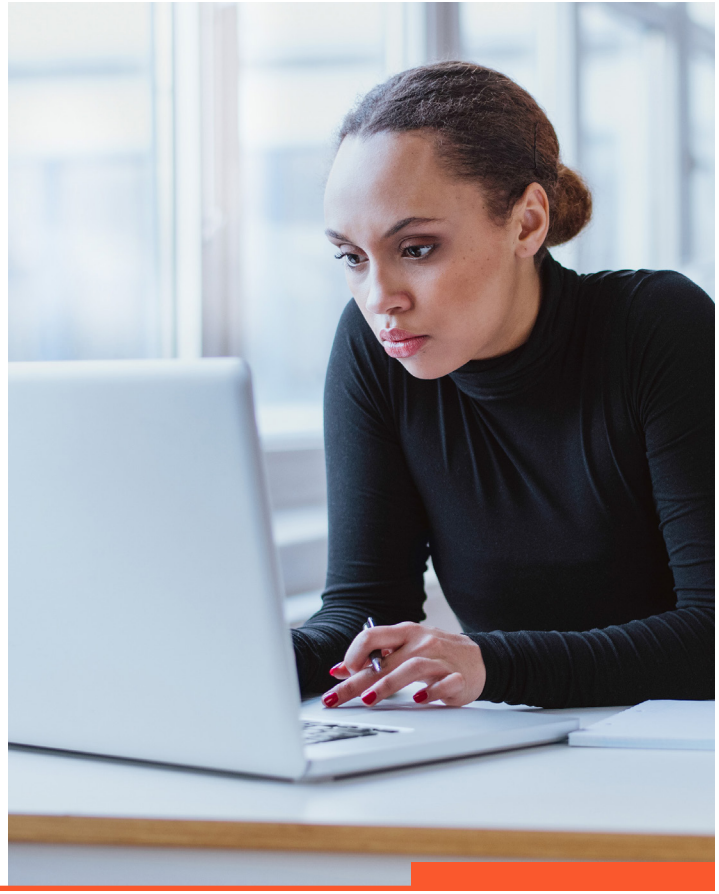
Navigating the SaaS Security Jungle

With the Only Next-Generation CASB That Automatically Keeps Pace with the SaaS Explosion



paloalto NETWORKS

Table of Contents

Introduction

The emergence of the hybrid workforce—where employees can now work fluidly between corporate offices, branch offices, home offices or on the road—has dramatically changed how and where business is done. To adapt to this new environment, businesses have increased their appetite for software as a service (SaaS) to bolster productivity and increase agility. Now employers and employees have become increasingly dependent on a host of mission-critical collaboration applications, like Slack, Teams, Zoom, Jira, and Confluence.

While there are tremendous advantages to adopting and using the cloud, the explosive growth in volume and types of SaaS apps now in use as well as the reliance on modern collaboration tools pose significant security risks to companies, such as:

- **Shadow IT:** Employees can directly access myriad SaaS applications without having to go through their company's network—often without the IT department knowing—leading to a lack of visibility into, or control over, application usage and risk.
- **Expanded network perimeter:** In a cloud environment, a company no longer has a single network perimeter to protect, as company data, applications, and users have expanded beyond the corporate premises.
- **Data is increasingly shared through the web:** Companies have and use massive amounts of data, ranging from highly confidential and sensitive to mundane, and this data is now literally everywhere—in SaaS applications, in the public cloud, in the data center, and on users' devices.
- **Shared security and compliance responsibilities:** In the cloud, the customer and the cloud providers share responsibility for specific aspects of security and compliance, meaning companies can't rely on service providers to take care of all their compliance needs in these areas.

As a result of all this, companies are losing visibility into and control over their networks, including users' web activities, what resources users are accessing, where and how sensitive data is protected, and their overall corporate security.

This e-book provides an overview of the challenges companies face when moving to the cloud and offers best practices that can help companies better protect and secure their applications, data, and users.

The Challenges Companies Face in Adopting SaaS Applications

SaaS application adoption and usage have exploded in response to the massive shift to hybrid work. Location changes have also changed how employees communicate with colleagues and customers, giving rise to a host of new collaboration tools. And these trends show no sign of slowing down.

