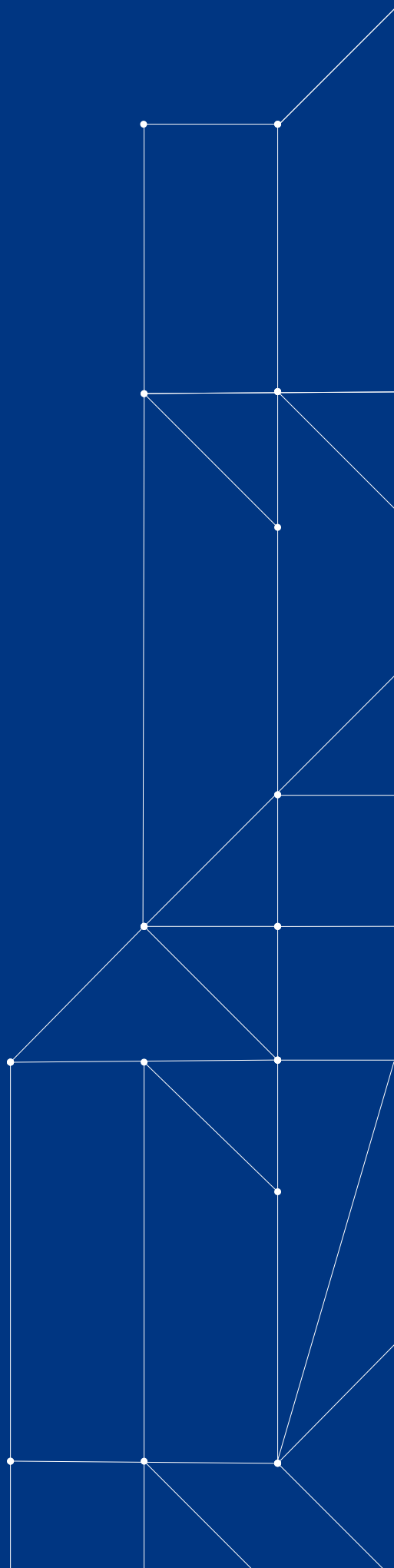
CLOUDFLARE

WHITEPAPER

Simplifying the way we protect SaaS applications

How to protect users and data with a Zero Trust approach

Content



Introduction

In today's distributed environment, software-as-a-service (SaaS) applications have given organizations greater flexibility to support corporate employees and contractors across the world. Some of the most notable SaaS application suites currently include communication (email delivery, chat platforms), productivity (documents, spreadsheets), and collaboration (online storage). By 2025, Gartner predicts that 85% of enterprises will run their businesses with a cloud-first principle — with SaaS as the preferred vehicle for access management deployments[1].

While SaaS applications allow organizations to remain more agile, however, the shift to the cloud comes with associated security and performance risks, especially for organizations that are juggling multiple point solutions designed to operate independently of each other. Tasked with implementing and managing dozens, if not hundreds, of these applications, security, networking, and IT teams are often strapped for time, struggle to gain visibility across their entire organization, and wrestle with security and connectivity gaps left by services that are not inherently designed to work together.

As a result, many organizations are driven to find better ways of consolidating security products across their SaaS landscape — to improve efficiency, reduce management and implementation complexity, and receive consolidated support.

Gartner predicts that by 2025, 80% of enterprises will turn to single-vendor solutions that unify web, cloud services, and private application access from a security services edge (SSE) platform[2].

Starting the journey to simplified SaaS security comes with several important considerations. The way workforces communicate and operate today calls for a simple and scalable approach to security, one that is designed to stay ahead of emerging risks, reduces incidents that come from SaaS applications, and makes it easy for security teams to monitor and prevent threats to their organizations.

Read on to discover how a Zero Trust platform — one that integrates cloud access security broker (CASB) and cloud email security (CES) capabilities — provides the easiest path to stop data loss, phishing, ransomware, shadow IT, and lateral movement across your organization.

[1] Gartner, "Forecast Analysis: Information Security and Risk Management, Worldwide." Analysts: Shailendra Upadhyay, Mark Driver, Christian Canales, Ruggero Contu, Lawrence Pingree, Elizabeth Kim, John A. Wheeler, Nat Smith, Rahul Yadav, Swati Rakheja, Dave Messett, Mark Wah, Shawn Eftink. August 12, 2021. Gartner. [2] Gartner, "Predicts 2022: Consolidated Security Platforms Are the Future." Analysts: Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans. December 1, 2021. Gartner.

