SaaS Security

The Industry's Only Next-Generation CASB That Keeps Pace with the SaaS Explosion

Today, the emergence of the hybrid workforce—where employees can work fluidly between corporate offices, branch offices, home, and on the road—has accelerated the change in how and where business is done. To adapt to this change, every organization has embraced the convenience of software-as-a-service (SaaS) cloud applications, such as Microsoft 365, Google Workspace, and Salesforce, to bolster the productivity of their hybrid workforces. Meanwhile, Gartner forecasts that the worldwide public cloud services market will grow by 19% in 2022, and SaaS remains the largest market segment, forecast to grow to $140 billion by the same year.[1]

Main Business Benefits

- See and secure applications automatically to keep pace with the SaaS explosion, including modern collaboration apps.
- Eliminate the risk of compromise and data loss due to misconfigured security settings with SSPM.
- Accurately protect sensitive data in real time with the industry's most comprehensive cloud enterprise DLP, powered by ML.
- Stop known/unknown threats, and detect compromised accounts and malicious insider activity, leveraging the first ML-powered malware prevention and latest behavior analytics.
- Simply and consistently protect all users everywhere with centralized control that brings SASE and CASB together through a single console.

1. "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.3% in 2020," Gartner, July 23, 2020, https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020.

Particularly, organizations have become increasingly dependent on a host of mission-critical collaboration applications like Slack, Microsoft Teams, Zoom, Jira, and Confluence. Today, these collaboration apps are driving business agility because they keep employees connected anywhere they are—all day, every day. These apps have created a fundamentally different way of conducting business though, as messages are now shorter and more frequent; people use fewer file attachments and more screenshots, and a conversation is made of multiple posts between two or more users.

If they are not properly secured, SaaS applications can be harmful and create new risks. As sensitive data is increasingly uploaded, created, shared, and exposed across multiple sanctioned applications, it becomes more vulnerable to loss and theft. Such confidential information is also more unstructured than ever, and increasingly difficult to protect, making data breach prevention, compliance, and data privacy very difficult tasks.

In addition, cloud-based threats have increased in volume and sophistication, using advanced techniques to bypass standard defense methods, affecting sensitive data and users.

Aside from corporate-sanctioned applications, there are countless public SaaS applications, exponentially growing in number, that employees can access without the knowledge of the IT department. Lack of visibility into SaaS usage prevents the IT department from having control over the employees' use and abuse of unsanctioned SaaS applications, which can introduce serious risks to the organization, such as data leakage and noncompliance.

In our work-anywhere world, all sanctioned and unsanctioned SaaS applications remain accessible when employees choose to bypass VPN backhauling systems, preventing IT departments from having the necessary visibility or control over the extent of their use by employees.

