



The Enterprise Buyer's Guide to

Next-Gen CASB Security



Table of Contents

1. Enterprise SaaS Adoption is Growing at Rapid Rates	3
2. The Explosion of SaaS is Creating an Unbearable Chaos	4
3. Shadow IT: It's a Bigger Threat Than You Think	5
4. Three Questions About SaaS in the Enterprise.....	6
5. SaaS Security Problems that Keep CISOs Up at Night	7
6. Legacy CASBs Can't Keep Up with the Explosion of SaaS.....	9
7. The 5 Must-Haves to Look for in a Next-Gen CASB Solution	10
8. SaaS Security by Palo Alto Networks.....	16
9. Summary of Benefits	18

Enterprise SaaS Adoption is Growing at Rapid Rates

SaaS applications continue to transform how organizations do business. The pandemic has only served to intensify their adoption.

Modern enterprises strive to achieve the highest levels of efficiency and business productivity in the shortest amount of time to maintain their competitive edge and remain relevant. Software-as-a-Service (SaaS) applications built for the modern enterprise make this possible with their unmatched simplicity, intelligence, ubiquitous availability, and ease of use.

It's no surprise that the valuation of the market for cloud-delivered SaaS products such as Salesforce, Hubspot, Google Apps, Zoom and many others continues to grow. As the first cloud-based service to truly take off and proliferate, SaaS has a significant lead on other cloud services. Gartner estimates that SaaS will continue to maintain its dominance as the largest market segment in worldwide IT spending this year and beyond.

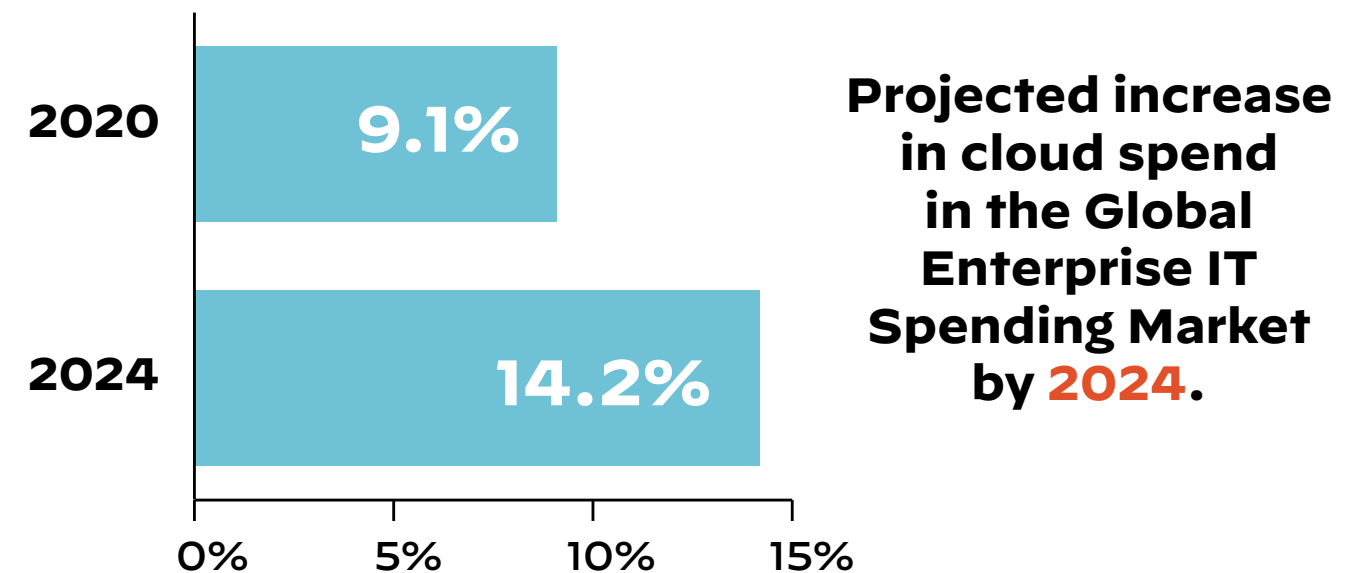
Gartner predicts that worldwide end-user spending on public cloud services is forecast to grow **23.1%** in 2021 to total **\$332.3** billion, up from \$270 billion in 2020, according to their latest forecast. Enterprise SaaS is still the largest market segment in worldwide IT spending and is forecast to grow to **\$145.3B** in 2022.

50%

The percentage rise in the overall spend per company on SaaS products in 2020.

30%

The YoY percentage increase in the number of sanctioned apps in use per company in 2020.



The Cloud of the future will be a disruptive market. It'll enable enterprises to adopt emerging technologies such as containerization, virtualization and edge computing that continue to spawn and become mainstream.

Sources:

- Blissfully SaaS Trends Annual Report, 2020
- Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021

But the Explosion of SaaS is Creating Chaos

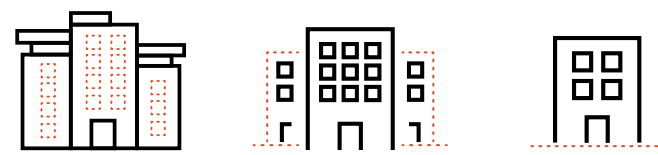
SaaS adoption across numerous departments creates a chaos that is hard to contain.

