Publication date:
02 Feb 2023
Author:
Rik Turner, Principal Analyst, Emerging Technologies

Microsoft is developing a full cloud-native security platform

Licensed Reprint

Brought to you by Informa Tech

Table of Contents :

Omdia view

Summary

There is now a proliferation of security technologies for applications and workloads that reside in infrastructure- or platform-as-a-service (IaaS and PaaS) cloud environments, a.k.a. cloud-native applications. As a result, there is now a move to bring the disparate capabilities under a single umbrella, called a cloud-native application protection platform (CNAPP).

Microsoft is already in the market with a CNAPP, namely Microsoft Defender for Cloud, with three distinct offerings under the hood: CSPM, CWPP, and code security. This report looks at the CNAPP concept and describes how Microsoft's own CNAPP offering is evolving and places it in the context of the wider market for such technology.

The dawn of the cloud-native paradigm

The term "cloud native" or, in its adjectival version, "cloud-native," has been around for a number of years, with many pundits tracing its entry into the vernacular to 2015, when the Cloud Native Computing Foundation (CNCF) was founded. Omdia would actually edit the first part of the name to read Cloud-Native, but then the tech world plays notoriously fast and loose with its hyphen usage (see "open source software" vs. "open-source software," for example). The CNCF itself has a definition of the term, which is a reasonable place to start, but is far from precise. Here is an excerpt:

"Cloud native technologies empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach."

It continues:

"These techniques enable loosely coupled systems that are resilient, manageable, and observable. Combined with robust automation, they allow engineers to make high-impact changes frequently and predictably with minimal toil."

While none of this is wrong, neither are any of the technologies CNFC lists in the first extract cloud-specific: containers and microservices can be deployed on an organization's premises, and APIs are not the exclusive preserve of the cloud. This, the definition is, if you'll pardon the pun, somewhat nebulous, and other definitions that Omdia has seen tend to build out from the CNCF's, which is fine, but we feel the need for a clear one, for our current discussion.

Pre-cloud apps were monolithic and hardware-dependent

For the purposes of this report, therefore, let us say that a cloud-native application is one that is purpose-built (a.k.a. developed) to run in either an IaaS or PaaS environment, or at least using the same methodology and technologies as ones that are, even if it resides somewhere else for all or part of its working life.

Of course, all applications in the cloud, whether created for that environment or migrated from a company's premises, require security. The reason a need arose for the "cloud-native" epithet is that the mass uptake of IaaS and PaaS has resulted in profound changes to how software is developed and how it operates, with those changes still ongoing.

In the pre-cloud era, applications sat on an organization's premises, which by the late 20th century was a dedicated data center, to which all corporate users would connect from their desktop machine each morning. Prior to deploying an application, there would be a provisioning phase, in which the organization would need to provide the hardware (servers, storage, and network) required for its operation, with best practices mandating that scalability be factored in, so that as use of the app grew, there would not be hardware constraints. As a result, overprovisioning was common, at least until server virtualization took off in the early 2000s. And of course, the provisioning process almost inevitably meant a delay of days or weeks.

Furthermore, application architectures were different. Apps were typically monolithic, i.e., self-contained entities that had all the necessary features and routines within themselves that they needed to function.

Cloud-native apps are fragmented by design

Cloud changed, and continues to change, that situation dramatically. Firstly, because there are none of the time lags that hardware provisioning imposed in the on-premises world. Even for apps that organizations are writing themselves rather than buying from independent software vendors (ISVs), the underlying infrastructure enables rapid deployment and scalability. Indeed, initiatives such as the development of infrastructure-as-code (IaC) technology has streamlined the process still further via machine-readable definition files written by the developer.

Furthermore, as organizations have become more comfortable with cloud computing, and specifically with its IaaS and PaaS delivery modes, increasing numbers of them are writing their own application code, both for the sake of speed and, crucially, for competitive differentiation.

The apps they are writing, meanwhile, are increasingly disaggregated, with the organization itself writing only the core functionality and invoking external web services for common functions such as writing to disk, searching a database, presenting a map, or verifying a credit card number. To achieve such functionality, apps use application programming interfaces (APIs), the universality of which in modern app infrastructures has popularized the phrase "the API economy" to describe the current stage in the evolution of cloud technology.