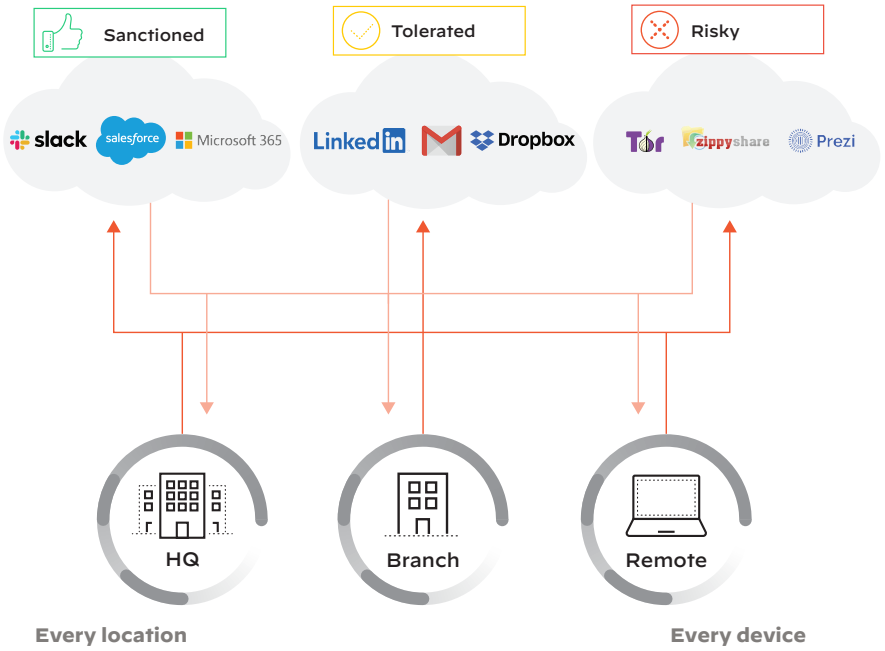

Figure 1: Hybrid work and hypergrowth of SaaS applications

What IT Security Teams Need Today

IT security teams are challenged with securing more and more sanctioned and unsanctioned SaaS applications, protecting sensitive data in the cloud, and maintaining compliance consistently across different cloud environments. At the same time, they must also block ever-evolving threats to their sensitive information, users, and resources. Today, they need a SaaS security solution that:

- Provides visibility and control over all the SaaS apps in use, and their shadow IT risks, and can intelligently keep up with the unstoppable SaaS growth.
- Reliably protects sensitive data and ensures compliance across all SaaS apps, including modern collaboration apps like Slack, Teams, Zoom, Jira, and Confluence.

- Continuously monitors critical security settings, alerts them when a misconfiguration gets detected, and provides guided remediation to fix the issue.
- Secures corporate SaaS apps from known, unknown, and zero-day threats, and detects compromised accounts and malicious insiders that target sensitive data and users.
- Protects all users everywhere, with an architecture that doesn't add unnecessary complexity and cost, and is tied to the existing network security deployment as a comprehensive enterprise platform.

To safely adopt the cloud, companies need a single, consistent way to protect all their applications, data, and users from all threats.

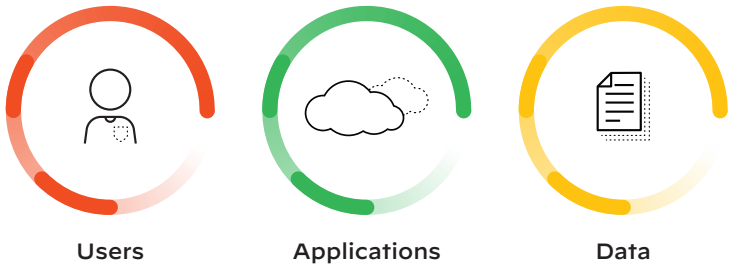

Figure 2: What your SaaS security offering must protect

Limitations of Today's Conventional CASB Approaches

When it comes to securing cloud-based applications and the sensitive data that flows through them, security teams have typically turned to cloud access security brokers (CASBs). However, current first-generation CASB solutions are inadequate due to numerous architectural and operational inefficiencies. Organizations often need to deploy several tools to try to get holistic defense, increasing operational complexity and reducing security efficacy. Moreover, the capabilities of these legacy CASB solutions only partially address today's business needs, leaving organizations exposed and vulnerable due to several critical limitations.

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.

Overlook the Impact of Misconfigurations

Conventional CASB solutions have focused on data security and have overlooked the impact that a misconfigured security setting can have. As SaaS apps become more complex and abundant within enterprises, security teams are struggling to keep up. Each app requires in-depth research to understand the ideal configurations that emphasize security, and with hundreds of sanctioned SaaS applications, these app audits quickly become outdated if somebody changes a configuration.

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.

Poor Security

Security, unfortunately, has always been only a checkbox in legacy CASB, with the majority of vendors providing limited efficacy on 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.

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.

Solution: Contain the SaaS Explosion with Next-Generation CASB

Palo Alto Networks elevates the state of cloud-delivered SaaS security with the industry's only Next-Generation CASB that automatically keeps pace with the explosive SaaS growth with proactive visibility, real-time data protection and best-in-class security. Delivered via Prisma Access and the entire Palo Alto Networks Next-Generation Firewall platform (cloud-based, virtual, and hardware form factors), it provides simple and flexible deployment and helps organizations enable the safe adoption of SaaS applications.