Gartner estimates public cloud services are forecast to grow 18.4% in 2021 to total $304.9 billion, up from $257.5 billion in 2020. It further forecasts $168 billion in global spending on SaaS in 2022, representing a 19% YoY growth.[1]

However, while SaaS adoption and use are exploding, most companies are struggling to contain the sprawl of SaaS applications throughout their enthronements with confidence because:

- Companies have to deal with a mix of sanctioned (company approved), tolerated (not ideal, but allowed), and unsanctioned (unauthorized/shadow IT) SaaS applications that employees use for both business and personal reasons.
- Companies are storing and using more data than ever in the cloud, including highly sensitive business and customer data. It's very difficult to protect so much data when it leaves the network and moves across multiple cloud applications and users.

Shadow IT and data protection are the top cloud security challenges organizations face today, according to research by ESG. Specifically, employees signing up for cloud applications and services without the approval and governance of IT departments (35%) and discovering and classifying personally identifiable information to address data privacy concerns and comply with regulatory requirements (30%) are among the main security concerns.[2]

1. "Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021," Gartner November 17, 2020. https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021.
2. "ESG Master Survey Results: Trends in Data Security," ESG, January 28, 2019, https://www.esg-global.com/research/esg-master-survey-results-trends-in-cloud-data-security.

Cloud has no boundaries

- Direct access to cloud
- Shadow IT
- External data sharing

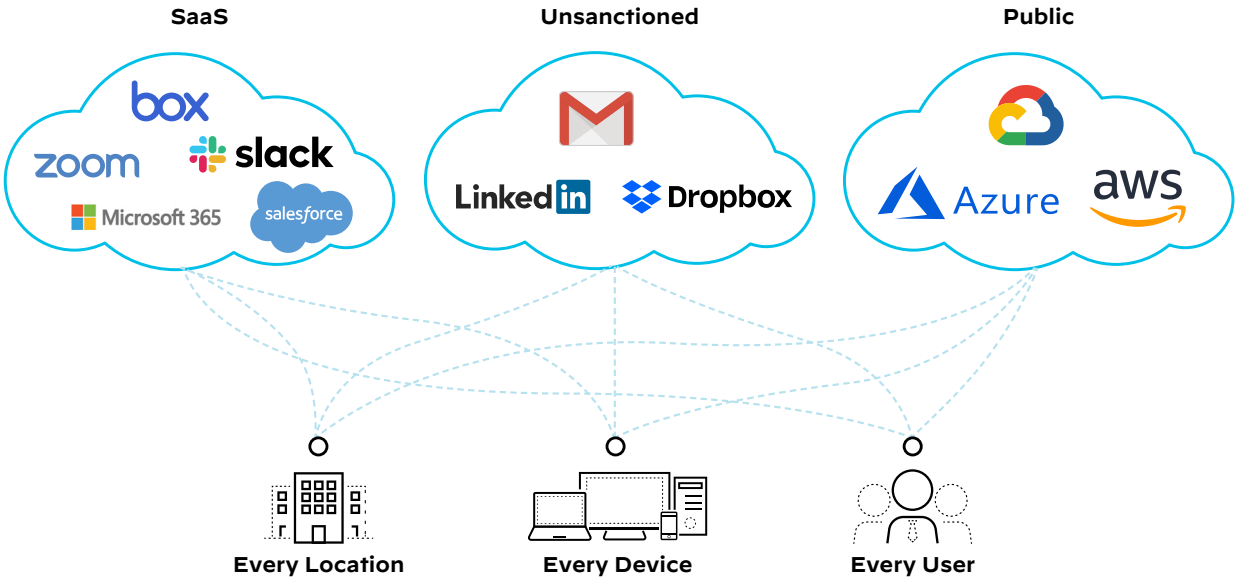


Figure 1: Cloud adoption and usage everywhere

Modern Collab Apps Wreak Havoc on Data Protection and Compliance

Today's collaboration applications have created a fundamentally different way of conducting business. Messages are now shorter and more frequent, consisting of multiple posts among two or more users. What's more, these new collaboration tools leverage more screen sharing and screen captures rather than traditional file sharing to quickly convey ideas and information. As a result, confidential information is more unstructured than ever, making it increasingly difficult to protect.

Additionally, depending on their location and industry, many organizations must adhere to various data privacy laws and regulations, such as the EU General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), the California Consumer Privacy Act (CCPA), and others.

Most companies will experience a data breach or security incident at some point, and those incidents can be costly. They can result in significant fines for noncompliance, class-action lawsuits, and reputational damage that can lead to loss of customer trust and confidence.

