Publication date:
21 Oct 2022
Author:
Rik Turner, Principal Analyst, Emerging Technologies

Microsoft recognizes the need for a more comprehensive SaaS security offering

Table of Contents :

Table of Figures :

Omdia view

Summary

Microsoft is working on the expansion of its security offerings for organizations using software-as-a-service (SaaS) applications, going beyond cloud access security broker (CASB) technology. The expanded scope of technologies the vendor is working on includes

- SaaS security posture management (SSPM)
- Securing integrations with other SaaS apps

Omdia applauds this broader view of the SaaS security requirement on Microsoft's part and wonders whether there might be a need for a new acronym or initialism to describe a broad SaaS security platform, along the lines of the cloud-native application protection platform (CNAPP) acronym for all things related to infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) security.

CASB was the first SaaS security tool

Microsoft has been in the SaaS security market since 2015 with its acquisition of CASB vendor Adallom, which it bought at a time when CASB was a hot topic and startups in the space were the target of M&A activity for many a tech heavyweight. Adallom formed the basis of what is now Microsoft Defender for Cloud Apps.

The CASB boom of the mid-2010s was recognition on the part of security vendors that SaaS adoption was outpacing companies' ability to keep track of which apps were being used by their employees. The ease of signing up for or starting to use SaaS apps meant that line-of-business users could adopt them without the knowledge of their IT department, leading to a phenomenon known as "shadow IT."

CASBs emerged to shine a light into those shadows, providing visibility into SaaS usage across an organization, then fairly quickly evolved to deliver policy enforcement too, in the form of

- Blocking an app altogether
- Limiting its usage to certain individuals or teams within a company
- Restricting what could actually be done with that app (e.g., enforcing encryption of uploads, read-only access, or no copying or printing of data)
- Limiting access to when the employee was in the office, to certain time periods during the day, or to specific geographies

The threat protection aspect

Beyond the discovery of the SaaS apps in use within an organization and the enforcement of usage policies on them, CASBs were also tasked with protecting interactions with the apps, which took two main routes:

- Malware detection, identifying whether anything malicious had been uploaded to the app that would enable threat actors to see and exfiltrate corporate data

- The use of user and event behavior analysis (UEBA) to detect anomalous activity on the part of users, peers, and tenants, indicating that an attack might be underway, then alerting and blocking it

So important were all these capabilities perceived to be that a veritable land grab ensued in the late 2010s, with larger vendors such as Microsoft acquiring CASB specialists to add their technology into a broader portfolio.

As a result, CASBs as a standalone product category have largely disappeared, and the capability has been included in broader security offerings such as secure service edge (SSE, which is not a product but rather a service, bundling CASB, secure web gateway, and next-generation firewall).

Now the SaaS security challenge is broader

After a somewhat frenzied period of M&A in the CASB market, the focus shifted in the late 2010s to IaaS and PaaS security. New types of platforms emerged as innovation picked up that area: after cloud security posture management (CSPM) and cloud workload protection platforms (CWPPs), we have seen runtime API security and, more recently, the likes of infrastructure-as-code (IaC) security and CPM.

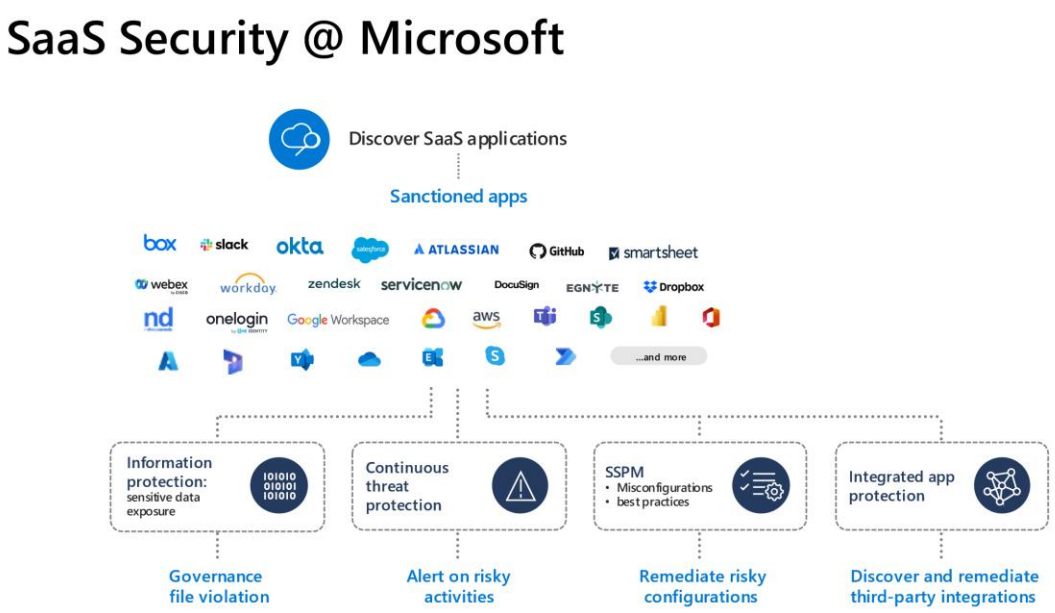
SaaS security, in contrast, was largely restricted to CASB for a number of years. Now, on the other hand, Microsoft identifies a need for a broader portfolio of capabilities to defend organizations from a wider set of threats in their use of SaaS apps.