Key Components and Capabilities

The sections that follow cover the core components and capabilities of Next-Generation CASB.

See and Secure All Applications Automatically

Automatically discover and prevent risks for thousands of new SaaS applications before they become problems. The solution scans all traffic, ports, and protocols in addition to HTTP/S, including Tor, FTP, and PrivateVPN, to detect all types of applications. Its App-ID technology leverages the power of the broad global community and machine learning models to automatically provide continuous identification, categorization, and granular risk-based control of known and previously unknown SaaS applications, ensuring new applications are discovered automatically as they become popular. The SaaS Security catalog delivers granular visibility into applications, their usage within the organization, and their risks.

There are more than 10 descriptive attributes and more than 30 compliance-related attributes in addition to users' information and their activities (e.g., uploads, downloads, sessions). Applications are classified across more than 400 different categories in the catalog. Default risk scores can also be customized based on the risk attributes that matter most to your organization. Risk mitigation controls and policy recommendations can be automated for existing and future applications, eliminating time-consuming manual policy definitions.

Enforce Proper Configurations with SaaS Security Posture Management

SaaS Security Posture Management (SSPM) helps identify and remediate misconfigurations in sanctioned SaaS applications, preventing data loss and reducing the risk of security breaches. Going beyond CIS and NIST compliance checks, our solution provides comprehensive security with the industry's first Posture Security Policy Engine, aligning thousands of app-specific configurations to a common security framework that security teams can easily understand and manage. With continuous monitoring and analysis of SaaS applications, risk of data loss due to human misconfigurations is eliminated. Remediation time is reduced by allowing users to fix misconfigurations with a single click, and configuration drift is avoided by locking critical security settings in place.

Accurately Protect Sensitive Data with Enterprise Data Loss Prevention

Achieve unparalleled protection of all sensitive data with more automated detection engines, more control points, and content-aware technologies. The solution provides data protection and compliance controls consistently across all SaaS applications, and comprehensively throughout the enterprise across clouds, on-premises networks, and users, with the industry's first cloud-delivered enterprise DLP. Palo Alto Networks Enterprise DLP is based on a single cloud engine to deliver unified policies for sensitive data everywhere, both at rest and in transit. It scans, classifies, and protects all data stored within SaaS applications while it's in motion to make sure policy violations, exposures, and regulatory compliance are properly addressed.

Enterprise DLP ensures the highest levels of accuracy. It automatically detects sensitive content via ML-based data classification and an extensive number of described data identifiers using regular expressions or keywords (e.g., credit card or ID numbers, financial records, GDPR, other data privacy- and compliance-related information) and applies customizable data profiles and Boolean logic to scan for collective types of data. The type of exposure (e.g., public or internal), confidence levels, and precise context criteria (e.g., number of occurrences and pattern logic) reduce incidents and inaccurate detection. Exact data matching (EDM) is an advanced data fingerprinting method to detect specific sensitive data and protect it from malicious exfiltration or loss.

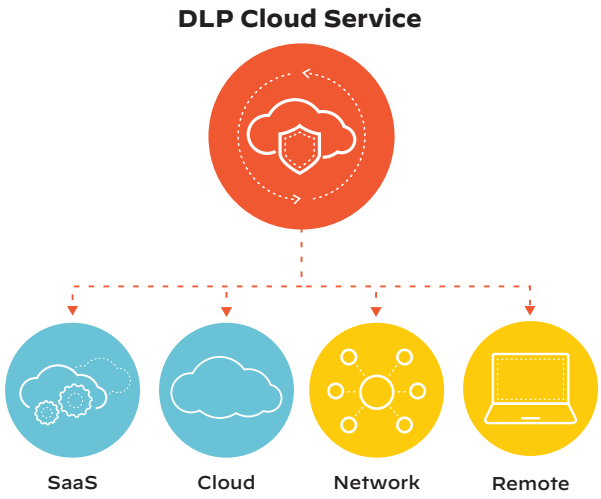

Figure 3: Palo Alto Networks Enterprise DLP

Most importantly, the solution is able to automatically identify sensitive information even within the context of unstructured users' conversations on collaboration apps like Slack, thanks to deep learning, natural language processing (NLP), AI models, and advanced optical character recognition (OCR), ensuring high accuracy and fewer false positives. Automated incident workflows with policy-based response actions include user alerts and auto-remediation. Detection of flexible document properties, such as third-party data tagging, augments the identification of sensitive data.