While the adoption of SaaS is transforming how companies of all sizes conduct business, a growing trend of note is that SaaS products are being adopted and used by nearly every business function across the organization. Besides IT and Security, these include customer support, HR, product, engineering, devOps, finance, marketing and sales.

As SaaS proliferates across all these business functions, it also means that its ownership and management is becoming increasingly distributed. In the earlier days, IT teams were primarily responsible for selecting technology for the entire organization and handled most software vendor management challenges, including budgeting, purchasing, onboarding, offboarding, and security.

Today, the shift towards decentralization of SaaS is catching IT teams off-guard in terms of tracking, evaluating, maintaining and protecting all SaaS apps in use from a security perspective. The typical enterprise uses hundreds of sanctioned apps that lead to thousands of app-to-people connections—that need to be secured.

SaaS Spend & Usage Stats by Market Segment in 2020



SaaS Statistic (per company)	Overall	Enterprises	Medium-level companies	Small-level companies
Spend	Up by 50%	\$4.16M	\$2.47M	\$202K
Unique Saas Apps	137	288	185	182
App to person connections	–	21,580	4,406	624
Saas app churn	30%	46%	29%	35%
# of duplicate apps	3.6	7.6	5.8	2.3
# abandoned app subscriptions	2.6 (up by 100%)	7.1	4.3	1.4
# of billing owners per company	–	98	32	10

Sources:

- Blissfully

Shadow IT is Here to Stay and a Bigger Threat Than You Think

To ensure data security, organizations need to effectively monitor, govern and moderate the use of unsanctioned SaaS apps.

When employees from various teams prefer to access their own SaaS solutions to get work done and also for personal needs, this situation gives birth to “**shadow IT**” that nearly exclusively refers to the unsanctioned use of SaaS applications and other cloud services. The risks of shadow IT have increased substantially with remote employees working from home on unsecured networks. Many employees circumvent the corporate VPN to access these apps directly and several others access company resources using personal, unmanaged devices, which makes shadow IT harder to detect and block.



SHADOW IT DISABLES IT TEAMS FROM ADMINISTERING CONTROL OVER DATA SECURITY

IT has no centralized control over what sensitive and proprietary business data gets dispersed across thousands of unvetted and unsanctioned cloud services and applications. The unmanaged repositories of data residing outside the organization’s established security boundaries result in unknown expansion of attack surfaces.



SHADOW IT GOES AGAINST AN ORGANIZATION’S DATA COMPLIANCE REQUIREMENTS

Shadow IT is not managed by the IT team so they have little to no visibility into the compliance ramifications of these unapproved apps and the data being transferred or stored through them. Shadow IT creates the burden of additional regulatory audit points, where proof of compliance must be expanded.



SHADOW IT STRAYS EMPLOYEES FROM PRESCRIBED SECURITY BEST PRACTICES

Most of the time, employees’ motivations for using shadow IT apps are not malicious or negligent, but despite their best intentions, shadow IT poses serious risks to enterprise cyber security by opening up the organization to the possibility of data breaches, insider threats and by turning into entry points for malware and other adversaries.

Gartner predicts that Shadow IT takes up 30 to 40% of overall IT spending for large enterprises. This means close to half of your IT budget is spent on technology that is unapproved by IT. Additionally, by 2022, one-third of successful attacks experienced by enterprises will be on their shadow IT resources.

Source:

- Don't Let Shadow IT Put Your Business At Risk, Smarter with Gartner

Every Organization is Grappling With Three Key Questions

As cloud adoption accelerates, decision-makers from companies of all sizes and across geographies admit that cloud security is top of mind.



Applications

What apps are employees using and how?

All organizations witnessing a massive expansion of their remote workforce are pursuing a bold multi-cloud SaaS strategy. But a lack of supervision over SaaS app usage behavior by remote employees creates doubt about the confidentiality and privacy of sensitive data and may introduce risks or threats.



Data

How do we protect sensitive data in the cloud?

Some types of data by its very nature needs to be accessed by a wide group of users, while access to more sensitive data often needs to be limited to a smaller subset. An endless array of data use case requirements across various teams create daunting levels of data protection complexity.



Users

Can we govern access to SaaS apps and secure them from threats?

Cloud service providers offer some security and compliance, but that doesn't absolve enterprise customers from protecting their data, users and apps from threats. The question of who is responsible for security in the cloud – the enterprise customer or the cloud service provider – is a point of contention.

While SaaS Security Problems are Keeping CISOs Up at Night

For all the business value that SaaS offers, security concerns are a key factor that restrict enterprises from taking the leap from on-premises data centers to SaaS solutions.

While transformative SaaS solutions help businesses thrive and scale at speeds hardly seen before, there's also a dark and challenging side to adopting them. Enterprise CISOs often find themselves plagued with 'unknowns' when the spotlight is turned on the question of securing SaaS. Cloud-based SaaS solutions elicit concerns in CISOs because they require having to give up a degree of control and visibility to the SaaS vendor. That control is harder to let go when data happens to be at front and center of it all. Moreover, CISOs have to content with different degrees of security from app to app, with many apps having no security at all—creating inconsistencies in their SaaS security strategy.

Pressing Security Problems with SaaS Applications



SHADOW IT

Unauthorized apps used and managed without IT's knowledge and approval.



LACK OF VISIBILITY

Lack of visibility into what data resides or travels in the apps—from sensitive information to malicious files.



