SaaS Security

The First Integrated CASB That Keeps Pace with the SaaS Explosion

Business Benefits

- Automatically discover and control new applications to keep pace with the SaaS explosion.
- Ensure data protection and compliance across all SaaS applications with the industry's first cloud-delivered enterprise DLP.
- Prevent zero-day threats in real time with natively integrated, ML-based attack prevention without third-party security tools.
- Leverage easy-to-deploy enterprise SaaS security with the lowest TCO compared to legacy CASB solutions.

For years, companies have tried to keep all their applications, data, and devices confined in managed environments where they have visibility and control over their risks.

Today, every organization is embracing the convenience of the cloud, migrating applications and data from their in-house data centers to software-as-a-service (SaaS) applications, such as Microsoft 365®, Google Workspace™, Slack®, and Salesforce®. Enterprises use 288 different SaaS apps on average across their business, with a year-over-year upward trend of 30%.[1] 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.[2]

1. "Blissfully's 2020 SaaS Trends," Blissfully, October 23, 2019, https://www.blissfully.com/saas-trends/2020-annual-report.
2. "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.

As sensitive data is increasingly uploaded, created, shared, and exposed across multiple sanctioned applications, it becomes more vulnerable to loss and theft. If they are not properly secured, sanctioned SaaS applications can be harmful when it comes to creating new risks. In addition, cloud-based threats have increased in volume and sophistication, using advanced techniques to bypass standard defense methods, affecting sensitive data and users.

Besides corporate sanctioned applications, there are countless public SaaS applications available 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.