SaaS Security also includes file blocking profiles that can be used to prevent files from being downloaded, which is an important part of a cloud data protection strategy.

API-Based Protection

Using an out-of-band, API-based approach, Next-Generation CASB connects directly to the industry's largest number of sanctioned SaaS applications, including the most popular cloud collaboration apps like Slack, Teams, Jira, and Confluence. SaaS Security protects all these SaaS applications consistently by applying Enterprise DLP, ML-powered threat prevention, and ongoing monitoring of user activity and administrative configurations. This deployment model works across any access point regardless of the user's location or device. It preserves the user experience with corporate SaaS applications because it's nonintrusive and doesn't interfere with standard business processes.

Enterprise DLP and ML-powered threat prevention are consistent across all SaaS applications and with your entire enterprise. These capabilities help accurately protect all sensitive data stored in cloud applications, maintain compliance with regulations such as PCI DSS and GDPR, and stop all unknown and known threats in real time, without requiring third-party security tools.

Adaptive access control lets you granularly manage access to SaaS applications as well as define acceptable use policy. Clientless capabilities are also supported to secure access from unmanaged devices accessing SaaS applications. Finally, the solution can detect and report on anomalous user activities that may be associated with stolen credentials or malicious insider behavior, such as bulk data downloads or large data sharing, using our advanced behavior analytics.

Comprehensive Inline Security

The solution protects all SaaS applications and secures all traffic—web and non-web, leveraging the industry's first ML-powered malware prevention. With more than 15 years of innovation in threat analysis as well as the world's largest datasets, Palo Alto Networks enables customers to quickly and easily stop threats with real-time, zero-day protections. SaaS Security extends the NGFW security services to SaaS applications inline and via API with deep application visibility, segmentation, secure access, and threat prevention. Trained by the largest datasets, the solution delivers signatures in under 10 seconds, resulting in a 99.5% reduction in systems infected. These comprehensive capabilities span the on-premises and mobile workforce to stop threats across all applications, resulting in a 45% breach reduction over three years.[2]

Unified Cloud Console and Fastest Time to Value via an Integrated Architecture

SaaS Security is natively integrated with Prisma Access and the entire Palo Alto Networks NGFW platform in multiple form factors (physical, virtualized, and cloud-delivered) for deployment flexibility, consistently protecting all applications, all data, and all types of workloads as well as all users working from any location with any device. This comprehensive approach substantially simplifies the CASB deployment and its ongoing operations. Centralized control brings SASE and CASB together in a single unified, cloud-delivered console to