DATA EXPOSURE

Accidental data exposure and risk of data theft.



THREATS AND MALWARE

Advanced threats and malware targeting SaaS applications, users and data.



USER BEHAVIOR

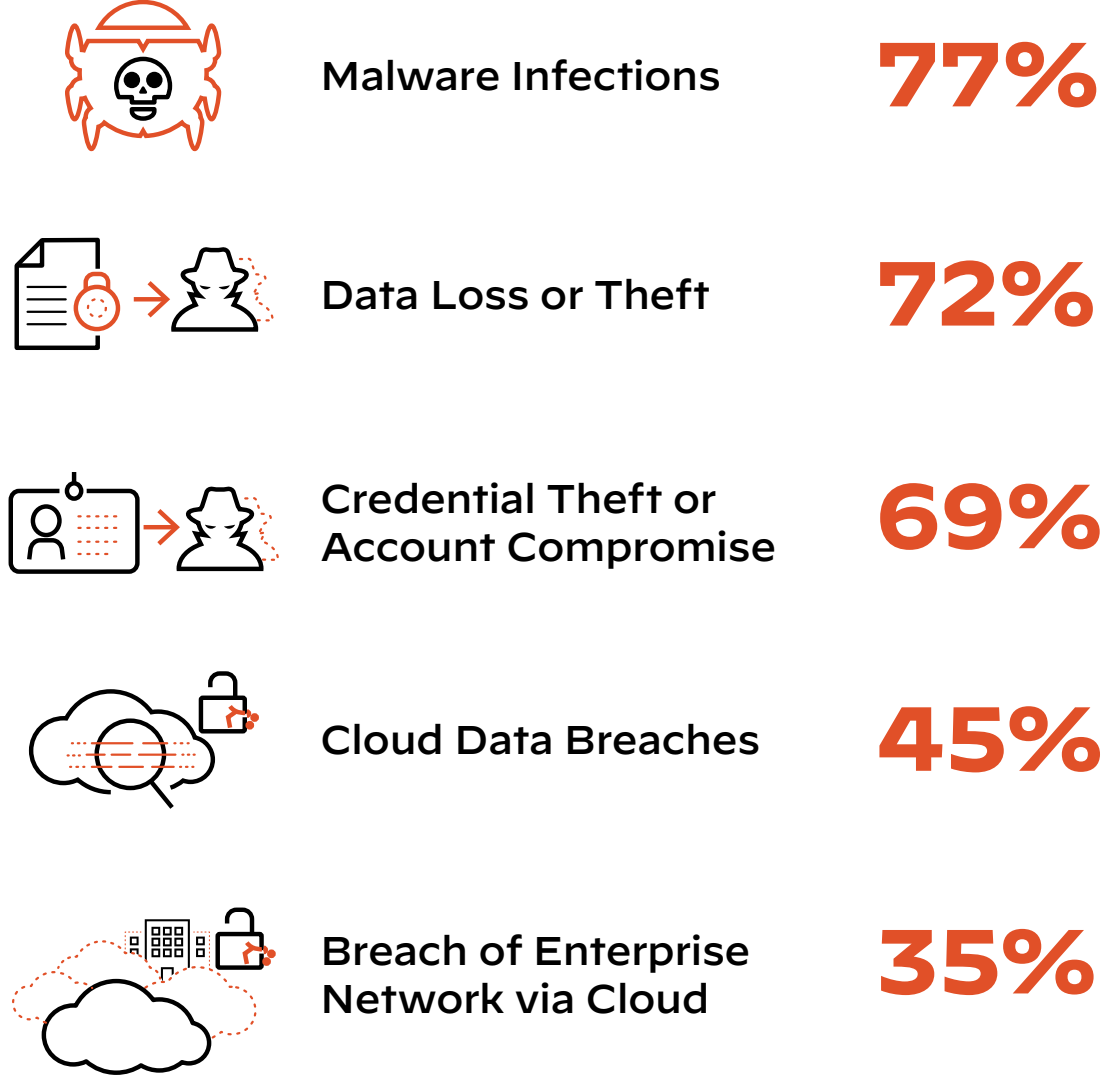
Negligent oversharing of data and malicious insiders, and IT's inability to monitor user behavior.



