Navigating the SaaS Security Jungle

How you can better protect your
applications, data, and users

Table of Contents

Introduction

As new technologies have emerged over the past decade, companies have begun moving their applications and data from in-house data centers to software-as-a-service (SaaS) applications, such as Microsoft Office 365, Box and Salesforce, as well as public cloud offerings, such as Google Cloud Platform (GCP), Amazon Web Services (AWS), and Microsoft Azure. The cloud enables organizations to enhance collaboration between users located around the world as well as realize cost savings when compared to on-premises solutions.

Unfortunately, while there are tremendous advantages in adopting and using the cloud, these technologies can also pose significant security risks to companies in areas 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.
- **Too many different kinds of data:** 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 applications have become incredibly popular in recent years due to their widespread availability, ease of use, and low costs.

Gartner estimates that, by 2021, more than 70% of business will be substantially provisioned with cloud office capabilities.

However, just because SaaS applications are easy to use doesn't mean they're secure. In fact, most companies struggle to adopt and use SaaS applications 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 data 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.

Cloud has no boundaries

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

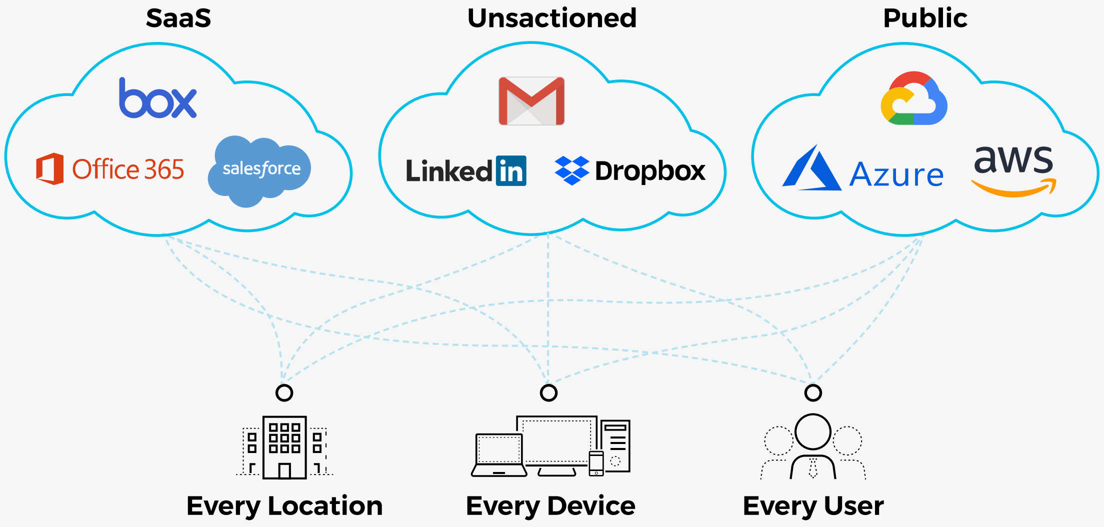


Figure 1: Cloud adoption and usage everywhere

1. "Widespread Adoption of Cloud Office Is Now Well Underway," Gartner, June 28, 2017, https://www.gartner.com/smarterwithgartner/widespread-adoption-of-cloud-office-is-now-well-underway.
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.

Data Protection and the High Cost of Compliance

Data protection becomes a major concern when data begins to bleed between internal and external networks, becoming exposed across SaaS applications with users who may or may not be authorized to access said data. Adding third-party vendors, such as different SaaS providers, to the mix creates security gaps, increasing both data exposure risk and compliance concerns. With so many egress points and assets shared throughout a company, the process of knowing and tracking where all the sensitive and regulated data resides and moves becomes tedious, making it difficult for companies to find, monitor, and secure those assets.

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

an average data breach cost in 2019[3]

36%

is the loss of business stemming from loss of customer trust after a cyberincident[3]

Figure 2: The cost of a data breach in 2019[3]

$11.45M

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

Figure 3: The cost of insider threats in 2020[4]

$644K

is the 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]

Figure 4: The hefty cost of noncompliance[4]

[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 when transitioning to the cloud, 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 Office 365, G Suite®, 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?

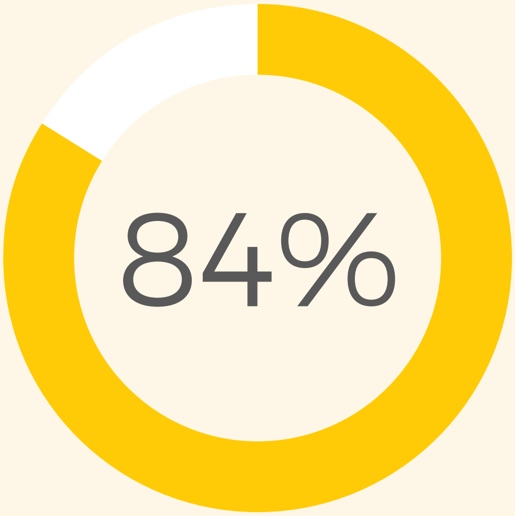
Can I govern access to my SaaS apps and secure from threats?