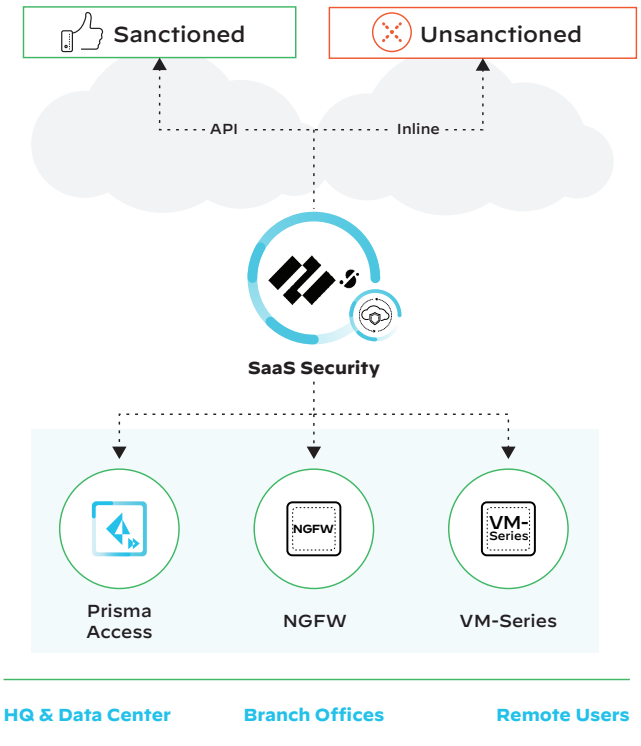

Figure 4: Consistent user experiences with better security and visibility

2. "The Total Economic Impact™ of Palo Alto Networks for Network Security and SD-WAN," Forrester, February 2021, https://start.paloaltonetworks.com/2021-forrester-tei-report-network-security.html.

easily and consistently extend best-in-class protection across the hybrid, local, and remote workforce. SaaS Security ensures the fastest time to value and the most easily deployed enterprise SaaS security solution, compared to legacy CASB, because it eliminates the man in the middle and is up and running in minutes. This results in a 247% return on investment (ROI) for a typical enterprise using our firewall platform,[3] along with high operational efficiency, five times faster CASB deployment, and 30% lower TCO compared to a traditional CASB because it's based on a much leaner architecture.

CASB and Enterprise DLP: Key Enablers for SASE

Traditional hub-and-spoke architectures with disparate network and security stacks don't scale for hybrid work and cloud. Palo Alto Networks Prisma SASE brings together best-of-breed security and next-generation SD-WAN into a cloud-delivered platform that consistently secures all apps used by your hybrid workforce, regardless of whether users are remote, mobile, or working from a branch office.

As core elements of Palo Alto Networks SASE, SaaS Security, and Enterprise DLP play a key role in enabling organizations to consistently protect their data, applications, and users across networks and clouds while avoiding the complexity of multiple point products, significantly simplifying adoption and saving resources—technical, human, and financial.

Our comprehensive SASE solution consolidates multiple point products, including ZTNA 2.0, Cloud SWG, Next-Gen CASB, FWaaS, and SD-WAN, into a single integrated service, reducing network and security complexity while increasing organizational agility, assisting you through your cloud and network transformation while helping you safely adopt SaaS applications.

Building on Zero Trust with SaaS Security

Implementation of an effective Zero Trust security strategy for cloud-enabled enterprises has to take into account a least-privileged access strategy for SaaS applications and their sensitive data. Palo Alto Networks SaaS Security is a fundamental part of the Palo Alto Networks Zero Trust architecture, allowing organizations to consistently secure access to SaaS applications and data across a highly distributed environment, including employees working from remote locations with their bring-your-own devices.

Table 1: Features and Capabilities Highlights

• Unified management across inline, API, and DLP • Directly integrated with NGFW platform; no need for proxy • Integrated with WildFire, the industry's leading cloud-based malware prevention solution • Visibility and risk control over thousands of SaaS apps • SSPM with continuous monitoring and guided remediation	• Customizable risk scores with 40+ attributes • User activity and data exposure monitoring • Multimode: inline and API controls • Unmanaged device access control • Out-of-the-box compliance reports (e.g., GDPR) • Custom tagging

Table 2: Privacy and Licensing

Trust and Privacy	Licensing and Support Requirements
Palo Alto Networks has strict privacy and security controls in place to prevent unauthorized access to sensitive or personally identifiable information. We apply industry-standard best practices for security and confidentiality. You can find further information in our privacy datasheets.	• SaaS Security includes SaaS Inline Security, SaaS API Security, and DLP, which are individually licensed • NGFW (hardware/virtual) or Prisma Access 3.0+ • Cortex Data Lake • PAN-OS 8.1.x+ (10.1 for ACE and policy recommendations)

3. Forrester Total Economic Impact study.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

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

www.paloaltonetworks.com