$3.92M

average data breach cost in 2019[3]

36%

loss of business stemming from loss of customer trust after a cyber incident[3]

$11.45M

annual average cost per company for insider-related incidents in 2020[4]

$644K

average incident cost[4]

€20 or 4%

of a company's annual global revenue, whichever is higher, can be the amount for a single GDPR fine[5]

3. "2019 Cost of a Data Breach Report," Ponemon Institute, July 2019, https://www.ibm.com/security/data-breach.
4. "2020 Cost of Insider Threats Global Report," Ponemon Institute, January 2020, https://www.observeit.com/cost-of-insider-threats.
5. "Understanding GDPR Fines," GDPR Associates, accessed April 22, 2020, https://www.gdpr.associates/what-is-gdpr/understanding-gdpr-fines.

Overcoming Visibility and Security Challenges

To protect your company, data, and employees and stay ahead of the SaaS explosion, you need to know:

- **Which cloud applications your users are using,** with what frequency, and the risks associated with each application, so you can take clear steps to mitigate the abuse of shadow IT.
- **Which users and devices have access** to your company's sanctioned SaaS applications (e.g., Microsoft 365®, Google Workspace™, Salesforce®, Box) to ensure only trusted individuals or devices have access.
- **What sensitive data** is being uploaded, downloaded, or stored in the cloud, and where.
- **How that data is being used and shared** (i.e., with authorized or unauthorized parties) in SaaS applications, and whether it is being shared according to your company's policies.
- **Which compliance risks your company must consider** with cloud applications and data, and how to minimize them.
- **Which threats are targeting your sanctioned applications,** which user behaviors are risky, and how to reduce these risks over time.

What apps are employees using and how?

How do I protect my sensitive data in the cloud?

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

Traditional Remedies Just Don't Work

Today's cloud-first digital businesses are facing a host of new challenges brought about by the shift to hybrid work and the explosion of SaaS and collaboration apps. When it came to securing cloud-based applications and the sensitive data that flows through them, security teams typically turned to:

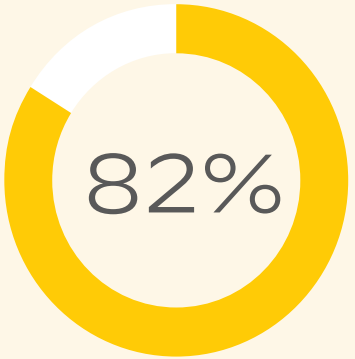
- **Built-in data protection capabilities** in SaaS applications and platforms, which differ from provider to provider, and app to app, and generally provide only basic security capabilities.
- **Cloud Access Security Brokers (CASBs),** which are specifically designed to address data protection, security and compliance across multiple SaaS applications.

  However, current CASB solutions only partially address today's business needs, leaving organizations exposed and vulnerable due to several critical limitations:

» They provide incomplete app visibility. These solutions miss over half of enterprise traffic which is non-web-based and rely only on static databases and support requests for app discovery, which hinders their ability to identify or contain new SaaS apps before they are a risk.

» They deliver inconsistent coverage. These disjointed and siloed solutions force organizations to apply different delivery methods and technologies to cover HQ, branch, and remote workers, resulting in massive gaps in protections.

» They provide inadequate data protections. Legacy data detection methodologies struggle to keep pace with the volume and sprawl of sensitive data in modern collaboration apps consistently in use throughout the enterprise, providing slow and inaccurate protection.