Traditional Remedies Just Don’t Work

Many companies have attempted to secure their adoption of the cloud by using:

- **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.
- **Tools from different vendors,** such as a standalone cloud access security broker (CASB), a secure web gateway (SWG) and cloud data loss protection (DLP), disjointed from one another and from the company’s existing security deployments on-premises.
- **Web proxies,** which are notoriously difficult to interoperate, as problems inherently arise around how proxies are supposed to interact with firewalls and with one another. Plus, proxies don’t scan all traffic.

Unfortunately, all these solutions can be 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.



of security professionals say traditional security solutions either don’t work at all in cloud environments or have only limited functionality.

6. “2018 Cloud Security Report,” Cybersecurity Insiders, August 2018, https://start.paloaltonetworks.com/cloud-security-report-2018.

How to Safely Adopt SaaS Applications

To safely adopt the cloud, companies need:

A single, consistent way to protect their…

Users

Applications

Data

Business

They also need:

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

Data protection to discover, detect and secure all sensitive and regulated data, both at rest and in motion, across networks and clouds.

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 and from the internet.

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).

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 offers a comprehensive SASE solution to safeguard against these risks, assist you through your cloud and network transformation, and help you safely adopt SaaS applications.

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 CASBs and web proxies), significantly simplifying adoption, and saving resources—technical, human, and financial.