The evolution of CASB

Comprehensive SaaS security requires several crucial technologies, so security teams can gain visibility into their entire SaaS landscape, easily monitor and mitigate threats, and secure access to sensitive data and systems. One of the most important components of any SaaS security strategy is a cloud access security broker, or CASB, which provides data security controls over and visibility into an organization's cloud-hosted services and applications.

SaaS security 101: CASB

CASB SaaS allows IT and security teams to view all of their data settings and user activity from a single dashboard. Its capabilities vary by provider, but typically include the following attributes[1]:

- **Data protection:** CASBs protect sensitive data and prevent it from leaving company-controlled systems.
- **Access control:** CASBs help control what users can see and do within company-controlled applications. They may also provide identify verification capabilities to ensure that users are who they claim to be.
- **Shadow IT detection:** CASBs help identify unauthorized systems and services (commonly referred to as "shadow IT") that employees use for business purposes. By cataloging these systems, they can detect and mitigate previously unknown security risks.
- **Threat protection:** CASBs use anti-malware detection, sandboxing, packet inspection, and other technologies to help block data leaks and external attacks.
- **Posture management:** CASBs give security teams insight into user behavior analytics and control over application posture, so they can easily survey movement and track threats across their SaaS environment.
- **Compliance:** CASBs help organizations meet regulatory requirements (e.g. SOC 2, HIPAA, GDPR, etc.) by identifying misconfiguations and, in doing so, avoid associated penalties and fines for compliance violations.

[3] This is not an exhaustive list of capabilities that may be included in a CASB offering.

Understanding modern CASB challenges

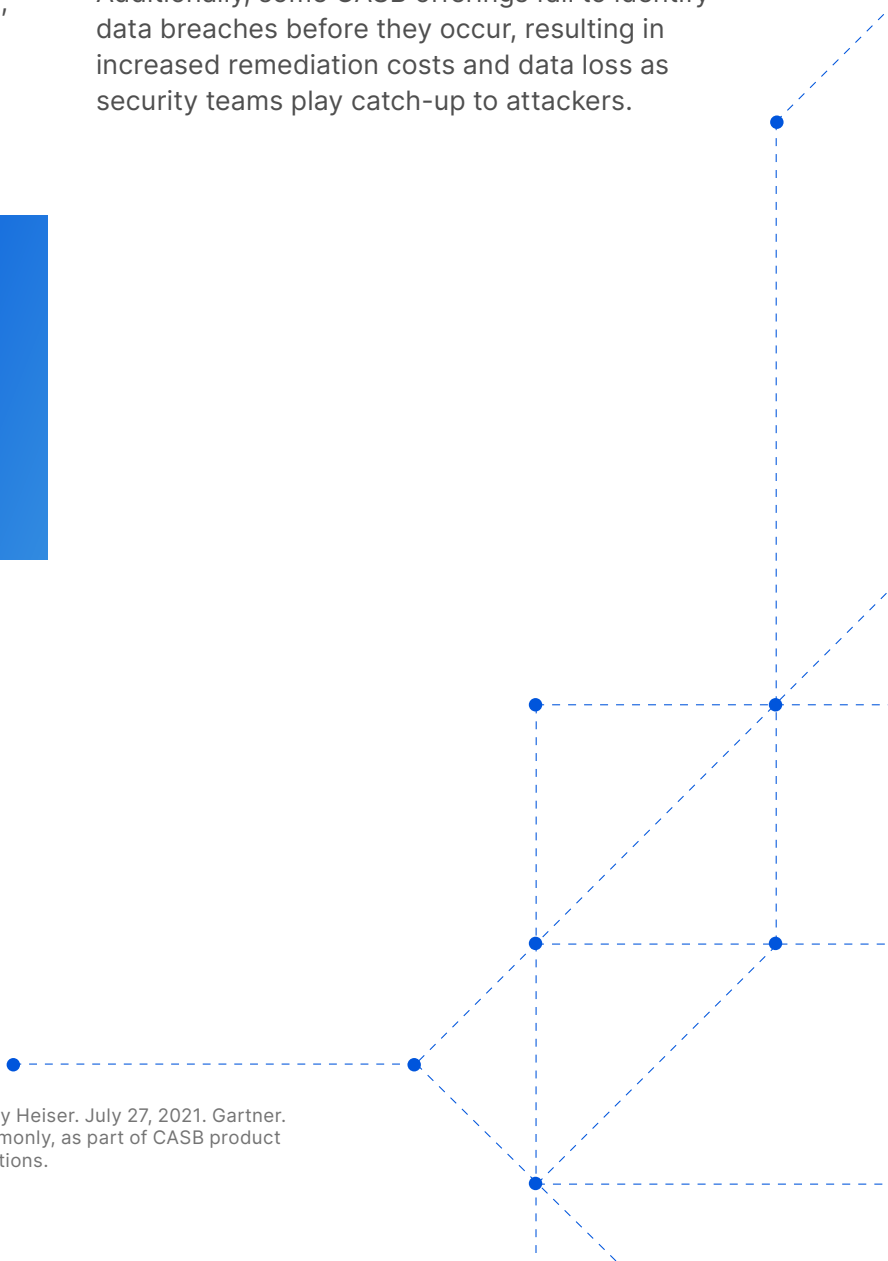
As SaaS adoption increases, so does the attack surface organizations need to protect. Instead of a single database containing valuable data, that data is now dispersed to applications that are managed by third parties (e.g. Dropbox, Google Drive, etc.) — whether or not you've sandboxed them for corporate use.