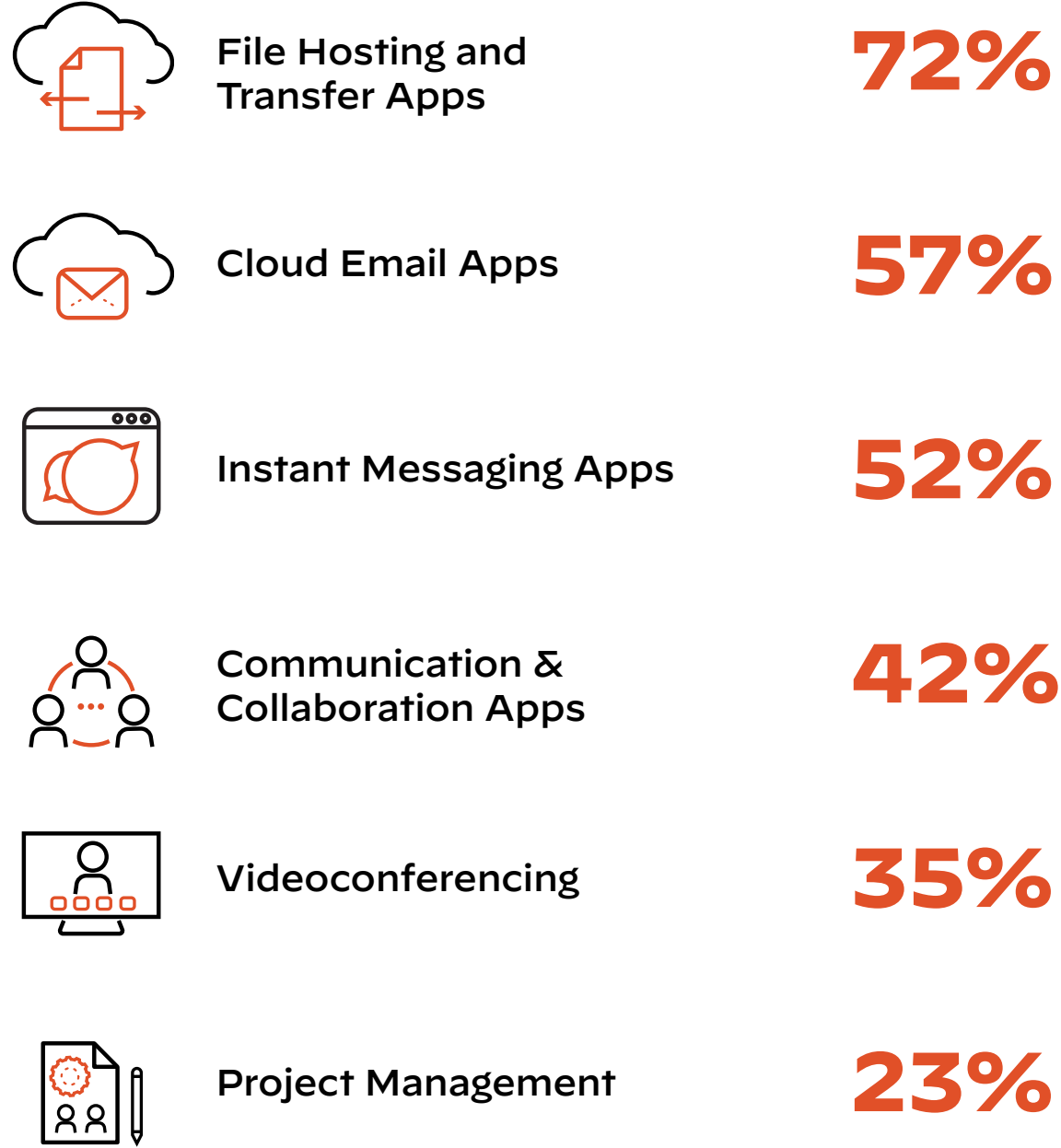
REGULATORY COMPLIANCE

IT's inability to extend regulatory compliance to their SaaS environments.

SaaS-Related Threats CISO's Are Most Concerned About



Most Concerning Types of SaaS from a Security Point of View



Sources:
 - Cybersecurity Insiders, The CISO Cloud SaaS Security Report, 2020

Limitations of Today's Conventional CASB Approaches

Their pitfalls eclipse their potential. An evolved approach to CASB is what enterprises need today to be in lockstep with the exponential growth of SaaS.

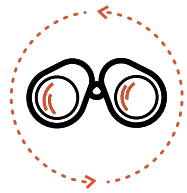
CASBs have undoubtedly become vital to enterprise security, when it comes to securing cloud-based applications and the sensitive data that flows through them. However, current first-generation CASB solutions present notable drawbacks that demand a departure from their inherent operating models.

- 1 Incomplete App Visibility:** First-generation CASBs focus on HTTP/S, missing over half of all traffic of non-web applications. They are still relying only on static databases of application signatures and reactive support requests for app discovery. This approach hinders their ability to identify or contain new SaaS apps before they become a risk. They also lack APIs to secure modern collaboration applications used by the distributed workforce.
- 2 Inadequate Data Protections:** Their data protection methodologies struggle to keep pace with the volume and sprawl of sensitive data. Their data loss prevention relies mainly on regex-based and traditional data fingerprinting methods, resulting in slow and inaccurate protection. Most importantly, they have not adapted to detect data leakage through modern collaboration apps like Slack, Teams, and Zoom, which use new ways of communicating with short and unstructured messages.
- 3 Poor Security:** Security, unfortunately, has always been only a checkbox in legacy CASB, with the majority of vendors providing very limited efficacy into high-priority threats, unknown malware, and breaches, most of the time by using third-party sandboxing tools as a threat detection method. Moreover, their inline proxy approach only gives visibility into HTTP/S—leaving customers only partially covered.
- 4 Inconsistent Coverage:** These siloed CASB solutions force organizations to apply different delivery methods and technology to cover HQ, branch, and remote workers, leaving huge consistency gaps in protection. Disjointed from the rest of the organization's security infrastructure, they also require network changes and a complex architecture to deploy, making it inefficient and cumbersome to manage across the hybrid workforce.

Now is the time to take a next-generation approach to CASB. One that is tied to the rest of your security deployment...and gives you the necessary visibility and control over all applications, users and data by keeping pace with the SaaS explosion in your enterprise.