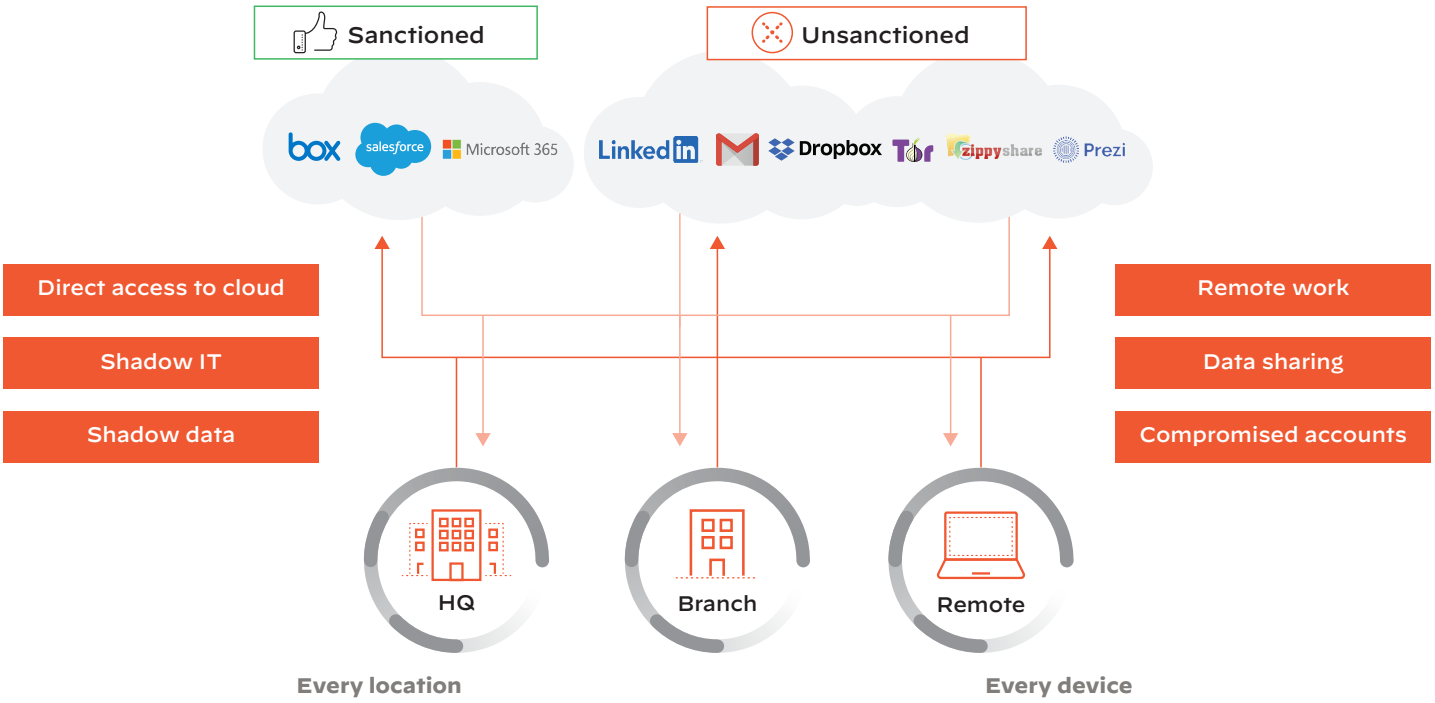

Figure 1: Cloud adoption and hyper growth of SaaS applications

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 shadow IT risks and can intelligently keep up with the unstoppable SaaS growth.
- Secures corporate SaaS apps from all known and unknown cloud threats.
- Reliably protects sensitive data and ensures compliance across all SaaS apps.
- Allows access to corporate SaaS apps only for legitimate users.
- Is simple to deploy and doesn't add unnecessary complexity and costs.
- Is tied to the overall existing network security deployment as a comprehensive enterprise platform.

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

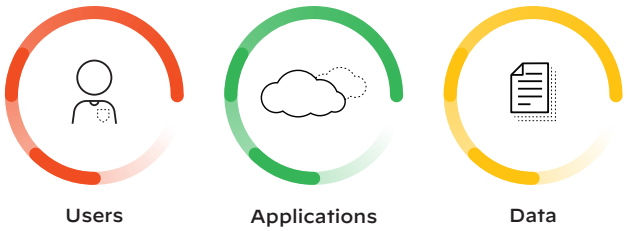

Figure 2: What your SaaS security offering must protect

Limitations of Today's Conventional Approaches

Today's conventional point controls, such as traditional cloud access security brokers (CASB), secure web gateways (SWG), and built-in SaaS security capabilities, are broken due to numerous architectural and operational limitations. Because these solutions only solve part of the problem, organizations often need to deploy several tools to try to get holistic defense.

Security teams patch these tools together, increasing operational complexity and reducing security efficacy. Moreover, piecing together information from disparate, individual tools that don't share data natively only provides part of the benefits. Ultimately this model is more time-consuming and hinders any security team's ability to keep pace with overexposure of data and defend against attackers.

Reactive Shadow IT Discovery

Legacy solutions rely on a signature-based approach for SaaS discovery via application libraries that are often populated out of context. In fact, they require security analysts to manually come up with SaaS application signatures in retrospect, rather than leveraging a global community to inform a proactive mechanism that will uncover emerging application risks before they become real problems.

Piecemeal Security

CASBs and a few SaaS providers offer basic security capabilities that are limited in breadth and depth. Their data protection implementation, for example, is not enterprise-grade and is limited to cloud environments only. Such solutions are also not designed to detect the endless variants of threats that adversaries are constantly creating to evade security systems. Embedded security capabilities offered by SaaS and cloud service providers don't secure multiple cloud environments.

Operational Complexity and High TCO

Legacy SaaS solutions like traditional CASB are standalone and disjointed from the security infrastructure. They are also quite difficult to deploy and manage because they are proxy-based and require complex traffic redirection from the network firewall and proxy auto-configuration (PAC) agents. Most importantly, these solutions don't provide a unified data protection policy approach together with the on-premises channels.

Solution: Palo Alto Networks SaaS Security

Palo Alto Networks SaaS Security is the first integrated CASB that keeps pace with the SaaS explosion. Natively integrated with the Palo Alto Networks Next-Generation Firewall platform (cloud-based, virtual, and hardware form factors), it delivers proactive visibility, best-in-class protection, and the fastest time to value for all SaaS applications, along with simple deployment and low total cost of ownership (TCO).

Key Components and Capabilities

Shadow IT Visibility and Control

Automatically discover and prevent risks for thousands of new SaaS applications before they become a problem. App-ID™ technology leverages the power of the broad global community to 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 your 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.

Comprehensive Inline Security

Protect all SaaS applications and secures all traffic—web and non-web. SaaS Security extends the NGFW security services to SaaS applications inline and via API with deep application visibility, segmentation, secure access, and threat prevention. Industry-first inline machine learning (ML) models run on the ML-Powered NGFW, trained by the largest datasets, deliver 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.[3]

Enterprise Data Protection

Provide 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 for accurate detection and consistent policy for sensitive data both at rest and in transit. It scans, classifies, and protects all data stored within SaaS applications and while it's in motion to make sure policy violations, exposures, and regulatory compliance are properly addressed.

Enterprise DLP automatically detects sensitive content via ML-based data classification and hundreds of data patterns 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. 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. Advanced ML simplifies data classification. Detection of flexible document properties, such as third-party data tagging, augments the identification of sensitive data.

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

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.