While CASBs help protect company data and users within SaaS applications, they are still not a perfect catch-all for threats. Because a higher volume of valuable data is processed using SaaS applications, attackers increasingly target these applications in order to carry out data breaches and other threats. And simple misconfigurations and user errors can leave the door open to these attacks as well:

Gartner predicts that more than 99% of cloud breaches through 2025 will originate from preventable misconfigurations or mistakes made by users[4].

When it comes to anticipating and remediating user misconfigurations and modern SaaS attacks, many CASBs still fall short. To address this, some vendors have started to offer cloud or SaaS security posture management (CSPM or SSPM[5]) services, which are designed to track configuration and compliance errors at the control plane. However, this is not the case across the board, leaving many organizations without the detection and remediation capabilities they need.

Additionally, some CASB offerings fail to identify data breaches before they occur, resulting in increased remediation costs and data loss as security teams play catch-up to attackers.



[4] Gartner, "Hype Cycle for Cloud Security, 2021." Analysts: Tom Croll, Jay Heiser. July 27, 2021. Gartner.
[5] These services and features are often offered alongside or, more commonly, as part of CASB product offerings — providing both in-line and API-based protection for applications.

The trouble with CASB implementation and integration

As SaaS vendors strengthen the capabilities of their built-in security offerings, two major hurdles remain: integration and visibility. These vendors make data accessible and easy to consume, but still place the burden on organizations to consolidate security capabilities in a way that is easy to manage. For organizations that adopt multiple point solutions, tracking threats across different platforms becomes more difficult when those solutions are not designed to integrate with each other or come with different levels of visibility.

This increases the complexity of the application environment, so even basic attacks become more difficult to anticipate and mitigate — as attackers only need to identify gaps between security platforms in order to carry out attacks undetected. With a CASB, organizations can access security products from the same place, giving them better visibility and mitigation capabilities across their entire security stack.

Even so, CASBs are only one piece of a larger SaaS security strategy. To cover the entire SaaS landscape, organizations need to converge CASB capabilities with other Zero Trust technologies, without adding unnecessary complexity or forcing security teams to manually configure and maintain each tool. Successfully controlling SaaS at scale cannot be a manual process — automation is required to complement SaaS management platforms and CASB tools, allowing organizations to effectively mitigate a wide range of threats without risking team burnout or user misconfigurations and errors.

The evolution of email security

As with most SaaS services, email communication has evolved as an essential business application for organizations of all sizes. With the shift to the cloud and remote work, more organizations are turning to cloud email solutions within Microsoft 365 and Google Workspace — as much as 70% of organizations worldwide, per Gartner[6].

Consequently, email is now the most widely-adopted SaaS application and makes up one of the largest attack surfaces — attracting phishing, malware, spoofing, business email compromise (BEC), and other modern threats.

Protecting against email attacks can be a tedious and overwhelming task for security teams, however, especially as attackers continue to employ more sophisticated tactics against unsuspecting employees. To safeguard users and data from these threats, security leaders should consider integrating email on their SaaS security platform in a way that improves visibility and provides more robust and simplified protection.

