not important and 5 = critical)," respondents rated "integrated CASB" as the top response (source: IDC's *Data Security Survey,* January 2020, n = 620). CASB expectations continue to expand to address data security concerns. Exact data match (EDM), natural language processing (NLP), optical character recognition (OCR), and other advanced capabilities are becoming a "must-have" for CASB to identify data, accurately and with actionable reporting. Each technology plays a key role, such as:

- **EDM:** Detection of specific sensitive records instead of pattern matching (EDM allows administrators to identify specific data points flagged as sensitive, rather than all data points that resemble sensitive data.)

- **NLP:** Provides analysis of conversational human language, including identification of forms of speech (e.g., suggestions, requests, and queries) (NLP provides insight into intent and possible forms of manipulation, such as a call to action under implication of urgency or penalty.)
- **OCR:** Analytics applied for image analysis purposes (OCR detects data latent in images, including various typefaces and handwritten characters.)

While these technologies are essential for data security, the role of CASB is quickly evolving to a broader mission of information protection. Information is "data with context" – a contextual understanding of data allows security teams to apply security smartly. Cloud security must expand to include a full understanding of data, data types, data usage, and context in order to detect threats and abuse. Context is required to minimize false positives, which can create alert fatigue, because alerts must be accurate to be actionable. NLP and other advanced technologies are required to achieve context-aware, intent-based protection of information and data.

For Consideration: Palo Alto Networks Next-Generation CASB

Palo Alto Networks made significant strides in the CASB market in 2021 and has continued to invest in the CASB offering. CASB-related developments in 2022 are discussed in the sections that follow.

Breadth and Depth of Cloud Coverage

In the CASB market, "more is more" – with incalculable numbers of applications available from the comfort of their browser, end users are driving a rapid expansion of the IT environment. For IT organizations, the fundamental challenge is to understand the scope and extent of cloud application usage. To support these enterprise requirements, Palo Alto Networks has expanded its application coverage in 2022, including supporting more applications with inline, holistic visibility and with a more robust set of API integrations for deep functionality control.

This development required extensive investment into automation, which in turn provides customers with scale and time to value. For example, machine learning applied to application profiling enables categorization of new applications at the pace required for cloud adoption. The approach also leverages crowdsourced intelligence to ensure complete coverage. Palo Alto Networks is further expanding coverage to support specialized applications, supporting full protocol analysis beyond HTTP traffic.

Meeting Growing Data and Information Security Requirements

Data and information protection has been a growing strategic focus for CASB vendors. Collaboration applications in particular present unique challenges to legacy CASB solutions because they encourage natural conversations and real-time sharing. These conversations are unstructured and made of multiple posts that need correlation and contextualization. Static DLP detections and coarse-grained CASB controls are quickly emerging as a pain point for collaboration applications.

To address this particular use case, Palo Alto Networks has added NLP technologies to its Next-Gen CASB, which provides detection of sensitive conversations between two or more users on collaboration apps like Slack, Teams, Zoom, Jira, and Confluence. Overall, Palo Alto Networks has added multiple new technologies to its solution, including EDM, OCR, NLP, and machine learning to improve its data and information protection capabilities.

Integration and Ecosystem Support

Palo Alto Networks offers Next-Generation CASB as part of its complete Prisma SASE solution. This solution provides an important option for enterprises that not only require high-security efficacy and/or specific advanced features but also require consolidation or integration of network security tools.

In addition, Palo Alto Networks Next-Gen CASB features full integration into enterprise security ecosystems including SOC tools and SOAR tools. While the solution features deep integrations with Palo Alto Networks' suite of analytics and management tools including Cortex XSOAR and Cortex XDR, the company has maintained a vendor-agnostic approach to support heterogeneous customer environments.

Palo Alto Networks has smartly considered the end user as part of the ecosystem as well. The company now offers a new security bot to support user engagement. End-user feedback and coaching are critical to reducing risk completely, with real-time feedback providing immediate protection and long-term improvements in reduced high-risk behavior.

CHALLENGES/OPPORTUNITIES

Challenges

Palo Alto Networks has made a concerted push into CASB, with a strong value proposition based on the integration with the company's secure access service edge (SASE) platform. While convergence is a critical strategic priority in network security, the strategy is likely to require an ongoing level of education to assuage concerns of vendor lock-in. In addition, extensive convergence trends violate a key security principle of "separation of powers" – some security decision makers have expressed a desire to avoid over concentration of security tooling into a common potential point of failure, anecdotally. Colloquially, this is the "too many eggs in one basket" rule.

Opportunities

In the cybersecurity industry, this concern has been most prominent when vendors attempt to span key security control points such as network, endpoint, identity, or applications. For Palo Alto Networks Next-Gen CASB, the company will be able to address these concerns by highlighting the heightened accuracy and timely detection of advanced threats enabled by a smart integration strategy.

CONCLUSION

Security strategy is typically reactive – IT buyers are focused on the threats that are most evident and under attack. Cloud applications are in the crosshairs now, more than ever, as cybercriminals search for new vectors for data theft and malware propagation. CASB is evolving quickly in response, and vendors are racing to "meet the puck" as IT buyers begin to modernize and mature their cloud security practices.

Palo Alto Networks has demonstrated a strategic focus on navigating emerging trends of information and data protection evolution, changing business practices, new cloud technologies, and shifting convergence trends that affect the CASB market. Palo Alto Networks' continued progress in these key areas will empower enterprises meet the next generation of security requirements without sacrificing the business value of the cloud.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com