This is partly driven, of course, by the continued growth in SaaS usage: if CASBs arose to address a first wave of SaaS adoption, the coronavirus pandemic and the changes it wrought on modern work practices have driven a further uptick in the SaaS market. With millions of knowledge workers suddenly switching to work from home because of the pandemic, SaaS apps were often the only way to continue operating, and in this context, the security issues go far beyond shadow IT.

Among the tasks Microsoft now sets for a comprehensive SaaS security platform are

- Information protection: detecting risks of and preventing the exposure of sensitive data
- Continuous threat protection: detecting when an app is under attack and blocking the threat
- Detecting risky configurations and surfacing them for remedial action
- Discovering and addressing the risks involved in integrations with other SaaS apps

1. Figure 1: Microsoft envisages a broader SaaS security requirement



Source: Microsoft

Plans for broad SaaS security

The vendor is addressing each of these requirements with a range of initiatives.

CASB+

For *information protection* and *continuous threat protection*, Microsoft is adding functionality to its CASB, integrating it with its extended detection and response (XDR) technology. Companies can correlate sequences of SaaS events with other security workloads and discover attacks, even when anomalies are hiding in a "noisy" environment with lots of events.

The idea is to create detections based on a combination of additional signals coming from SaaS apps, generating greater confidence in detections in more complex scenarios.

SSPM

For *detecting and remediating risky configurations* and *enforcing best practices*, Microsoft is developing an SSPM capability. This ability to find misconfigurations and recommend remedial action mirrors what is already available in the IaaS and PaaS world with CSPM, and to date it has been offered by dedicated startups. Microsoft's move shows major vendors moving to add the technology to their portfolios.

Visibility and governance for other integrated SaaS apps

While CASBs emerged to help organizations manage risks associated with end users, there is ever more integration of apps via API, so a need arises to secure interactions within the application mesh, monitoring and controlling the way applications interact with each other.

Thus, for discovering and addressing the risks involved in integrations with other SaaS apps, Microsoft's App governance add-on as part of Defender for Cloud Apps enables customers to see how other apps are

interacting with each other at an API level. It surfaces apps that are overpermissioned and accessing Microsoft 365 data through Microsoft Graph APIs. App governance will be relevant for discovering other apps with which an app communicates, assessing their app hygiene, protecting against threats from them, preventing data loss, and imposing governance.

Is a new acronym in the offing?

Omdia applauds Microsoft's vision of a broader security offering for SaaS and suspects that other vendors will need to emulate its offering. We are already seeing other major players talking about SSPM, and protection for other SaaS app integrations is cropping up in more conversations. Indeed, one wonders whether, just as CNAPP has emerged to refer to a broad security platform for IaaS and PaaS, so a similar acronym or initialism might be required to describe the class of offering that Microsoft is putting together for SaaS.

It will be interesting to see how the vendor presents this more comprehensive SaaS security offering to the market. Will it use the "platform" language that we see with CNAPP, whereby each discrete capability can be seen as a module to which a customer can subscribe, or will it simply deliver the uber capability as a single entity? Omdia suspects the former would make more sense, particularly if customers are already using, say, an SSPM from one of the dedicated startups in that field. Stay tuned for an Omdia suggestion …

Appendix

Author

Rik Turner, Senior Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com