SaaS security 101: Email security

Modern email security encompasses a set of tools, processes, and techniques for protecting email accounts and content against malicious attacks and unauthorized access. Some of the most common types of email security technologies include the following:

- **Secure email gateways (SEG):** SEGs process and filter SMTP traffic, and require organizations to change their MX record to point to its mail transfer agent.
- **Cloud email security (CES):** CES analyzes email content (via API access to cloud email providers) without the need to change the MX record. (Note: Gartner refers to this category as “ICES” or “integrated CES.”)
- **Domain-based Message Authentication Reporting and Conformance (DMARC):** DMARC authenticates emails by checking a domain’s sender policy framework (SPF) and DomainKeys Identified Mail (DKIM) records. Within this system, emails that fail SPF or DKIM checks are marked as spam or blocked from reaching their intended recipient.
- **Email data protection (EDP):** EDP solutions use encryption to help prevent accidental data loss and unauthorized access to email content.

[6] Gartner, “Market Guide for Email Security.” Analysts: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. October 7, 2021. Gartner.

Understanding modern email security challenges

Originally delivered via on-premise software platforms, email has increasingly shifted to cloud-native delivery systems. Many organizations have turned to feature-rich productivity suites like Microsoft 365 and Google Workspace, which allow users to work and collaborate more effectively.

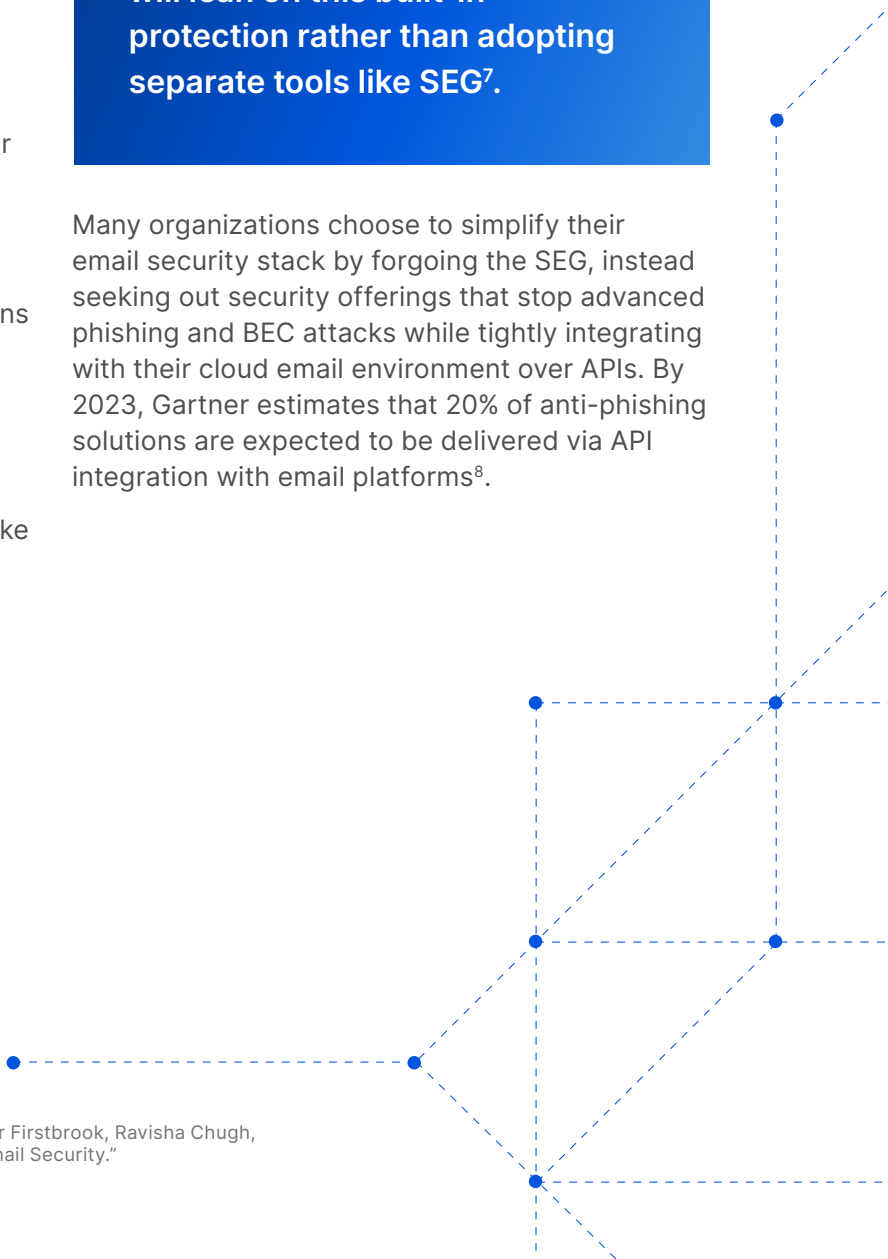
Since email has been around for a long time, even casual users are aware of some of the more prevalent threats they may encounter via email — including suspicious emails, malicious links, and more. As a result, attackers have evolved their strategies to make it more difficult to tell the difference between legitimate and malicious messages. These blended threats go across multiple communication channels in order to appear more legitimate (e.g. vishing, smishing, etc.), and are often successful in tricking users into giving up sensitive information.