5 Must-Haves to Look for in an Next-Gen CASB Solution

1



Your Next-Gen CASB Solution Must Support Cloud-Scale and Keep Pace with the Explosion of SaaS

Complete visibility into your SaaS environment is essential in determining the true state of your cloud and data security. When cloud-based solutions are used outside the purview of IT, your company's data is no longer under the influence and oversight of the company's governance and risk policies. A Next-Gen CASB solution should automatically see and secure all sanctioned and unsanctioned apps, including modern collaboration SaaS apps, to keep pace with the exponential growth of SaaS.

A Next-Gen CASB solution should be able to scan all traffic, ports, and protocols, automatically discover new apps, and leverage the largest set of APIs of SaaS apps, including APIs for modern collaboration apps like Slack® and Teams. It should provide accurate and customizable risk scores and risk attributes against all apps to monitor and prevent risky user activity—before the apps come into question and become carriers of threats. Comprehensive real-time SaaS visibility and risk scores will enable your IT teams to automatically keep up with SaaS growth, help ascertain granular risk-based controls of both known and previously unknown SaaS apps, and intelligently prevent them from becoming conduits of data loss.

Look for these capabilities to make sure your CASB solution supports cloud scale:

- ✓ Broadest security coverage for all SaaS apps, including the largest API-based security coverage to provide additional control for sanctioned SaaS applications.
- ✓ Continuous app discovery powered by an application ID-based cloud engine for shadow IT apps.
- ✓ Automated risk classification with 30+ attributes to help determine each organization's risk.
- ✓ Bulk tagging capabilities to help classify apps by adding their sanctioned status and customized tagging for detailed classification.
- ✓ Integrated inline controls and enforcement that can be deployed easily across all devices and users.

2

Your Next-Gen CASB Solution Must Be Simple to Deploy and Offer Lean Architecture

In highly-distributed modern enterprises with multiple sites and mobile users, the middleman approach of conventional CASB solutions becomes difficult to scale, costly and therefore, unsustainable. Standard CASBs are cumbersome to deploy because they add an unnecessary cloud gateway (typically a proxy) and require complex traffic redirection from log collectors like the network firewall and proxy auto-configuration (PAC) agents. On top of that, they need an active directory (AD) connector to enforce policies by user ID or the AD group. With multiple sites, this infrastructure has to be duplicated over and over again. Beyond that, due to users working from remote locations today, extra endpoints with PAC file installations or additional VPN agents to route remote user traffic through the cloud-based proxy are also required. While proxy architecture is a must for those who depend on it, it is a burden for everyone else to set up and definitely shouldn't be the only way.

A Next-Gen CASB solution should eliminate all the middleman components and unburden your IT teams from additional infrastructure investments. It should allow your IT security teams to simplify operations by leveraging SASE and CASB together in a unified platform for security, networking and data protection across all environments. Lastly, it should be capable of leveraging your existing Next-Generation Firewall investment for comprehensive and integrated SaaS security posturing and monitoring.

Look for these capabilities to make sure your CASB solution is simple and easy to deploy:

- ✓ 100% cloud managed solution with flexible deployment options to easily enable a hybrid workforce.
- ✓ Single dashboard for visibility applied throughout all cloud application policies.
- ✓ Simplified configuration using optimized workflows and ML-based automation.
- ✓ Automatic up-to-date Shadow IT visibility powered by native integrations.
- ✓ Out-of-the- box integration with data loss prevention, threat protection and inline controls for enforcement. No added PAC Files or proxies to complete deployment.

3

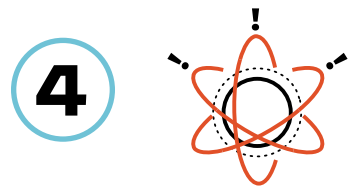


Your Next-Gen CASB Solution Must Detect Both Known and Unknown Threats Reliably & Proactively

The diverse nature of SaaS apps means a highly distributed environment where hundreds of apps “rain down” from different cloud provider environments to generate numerous points of compromise. Successful outcomes of your SaaS security posturing require actionable insights into detection and prevention of threats arising from your SaaS landscape. A Next-Gen CASB solution should be a proven solution that prevents zero-day threats with natively integrated inline ML models that don’t require you to rely on third-party tools. It should stop new and unknown threats instantly with evasion-resistant signatures, and then distribute updates globally within seconds, ensuring protection is distributed more quickly than the rate of infection. Going beyond traditional malware analysis, it should draw from a crowdsourced threat intelligence engine that leverages world’s largest datasets to quickly and easily stop threats with inline, real-time, zero-day protections. This new approach to threat prevention will ensure the most up-to-date security posture and defense against anomalous SaaS-based threats across your network—saving your IT teams valuable time and effort.

Look for these capabilities to make sure your CASB solution provide best-in-class threat prevention:

- ✓ Continuous malware and threat protection powered by a cloud-based malware analysis and prevention engine to help detect and prevent new unknown file-based threats.
- ✓ Incident remediation workflow with automated remediation.
- ✓ User activity monitoring and response.