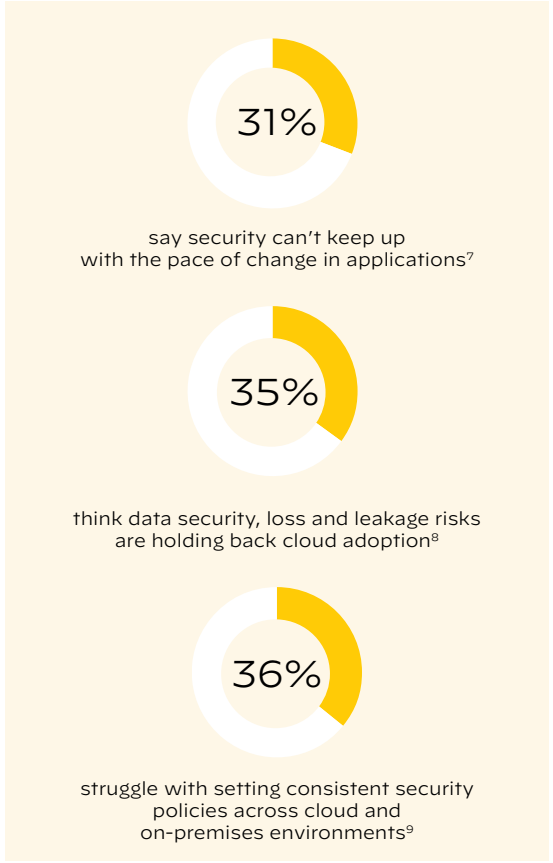


of security professionals say traditional security solutions either don't work at all in cloud environments or only have limited functionality[6]

6. "2020 Cloud Security Report," Cybersecurity Insiders, August 2020, https://www.cybersecurity-insiders.com/portfolio/2020-cloud-secuity-report-isc2/.

- They deliver poor security. Security unfortunately has always been just a check box feature in traditional CASB solutions, with the majority of vendors relying on loosely integrated (if at all) third-party threat detection capabilities. This approach provides limited security efficacy as well as little to no visibility of high-priority threats, unknown malware, and breaches.

What's more, legacy CASB solutions are notoriously complicated to adopt, deploy, and integrate with the rest of a company's security stack. Even when they are deployed, security and visibility may not always be available. Moreover, these approaches can create management complexity, siloed environments, and security gaps, leading to inconsistent security and compliance policies across different apps.



7–9. "2020 Cloud Security Report," Cybersecurity Insiders, August 2020, https://www.cybersecurity-insiders.com/portfolio/2020-cloud-secuity-report-isc2/.

How to Safely Adopt SaaS Applications

To safely adopt the cloud, companies need:
A single, consistent way to protect their ...

Users

Applications

Data

They also need:

Visibility into all traffic to know which applications employees are using—and how—to automatically discover and assess new shadow IT risks as well as monitor cloud usage in a granular way.

Enterprise data protection to discover, detect and secure all sensitive and regulated data, everywhere, both at-rest and in-motion, across every corporate network, cloud, and user.

Access control over corporate apps, with the ability to verify user identities and enforce company policies.

Advanced threat prevention to stop threats in the cloud in real time, with high reliability, without having to adopt third-party security tools.

Comprehensive security to protect all data, applications, and users across networks and clouds, regardless of their location, while avoiding the complexity of using multiple point products.

Compliance and risk management tools to automatically identify and remediate risks, exposures, and public links across all SaaS applications, protect all sensitive data, and ensure compliance consistently in a cloud environment.

A SaaS Security Strategy for Your Data

Ensuring safe cloud adoption includes ensuring secure storage and use of data in the cloud. Companies need to take a methodical approach to achieve a successful SaaS security strategy. This means making use of:

Automatic data discovery and classification for sensitive and regulated data transferred to and stored in the cloud, including personally identifiable information (PII) and intellectual property (IP) with a high degree of accuracy.

Data protection to secure data at rest or in motion (by alerting, encrypting, unsharing, applying digital rights, blocking unsafe transfers, etc.) to enable automatic data protection and leakage prevention, minimize user errors, and identify as well as stop risky or malicious behavior.

Compliance assurance to ensure the privacy and proper handling of regulated sensitive data, as well as to monitor and control what data can be shared—including how and with whom—and to facilitate compliance reporting and remediation.

To learn more about protecting data in the cloud, visit paloaltonetworks.com/cyberpedia/what-is-cloud-data-protection.

SaaS Security: A Key Step for SASE

To successfully secure your data in the cloud, your company needs an underlying architecture that supports both networking and security—in any location, including mobile users, branch offices, and retail locations—with applications and data.

A secure access service edge (SASE) solution brings together networking and network security services in a single cloud-based platform. Palo Alto Networks Prisma® SASE converges best-of-breed security and best-of-breed next-gen 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 part of Palo Alto Networks SASE solution, SaaS security plays 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 (such as traditional CASBs and web proxies), significantly simplifying adoption, and saving resources—technical, human, and financial.