The increase in email usage also opens organizations to breaches: once an attacker gains access to someone's email account, it's often easy for them to move laterally within an organization and compromise or steal sensitive data. And while cloud email providers offer limited built-in security capabilities designed to mitigate common threats like spam, malware, and phishing, they are notoriously weak against attacks from compromised internal senders moving laterally from inbox to inbox.

In order to combat these threats, email security solutions are evolving as well. Native cloud email platforms provide a base level of built-in security capabilities that can handle common spam and malware attacks.

By 2023, Gartner estimates that at least 40% of all organizations will lean on this built-in protection rather than adopting separate tools like SEG[7].

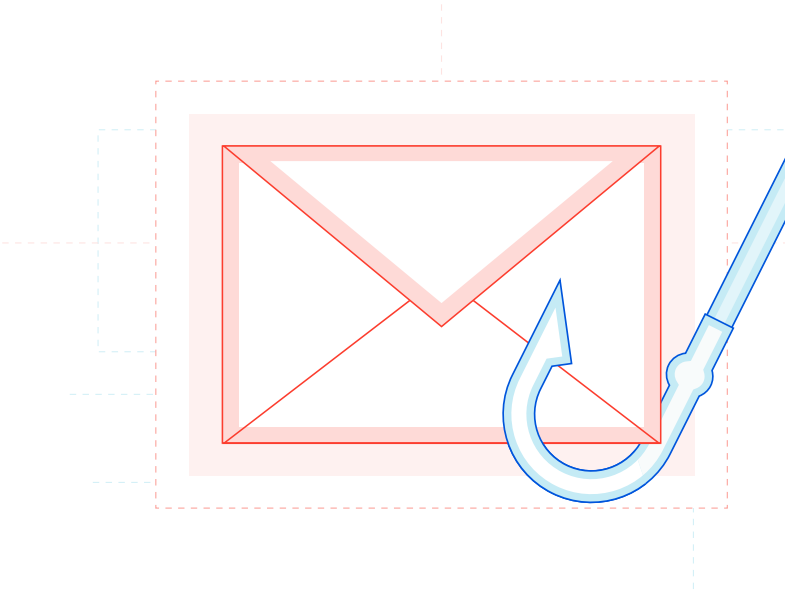
Many organizations choose to simplify their email security stack by forgoing the SEG, instead seeking out security offerings that stop advanced phishing and BEC attacks while tightly integrating with their cloud email environment over APIs. By 2023, Gartner estimates that 20% of anti-phishing solutions are expected to be delivered via API integration with email platforms[8].



[7] Gartner, "Market Guide for Email Security." Analysts: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. October 7, 2021. Gartner. [8] Gartner, "Market Guide for Email Security."

The trouble with email security implementation and integration

While these built-in capabilities provide organizations with some peace of mind, they are far from sufficient to combat modern email threats. Entire categories of attacks — like spear phishing, BEC, and more — require dedicated security platforms that are not offered by email providers. And legacy email security solutions are not designed to scale, combat cloud-native challenges, or catch highly targeted attacks.