Your CASB Solution Must Provide Comprehensive Data Protection and Compliance Using Highly Accurate Detection Techniques

Most CASB solutions offer basic security with regards to data protection and compliance that is only limited to cloud environments. While enterprise data loss prevention solutions deployed on premises rely on advanced techniques and superior capabilities, they create an unbalanced approach between on-prem and cloud. A Next-Gen CASB solution should provide data protection and compliance controls reliably, consistently and comprehensively throughout the entire enterprise, across clouds, on-premises networks—basically wherever your users and data reside. It should discover, classify, and protect all data stored within and transmitted across SaaS that is in-line and SaaS that is out-of-band via APIs to make sure policy violations, exposures, and regulatory compliance are properly addressed. Most importantly, a Next-Gen CASB also needs to adapt to new data models of modern collaboration apps like Slack and Teams and Zoom, where users communicate with short and unstructured messages and screen captures. Leveraging a powerful cloud detection engine, descriptive data profiles, exact data matching, image recognition, natural language processing, and AI models, it should accurately detect sensitive data, both structured and unstructured, both at rest and in motion.

Look for these capabilities to make sure your CASB solution offers comprehensive data protection and compliance:

- ✓ Enterprise data loss prevention for data at-rest and data in-motion including discovery of sensitive data in SaaS applications, data exposure detection through out-of-the-box EDM, OCR and Data Profiles, and prevention of data exfiltration.
- ✓ Data protection for mission-critical collaboration applications like Slack, Teams, Zoom, Jira and Confluence with the ability to automatically identify sensitive information in real-time within the context of unstructured users' conversations through deep learning, natural language processing, and AI models.
- ✓ Out-of-the-box reporting for compliance including a real-time GDPR report for data at-rest, an on-demand Risk assessment report for data at-rest and an on-demand SaaS Security report for Shadow IT applications.

5



Your CASB Solution Should Provide Integrated and Consistent Security Across All Locations

Detached from an enterprise's core infrastructure, CASBs are limited in their ability to provide consistent security controls across all environments—the cloud, on-premises, remote—and this limitation has a downstream effect on security teams who must synchronize risks, policies, and controls across multiple environments. A Next-Gen CASB solution should function as an “integrated” solution that securely enables a company's hybrid workforce across all locations—whether remote or in the office in addition to all the applications in use, and all data stored or transmitted through them. Circumventing the complexity of point products, such a solution would consistently protect data stored and in motion not only via cloud-based apps but also through the physical network. Being multimode, the reimagined CASB should secure both unsanctioned and sanctioned SaaS apps and secure all traffic—web and non-web—from a single unified cloud-delivered console. It should discover unsanctioned SaaS apps and manage risks while providing broad API-based security to connect and scan sanctioned apps running out of band in the cloud for at-rest detection, inspection, and remediation across all users, folders, and file activity.

Look for these capabilities to make sure your CASB solution is integrated and multimode:

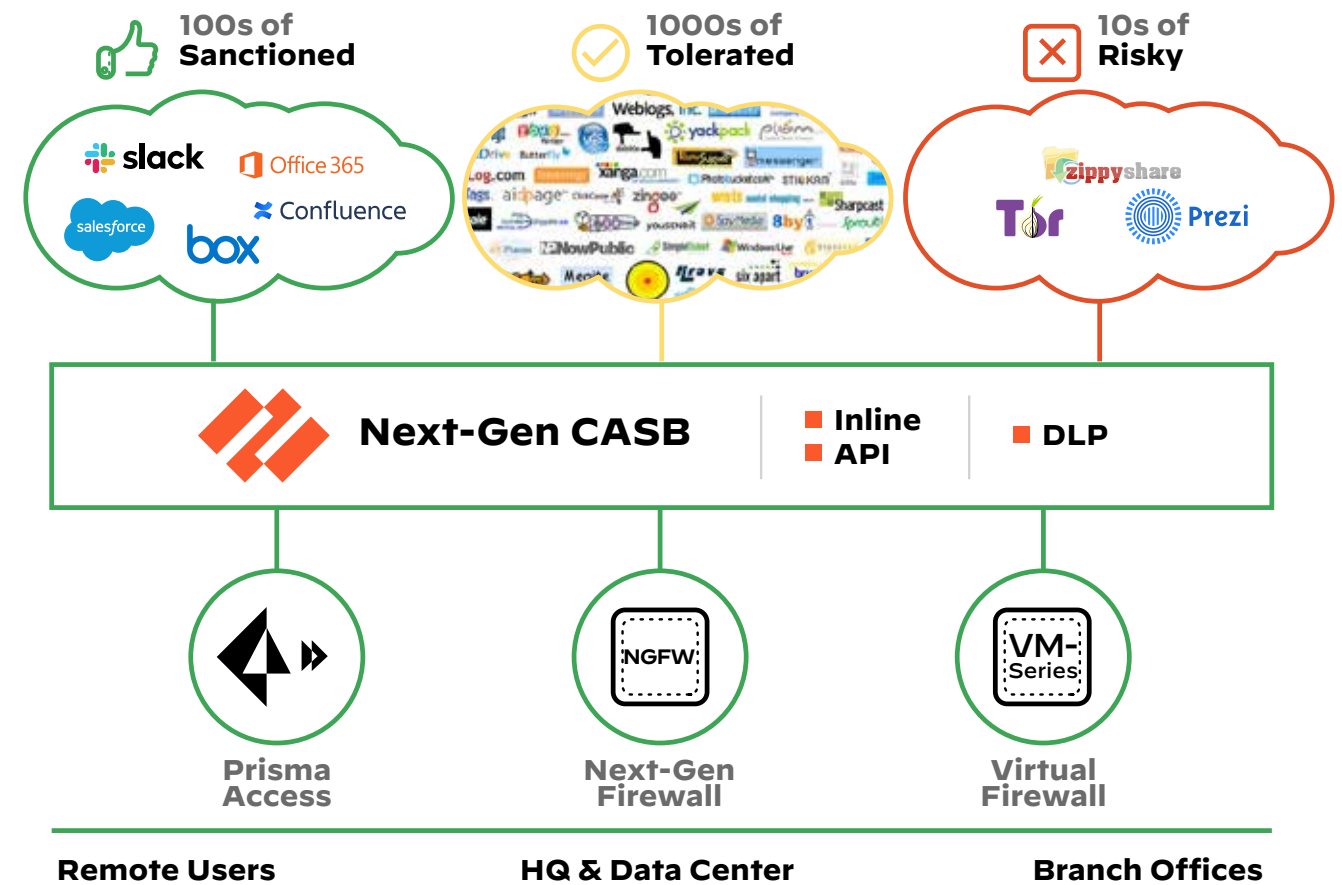
- ✓ Granular inline controls across all applications for all users and devices.
- ✓ Data security controls and compliance across all SaaS apps, networks and users, without any third-party tools.
- ✓ Threat prevention across all apps, networks and devices with WildFire, without any third-party tools.
- ✓ Reuses existing security infrastructure. No architectural changes, PAC files or additional VPN Agents required.