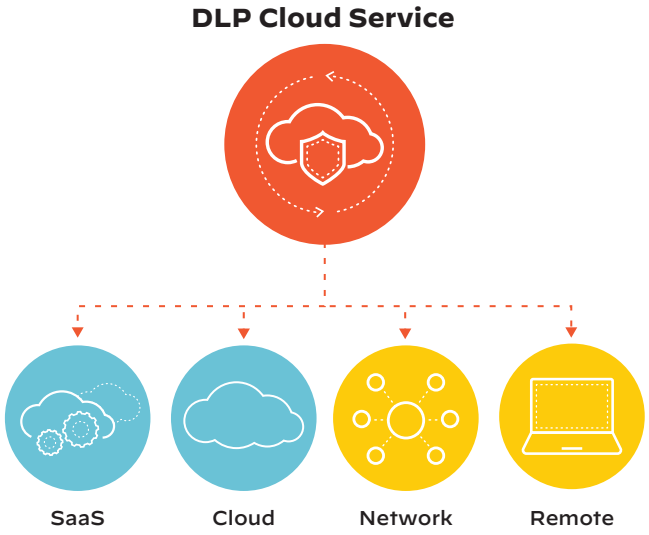

Figure 3: Palo Alto Networks Enterprise DLP

API-Based Protection

Connect directly to sanctioned SaaS applications, using an out-of-band, API-based approach. 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 mode 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 throughout 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.

Fastest Time to Value at Low TCO via an Integrated Architecture

SaaS Security is integrated with the Palo Alto Networks NGFWs in multiple form factors (cloud-delivered, physical, and virtual) to consistently protect all applications, devices, data, and types of workloads as well as all users working from any location. This comprehensive approach substantially simplifies the CASB deployment and its ongoing operations.

SaaS Security ensures the fastest time to value and the most easily deployed enterprise SaaS Security solution, compared to legacy proxy-based CASB, because it eliminates the man in the middle and is up and running in minutes. This results in 247% return on investment (ROI) for a typical enterprise using our firewall platform,[4] along with high operational efficiency, five times faster CASB deployment, and up to 50% lower TCO compared to a traditional CASB because it's based on a much leaner architecture.

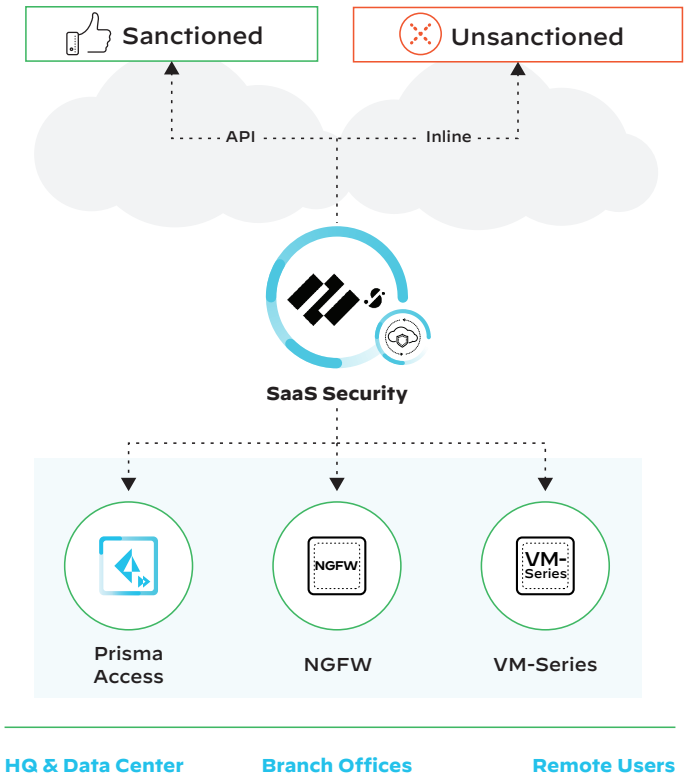

Figure 4: Example SaaS Security deployment

4. "Total Economic Impact," Forrester.

CASB and Enterprise DLP: Key Enablers for SASE

As key elements of the Palo Alto Networks secure access service edge (SASE) solution, 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 brings together networking and network security services in a single cloud-based platform to safeguard against risks to data, applications, and users; assist you through your cloud and network transformation; and help you safely adopt SaaS applications.

Building on Zero Trust with SaaS Security

Implementation of an effective Zero Trust security model 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 and their BYO 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 analysis solution
- Visibility and risk control over thousands of SaaS apps
- 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 • Cortex Data Lake • PAN-OS 8.1.x+ (10.1 for ACE and policy recommendation)

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