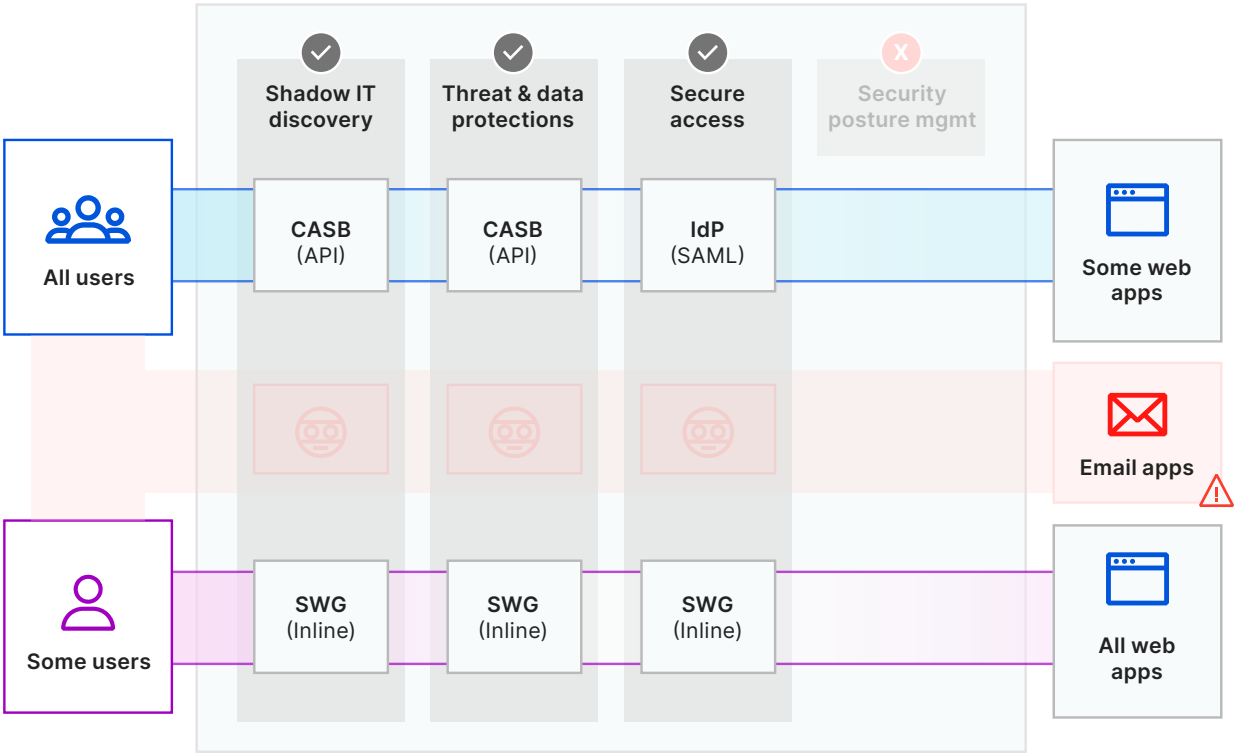
Even when security teams pinpoint email security tools that are designed to catch modern threats, they may run into additional problems: complex configuration requirements, time-consuming deployment processes, and tedious policy maintenance challenges. For example, SEG products are notoriously difficult to deploy against email attacks, as it is not feasible (or scalable) to maintain an ever-lengthening list of policies to stop every attack variant. Detecting advanced attacks requires using algorithms at scale that only cloud-native services are equipped to handle.

In order to shield corporate email systems from these attacks — without overburdening security teams, layering legacy hardware products, or relying on employees to catch every malicious message — organizations need a Zero Trust approach that integrates cloud-native email security capabilities and reduces implicit trust in email-based communications.

A better approach to SaaS security

SaaS applications, from communication platforms to email delivery systems, make up a sizable part of today's business operations. But protecting these applications against increasingly complex threats can be a nightmare for security teams, who are often tasked with wrangling multiple tools that are not designed to natively integrate with each other or capable of providing visibility into an organization's entire SaaS landscape.