SaaS Security by Palo Alto Networks

The Next-Gen CASB that Keeps Pace With the SaaS Explosion

To safely embrace the cloud, companies need a single, consistent way to protect their users, applications and data across every corporate environment. Our SaaS Security takes on the challenge of keeping up with the **SaaS explosion** by automating discovery and protecting them while being embedded into existing architectures and workflows. This leads to a whole new level of ease, simplicity and efficiency for enterprises. Here's everything SaaS Security does for you!

- It is the only solution that lets you automatically discover and control new SaaS apps using our patented **App-ID technology** that leverages the power of our Palo Alto Networks global community and machine learning to continuously identify new SaaS applications, ensuring applications are discovered automatically as they become popular.
- Compared to proxy-based CASB, our Next-Gen CASB's lean architecture eliminates man-in-the-middle components, ensuring five times faster time to value because it can be up and running on our SASE and Next-Generation Firewall platforms within minutes. And what are the perks you get to enjoy from our Next-Gen CASB? Highest operational efficiency, lower total cost of ownership (TCO) and a jump in ROI.
- It prevents threats with zero delay with the intelligent network effect of thousands of global customers to deliver evasion-resistant signatures within seconds of discovery, SaaS Security helps prevent all threats, including zero-day, in real-time, without needing third-party security tools.