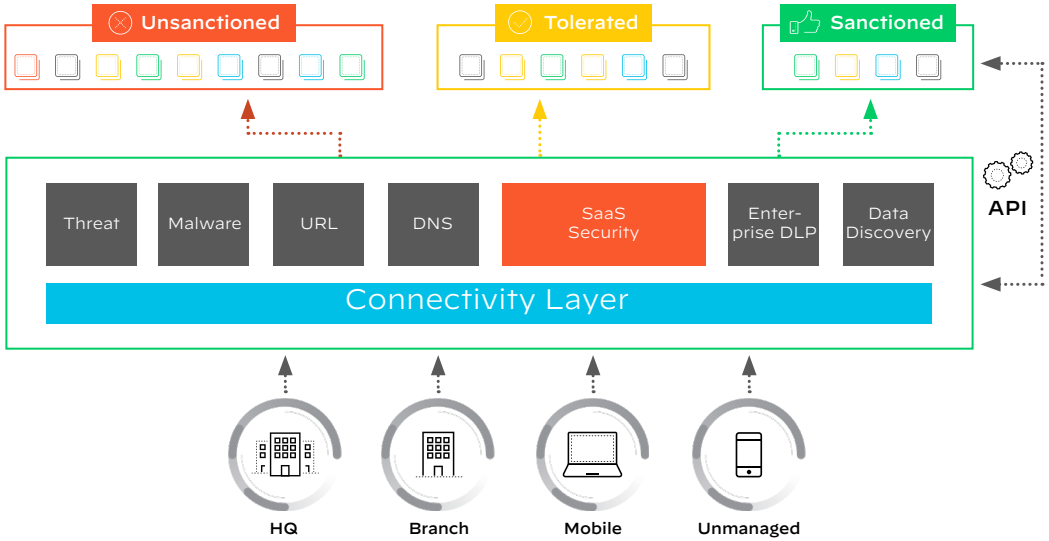


Figure 2: Consistent services from Palo Alto Networks

How Palo Alto Networks SaaS Security Can Help

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 SaaS explosion 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.

It specifically provides the following core security capabilities:

- See and secure all applications automatically, whether on-premises or in the cloud—ensuring you stay ahead of the app explosion. The reimagined Next-Gen CASB scans all traffic, ports, and protocols, automatically discovering new apps and leverages the industry's largest API-based coverage of SaaS apps—including modern sanctioned collaboration apps.
- Simply and consistently protect users everywhere with centralized control that brings SASE and CASB together in a single unified, cloud-delivered console. Optimized workflows and ML-based automation simplify configuration and provide deployment flexibility to easily and consistently extend best-in-class protection across your hybrid, local, and remote workforce.
- Accurately protect sensitive data in real-time with the industry's most comprehensive cloud-delivered enterprise DLP, powered by ML. Achieve unparalleled protection of even the most sensitive data with more automated detection engines, more control points, and content-aware technologies that ensure the highest levels of accuracy while seamlessly extending consistent protections across SaaS, IaaS, network, branch offices, and hybrid workforces.
- Stop known and unknown threats with the industry's most effective security, 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 data sets, we enable our customers to quickly and easily stop threats with inline, real-time, zero-day protections.

SaaS Visibility at Scale
Continuous discovery and control of new apps crowdsourcing a large global community.

Enterprise Data Protection
DLP and compliance consistent across all SaaS apps, networks, and users.

Best Security
Prevent threats in real time with ML-based attack prevention without third-party tools.

Easy and Cost-Effective
Easy-to-deploy and low TCO compared to legacy CASBs.

Conclusion

As you begin your journey to the cloud or adjust your existing cloud security strategy, consider a more comprehensive approach with a SASE solution that includes SaaS security. Palo Alto Networks can help safeguard your organization's users, applications, and data against cloud cyber risks through safe SaaS adoption. SaaS security is natively integrated into Palo Alto Networks SASE in order to provide consistent protection and secure access for cloud applications and data, delivered through a common cloud framework. Benefits include:

Comprehensive cloud visibility

- Get visibility into corporate cloud usage: what, where, and who.
- Discover shadow IT activities to minimize risks.
- Constantly monitor user behavior to unveil suspicious activities.

Complete and consistent cloud security

- Enable safe cloud adoption, branch expansion, and user mobility everywhere.
- Extend corporate policies, control and compliance, and data protection into SaaS.
- Eliminate unnecessary point products.

Compliance and data privacy in the cloud

- Manage user access and control privileges to protect data from untrusted users.
- Automatically discover, classify, and protect regulated information across multiple applications.
- Get assistance to meet data privacy and compliance requirements.

Learn more about the Palo Alto Networks SaaS security solution at paloaltonetworks.com/network-security/saas-security.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

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