Traditional SaaS security

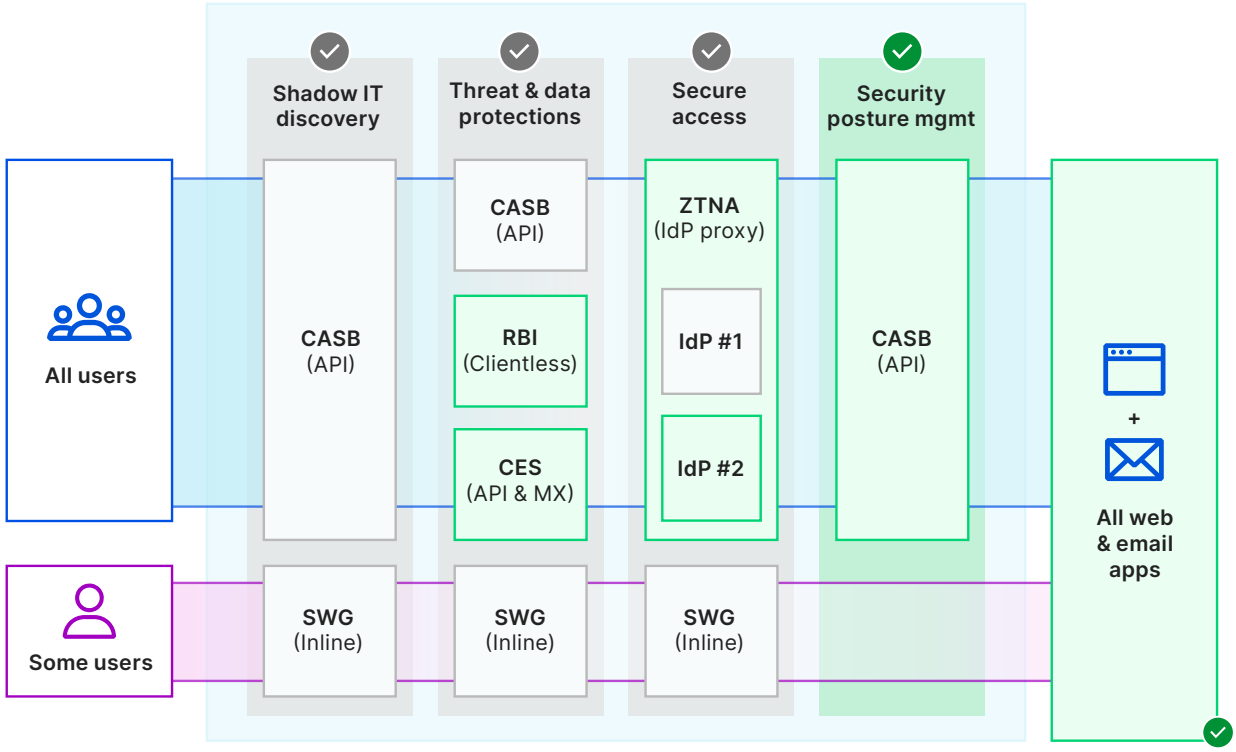


SWG = secure web gateway | CASB = cloud access security broker | IdP = identity provider

As vendors crafted more robust SaaS security tools, IT and security teams were tasked with piecing together these best-in-class solutions to secure their applications and data. This often required considerable time and internal resources to implement and manage — and, while point solutions were capable of addressing threats on an individual level, there was no overarching platform that provided multi-vendor support and visibility across the entire organization.

Often, traditional SaaS security measures also failed to fully extend their protections to email platforms, leaving organizations vulnerable to targeted attacks that replicated business-critical workflows, impersonated trusted partners and users, and easily bypassed existing email classification systems and built-in controls. And without native integration between these solutions — or visibility across the entire threat landscape — protecting applications against modern threats left even more gaps for security teams to remediate.

Modern SaaS security



SWG = secure web gateway | CASB = cloud access security broker | IdP = identity provider | RBI = remote browser isolation
CES = cloud email security | ZTNA = Zero Trust network access

To remedy the gaps left by traditional SaaS security and management solutions, organizations need modern threat protection that is designed to secure applications and data from a single, Internet-native platform. A critical component of this modern approach is robust security posture management, which allows security teams to better determine how users access critical resources and gain visibility into and control over external and internal threats.

Instead of requiring organizations to operate single-solution tools to remediate individual threats, a SaaS security platform can scan applications to detect anomalies in configuration, permissions, and sharing, then enable security teams to manage application access, mitigate email attacks, block insider threats and risky data sharing, and more.

This approach not only provides more robust and comprehensive protection for SaaS applications, but enables organizations to save time triaging tickets, automate security processes, and focus on strategic initiatives rather than worrying about data leakage, attacks, and manual configurations and maintenance.