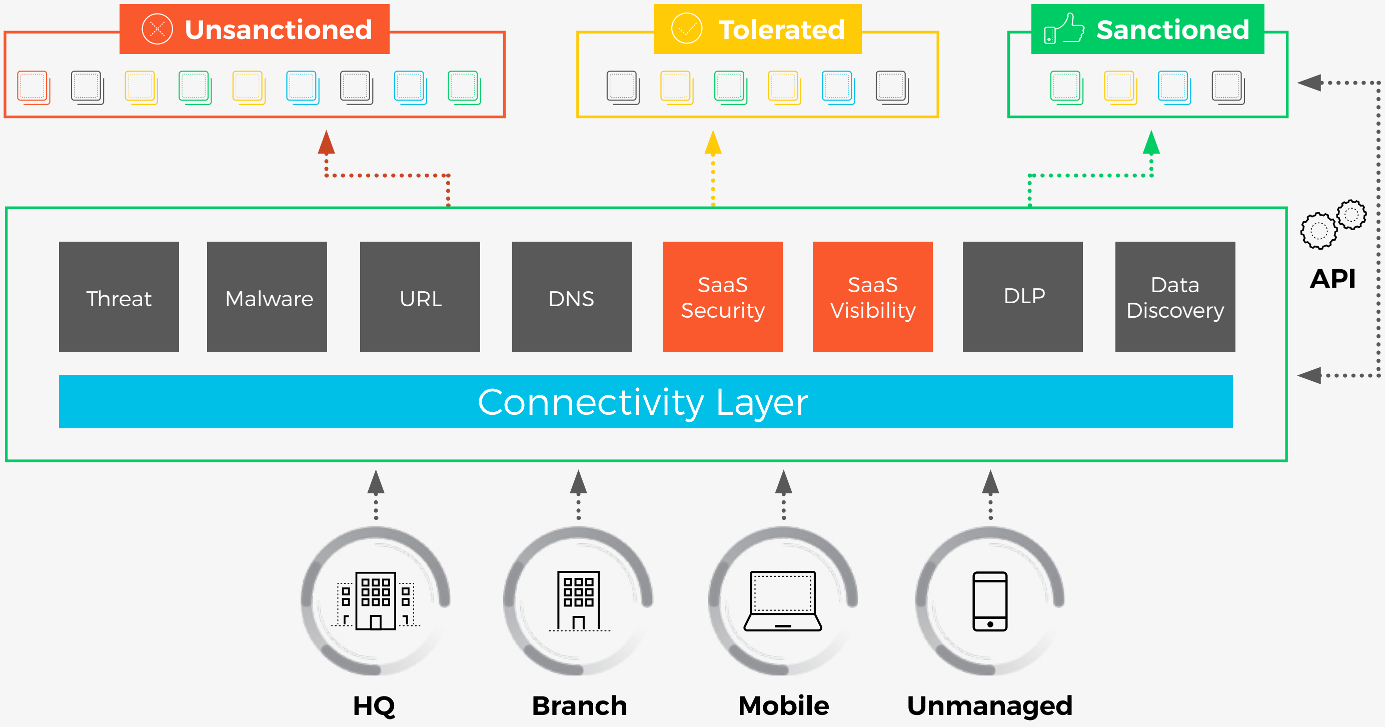
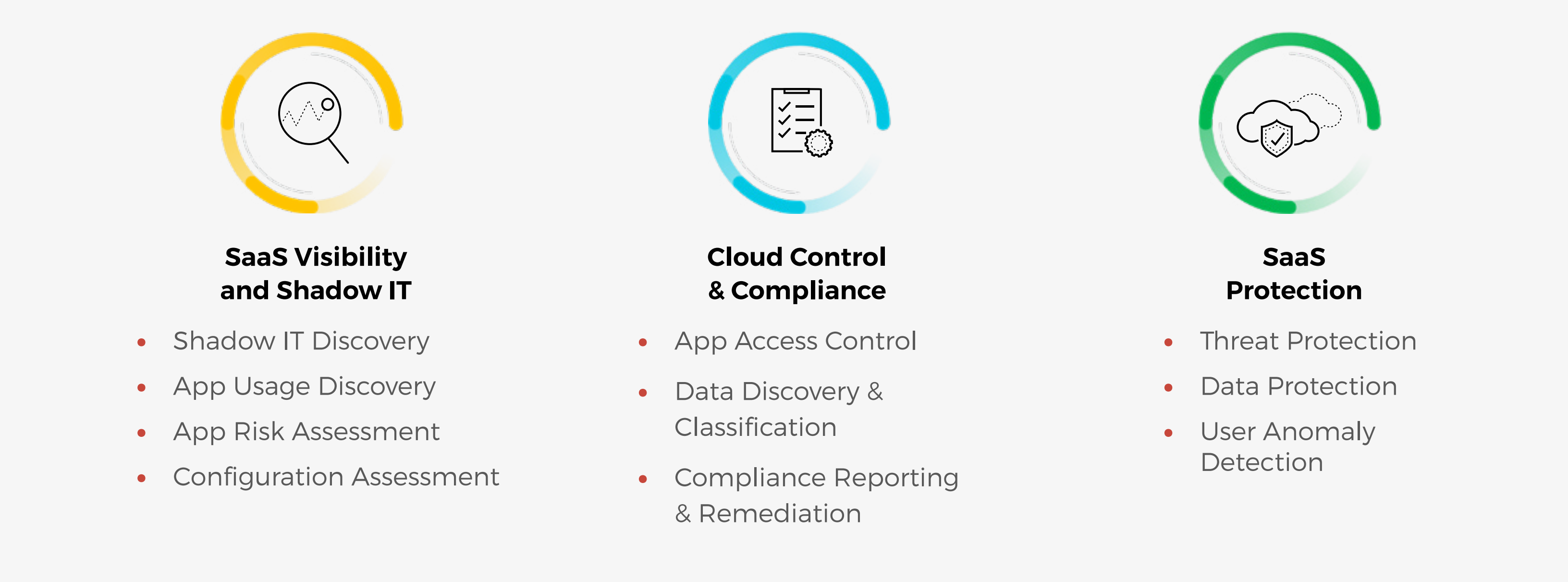


Figure 6: Consistent services from Palo Alto Networks

How Palo Alto Networks SaaS Security Can Help

Palo Alto Networks SaaS security offering specifically provides the following core security features:

- Complete visibility into the applications your organization uses, as well as application risks and use across all your enterprise traffic—including branch offices and mobile users—to minimize shadow IT.
- Enterprise data loss prevention (DLP) to discover, monitor and protect all sensitive data at rest or in motion, including uploads to sanctioned or unsanctioned applications as well as data stored, and shared in sanctioned applications.
- Access control to govern and manage access to sanctioned SaaS applications, ensuring only trusted access is guaranteed while maintaining a secure user experience that doesn't impede users' work.
- A solution that delivers comprehensive, consistent, and automated cloud security to protect SaaS applications and data.
- Protection against cyberattacks or behavior that might lead to data breaches.
- Robust incident management and remediation.



SaaS Visibility and Shadow IT

- Shadow IT Discovery
- App Usage Discovery
- App Risk Assessment
- Configuration Assessment

Cloud Control & Compliance

- App Access Control
- Data Discovery & Classification
- Compliance Reporting & Remediation

SaaS Protection

- Threat Protection
- Data Protection
- User Anomaly Detection

Figure 7: Palo Alto Networks SaaS security

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 organizations data, users, and networks against cloud cyber risks through safe SaaS adoption. SaaS security is integrated into Palo Alto Networks SASE solution to providing 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/prisma/saas

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.**