SaaS Security

The Current State of SaaS— A Spend, Usage and Risk Perspective

SaaS applications provide tremendous convenience to end users and are key enablers in driving business agility and user productivity. But as they continue to change the way organizations do business, their exploding numbers create security risks that organizations must address.

Reducing security risks in SaaS applications, where organizations' most sensitive data often resides, is key to securing the cloud-led enterprise IT of the future. As a result, protecting enterprise SaaS, users and data is at the top of every enterprise CISO's priority list.

Cloud is the Powerhouse That Drives Today's Digital Organizations

2021 → 2023

$152M → $208M

Worldwide Public Cloud Services End-User Spending Forecast for SaaS.

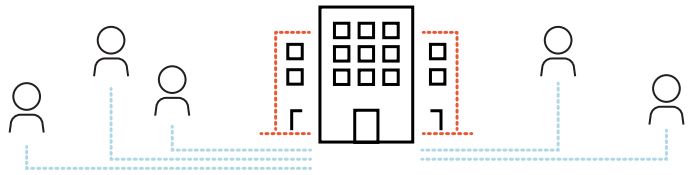
2020 → 2025

70% → 85%

Share of SaaS apps in terms of total company software use.

Companies spend an average of **USD 2,884** per employee on SaaS (more than hardware) and this figure is increasing with more industries transitioning to a SaaS model.

Remote Work Has Validated the Cloud's Value Proposition



26.7%

% of U.S. employees worked remotely in 2021.

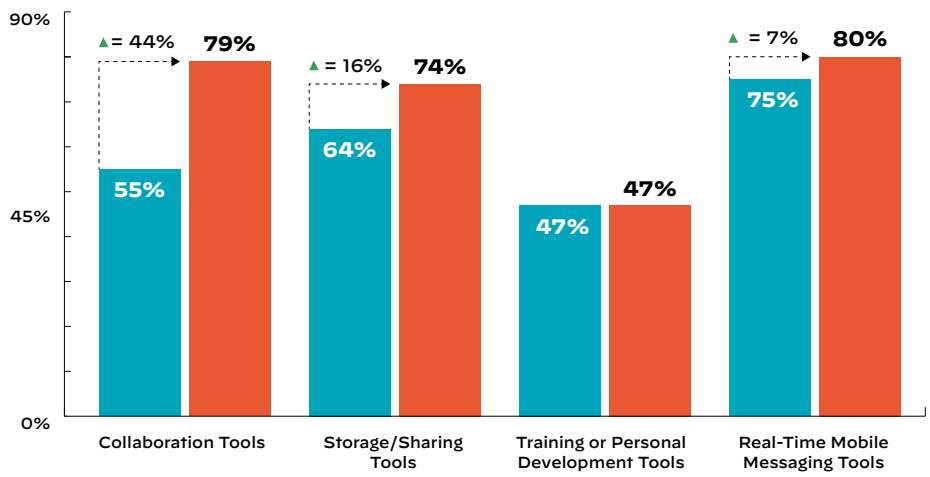
36.2M

U.S. employees are expected to work remotely by 2025 - a 417% increase from pre-pandemic levels.

Shifting to remote work for the longer term has resulted in most companies pivoting to SaaS-based offerings.

Collaboration App Usage Has Skyrocketed Since the Pandemic

Changes in Digital Workplace Technology Use, 2019-2021 (Percentage of Respondents)



Source: Gartner (August 2021)

Gartner predicts that by 2024, in-person meetings will drop from **60% of enterprise meetings to 25%**, driven by remote work and changing workforce demographics.

Collaboration Apps That Made it to the Top of the Popularity List

Chat tools

47%	Slack
32%	Microsoft Teams
14%	Skype
14%	WhatsApp

Video conferencing tools

44%	Zoom
33%	Microsoft Teams
29%	Google Meet

Calendar software

59%	Google Calendar
37%	Microsoft Outlook
13%	Microsoft Exchange

Knowledge sharing tools

34%	Confluence
23%	Google Docs
21%	Google Drive

File sharing tools

42%	Google Drive
23%	Microsoft OneDrive
14%	Sharepoint

Document collaboration platforms

39%	Google Docs / Sheets
36%	Microsoft 365
26%	Confluence

Tooling stacks

Issue trackers

Team collaboration tools

22%	Altassian	42%	Jira	35%	Confluence
21%	GitHub	30%	GitHub Issues	32%	Jira
19%	Google	17%	GitLab Issues	30%	Microsoft Teams

Transitioning to SaaS Has Been Great But Brings New Changes

SaaS Usage is Exploding

The typical enterprise now has over **>100** SaaS apps in use.

Data is Changing

Data comes in **all forms** and is collaborated on in **real-time**.

Attackers are Adapting

Attackers go where the data is — and now that place is **SaaS**.

New Changes Equals New Security Concerns

SaaS misconfigurations are a growing problem. They create vulnerabilities within enterprise SaaS apps.

Data moves in new ways, through **collaboration apps**, and **between apps** using integrations.

SaaS is used to attack users and steal data. Compromised users and malicious insiders **access data** inside SaaS from **anywhere**.

Up to **99%** Cloud security failures will be caused by human error.

80% Employees use collaboration SaaS apps to get work done.

470% YoY increase in SaaS being used to deliver attacks.

Existing Approaches Fail to Address New Security Concerns

Basic posture controls can't keep up.

Traditional approaches to DLP don't work for SaaS.

Attackers easily bypass second-rate security.

Securing Modern SaaS Requires a ZTNA 2.0 Approach

MONITOR ALL SaaS USAGE

You cannon secure what you cannot see.

Continuously **discover and control** all SaaS consumption.

SECURE THE APPS

Saas apps aren't "secure by default".

Secure sanctioned SaaS from **dangerous misconfigurations**.

PROTECT THE DATA

Sensitive data loss can occur anywhere.

Protect data **everywhere**, including modern **collaboration apps**.

PREVENT ATTACKS

Users and content in Saas can be malicious.

Inspect **all content** and user **activity** to stop attackers and malicious insiders.

So, What Should You Do Next?

Safely embrace the cloud, with a single, consistent way to protect your applications, data and users across every corporate environment.

Take a Next-Generation CASB approach that gives you the necessary visibility and control of all SaaS usage, comprehensive SaaS Security Posture Management, data security built for modern SaaS and protection from advanced threats.

Palo Alto Networks Next-Gen CASB with SSPM is available with **Prisma SASE** —the industry's most complete SASE solution that delivers ZTNA 2.0, CASB, SD-WAN, ADEM, and SWG all on a single, unified product—as well as—our **next-gen firewalls**. As your organization continues to adopt SaaS to enable a remote-hybrid workforce, consider our NG-CASB with SSPM to continuously monitor business critical SaaS apps, prevent configuration drifts and address security hygiene issues that put users and data at risk.

LEARN MORE

Sources:
Gartner, Forecast: Public Cloud Services, Worldwide, 2020-2026, 1Q22 Update
BetterCloud, 2020 State of SaaSOps Report
Deloitte, SaaS-enabled solutions deliver win-win for companies and customers
Zippia - Remote Work Stats 2022
Upwork, Future Workforce Pulse Report
The State of Developer Ecosystem 2021
Gartner, Is the Cloud Secure?
Unit 42

---

www.paloaltonetworks.com

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

3000 Tannery Way
Santa Clara, CA 95054

© 2020 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.