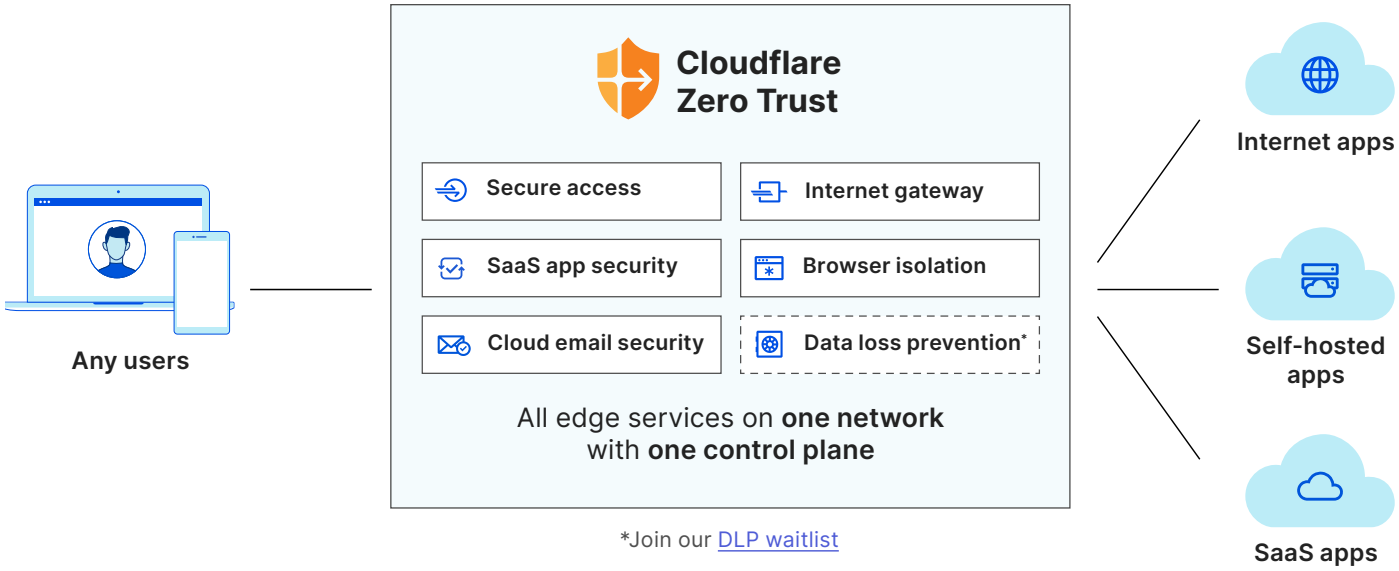
Applying a Zero Trust approach to SaaS security

Developing the right approach to SaaS security requires a bird's eye view of modern SaaS and cloud-based threats, but tailoring existing solutions to an organization's needs can be a heavy lift for IT and security teams. Instead of combating threats on an individual level — or relying on a patchwork of siloed tools — organizations need a security platform that is simplified, easy to manage, and capable of anticipating and mitigating modern threats.

While both CASB and cloud email security functionalities are essential components of a SaaS security strategy, they are designed to work best within a Zero Trust architecture — one in which every piece of technology works better together than it would alone. When implemented correctly, this layering also helps alleviate adjacent issues by eliminating security gaps, conserving security team bandwidth, and automating threat surveillance.

How Cloudflare protects SaaS apps

Cloudflare provides the easiest path to protecting your entire SaaS landscape, allowing organizations to control how their users access critical resources, how they keep those resources safe from external or internal attacks, and how they monitor and mitigate risks in real-time.



*Join our DLP waitlist

Securing SaaS applications with Cloudflare Zero Trust

To secure data in transit, Cloudflare Zero Trust places access (ZTNA), gateway (SWG), and browser isolation (RBI) controls in front of cloud and SaaS applications to support and operate as an inline CASB deployment architecture.

To secure data at rest within SaaS applications, easy-to-configure, API-driven integrations continuously scan highly-used applications for vulnerabilities and potential threats.

Combining Cloudflare Area 1 email security with Cloudflare Zero Trust

Cloudflare Area 1 email security is a representative ICES vendor that offers organizations more flexibility depending on their email security needs. It does this by integrating via API and acting as a gateway to verify, filter, inspect, and isolate email traffic inline via MX record changes.

Area 1 preemptively crawls the Internet to discover attack infrastructure and phishing campaigns, protecting customers from phishing attacks days before they reach recipient inboxes.

To learn more about how Cloudflare helps secure SaaS applications, visit https://www.cloudflare.com/products/zero-trust.

Sources

1. Gartner, “Forecast Analysis: Information Security and Risk Management, Worldwide.” Analysts: Shailendra Upadhyay, Mark Driver, Christian Canales, Ruggero Contu, Lawrence Pingree, Elizabeth Kim, John A. Wheeler, Nat Smith, Rahul Yadav, Swati Rakheja, Dave Messett, Mark Wah, Shawn Eftink. August 12, 2021. Gartner.

2. Gartner, “Predicts 2022: Consolidated Security Platforms Are the Future.” Analysts: Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans. December 1, 2021. Gartner.

4. Gartner, “Hype Cycle for Cloud Security, 2021.” Analysts: Tom Croll, Jay Heiser. July 27, 2021. Gartner.

6. Gartner, “Market Guide for Email Security.” Analysts: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. October 7, 2021. Gartner.

7. Gartner, “Market Guide for Email Security.” Analysts: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. October 7, 2021. Gartner.

8. Gartner, “Market Guide for Email Security.” Analysts: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. October 7, 2021. Gartner.

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-3303.2022JUN23