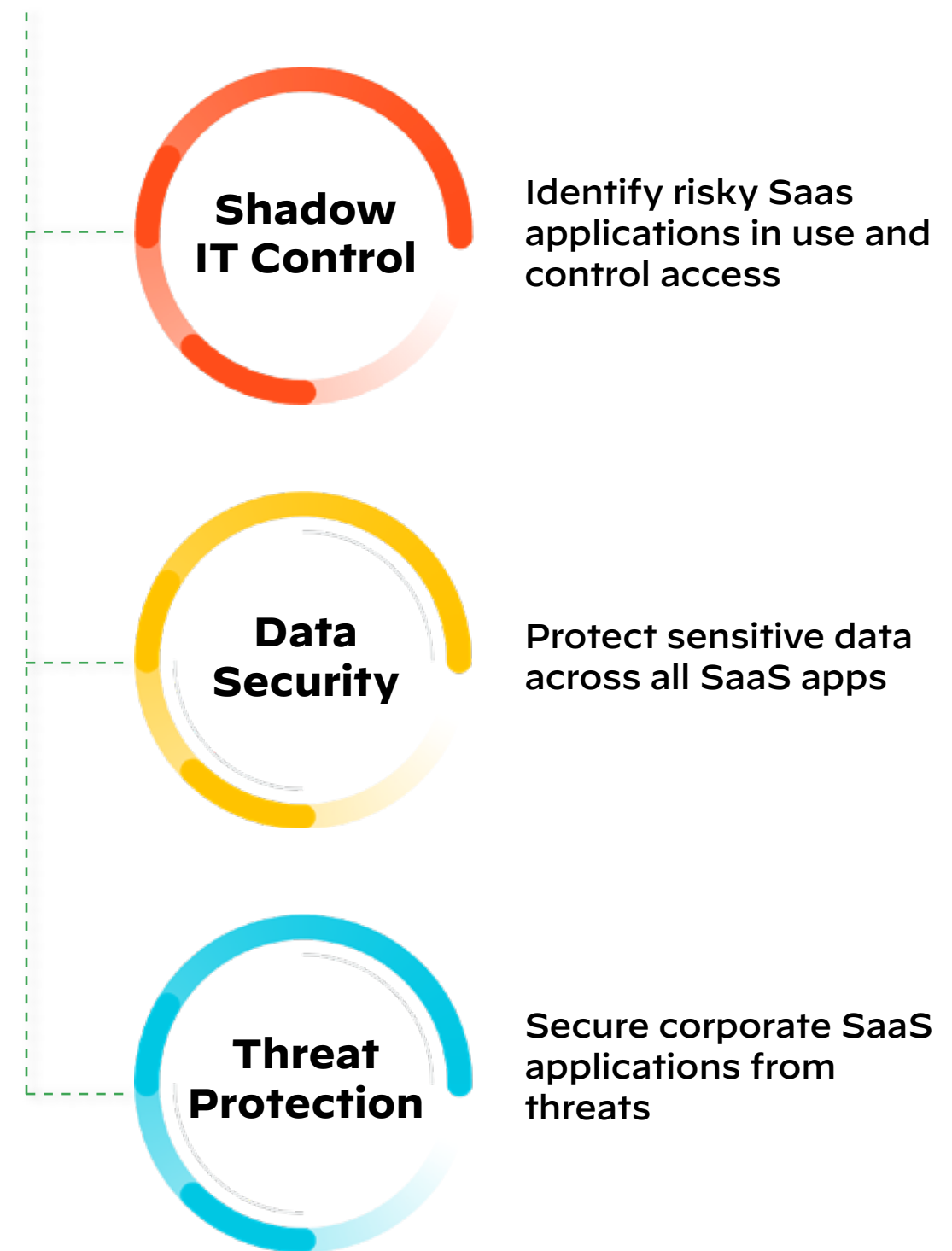


Palo Alto Networks Redefines CASB for The Modern Enterprise

- It uses the industry's most comprehensive cloud-delivered **Enterprise Data Loss Prevention** across all SaaS apps (both in-line and at-rest via out-of-band APIs), including modern collaboration apps, and comprehensively throughout the rest of the enterprise, across clouds, on-premises networks and remote users – basically wherever your users and data reside to provide data protection and consistent compliance controls.
- Through out-of-the-box compliance reports and by protecting SaaS apps consistently by applying **Enterprise DLP**, ML-powered threat prevention, and ongoing monitoring of user activity and administrative configurations, it helps you maintain necessary compliance with regulations such as PCI DSS, HIPAA and GDPR.
- Using cloud native implementation, it natively integrates with your network security infrastructure, forming an integral part of your comprehensive **SASE** platform or your **Next-Generation Firewall** and designed to see and protect all applications in use, both web and non-web, it offers enterprise data protection across all applications, networks, data and workloads as well as all users working from any location.

SaaS Security by Palo Alto Networks is our answer to the enterprise market's need for a disruptively simplistic approach to legacy CASB. **Our research shows taking this kind of a comprehensive yet uncomplicated approach results in a 45% reduction in breaches over three years!**

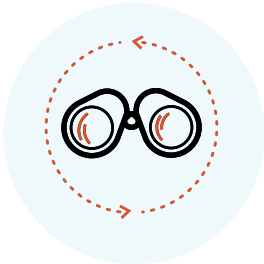
CASB



SaaS Security covers all CASB use cases

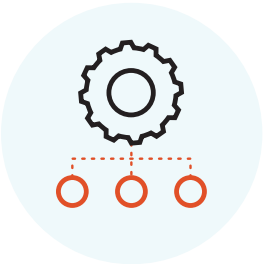
Your IT Team Deserves the Benefits of Integrated CASB

As your organization wrangles with its explosive SaaS adoption journey, consider our integrated CASB.



Your One-Stop Shop for Unprecedented SaaS Visibility and Control

- ✓ Automatic discovery and control of new apps with Cloud App-ID™ technology
- ✓ No middleman components, low TCO
- ✓ Broadest API-based security for sanctioned apps



Leaner Architecture with Easy Deployment Across form factors

- ✓ Secure Access Service Edge (SASE)
- ✓ Hardware Firewalls
- ✓ Software Firewalls

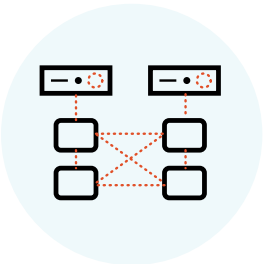


Delivers Accurate Data Loss Prevention and ML-Powered Threat Prevention

- ✓ Protect sensitive data across all SaaS apps and all locations where users and data reside
- ✓ Leverage descriptive identifiers, exact data matching, natural language processing and image recognition for highly accurate data detection
- ✓ Threat prevention via inline ML-models
- ✓ Zero-delay evasion-resistant threat detection signatures



Delivered as a Single, Unified Cloud-Delivered Console for inline + API + Enterprise DLP



Fully deployed on our Comprehensive SASE Platform or Next-Generation Firewalls



Maintain Compliance with Regulations such as PCI DSS, HIPAA and GDPR by Protecting SaaS Apps

Think Integrated CASB. Think Palo Alto Networks.

At Palo Alto Networks our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We are at the forefront of protecting tens of thousands of organizations across clouds, networks, and devices and help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration.

Founded in 2005, Palo Alto Networks is based in Santa Clara, California, and serves customers globally with offices worldwide. For more information, visit:

For more information, visit: www.paloaltonetworks.com

See What Our Customer
Had to Say:

“ We are convinced that Palo Alto Networks will accompany us into the future. Palo Alto Networks has a clear vision of the security required by SaaS environments, which covers all critical aspects of this type of deployment. ”

– Juan Carlos Alzate Garcia,
Vice President of Technology



Ready to Dive Deep?

Watch the SaaS Security
Product Demo!

Read the Case Study



www.paloaltonetworks.com

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

© 2021 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks>. All other marks mentioned herein may be trademarks of their respective companies.