Indeed, the disaggregation shows no sign of slowing down. The virtual machines (VMs) that started life in corporate datacenters and ushered in the world of cloud by their portability to the new environment (the so called "lift and shift" phase of migrating existing apps into the cloud) have in recent years lost their sheen in favor of newer, more compact formats for the compute environment: first containers and now, increasingly, serverless, with the common theme being ever smaller chunks of code, being evoked for ever shorter periods of time. Ephemerality of code is becoming the norm.

Airplanes and spaceships

A useful analogy for the differences between pre-cloud (i.e., on-premises) and cloud applications might be the comparison between airplanes and spacecraft. Planes, of course, travel within the earth's atmosphere, and so must contend with the vagaries of its weather (e.g., headwinds, tailwinds, and storms) and, even more critically, with its gravitational pull. By contrast, after a monumental initial effort to escape from our atmosphere, involving booster rockets and huge amounts of fuel, spacecraft move through the comparative vacuum of space in a gravity-free environment. To return to Earth, they must be able to resist the intense heat generated by re-entry.

Our analogy still holds into the present day. Just as AppDev and the compute constructs it uses continue to evolve, so too does spacecraft construction: where once all returning craft had to plunge into the sea, it is now the norm for them to land on terra firma.

It is also no coincidence that space scientists and engineers have posited the creation of a long-term base on the Moon to build spaceships for long-haul flights, such as to Mars there, since a lunar take-off will be a much easier proposition in much lower gravity (1/6th of Earth's) and no weather. In a sense, containers and serverless are to cloud-native computing what off-planet construction is to space flight, for example, the leading edge of where the technology is going.

The early entrants: CWPP and CSPM

Providing security for cloud-native applications has also been an evolving area of activity over the last decade. The first two approaches that hit the market were:

- **Cloud workload protection platform** (CWPP) technology to deliver security at runtime, detecting and responding to attacks underway against the application, and
- **Cloud security posture management** (CSPM), a more proactive technology that provides visibility into an organization's attack surface, which includes all dependencies, connections, and vulnerabilities across all public-facing assets, via the automated discovery and inventory of connections and assets.

Since they take remedial action on the workload, CWPP platforms are typically delivered via an agent placed on the VM or container (CWPP for serverless environments is still something of a work in progress, given their ephemerality). CSPM, on the other hand, can often be agentless, since it operates in observation mode, alerts to issues that need to organization's attention, and makes recommendations, but typically does not proceed to actual remediation.

CPM and others join the fray

These two cloud security modalities held sway through much of the 2010s, particularly the second half of the decade, when there was considerable M&A activity as specialist start-ups were acquired by larger, broad-based security vendors to fill out their portfolios for the emerging cloud-native security requirement. More recently, however, a second wave of security requirements for cloud apps has spawned a second generation of platforms delivering further functionality, such as:

Cloud permissions management (CPM) – technology that surveys all the permissions (a.k.a. access rights or entitlements) within an organization's cloud estates to detect any overly permissive situations and recommend their curtailment or outright removal. Another analyst firm calls this technology cloud infrastructure entitlement management (CIEM), which Omdia dislikes, both for its wordiness and its proximity to another common acronym in security, namely SIEM.

API security – as API use has become ubiquitous, so too has their abuse, since they enable access to application code. Requests to APIs most be verified as legitimate and blocked if they are not.

IaC checking – with IaC platforms gaining popularity, there is a need to inspect configured cloud resources after that have been deployed to ensure that periodic manual (re)configuration doesn't introduce new issues.

Enter CNAPP

With so many different security technologies emerging for applications residing in IaaS and PaaS environments, it was logical that the advantages of bringing them all under one umbrella would also come to the fore. A bundled offering covering at least the main components described above now has its own name and acronym: a cloud-native application protection platform (CNAPP).

The advantages for the organization using a CNAPP should of course go beyond the simplicity of procurement (the so-called “one-stop-shop” scenario). Yes, it means cutting a single cheque, but more significantly, the various tools within a CNAPP should be able to benefit from each other’s telemetry, findings, and understanding of problems.

Thus, if a CWPP detects a threat that seeks to exploit, say, an excessive right of access, it should be able to call upon the CPM to shut down or at least reduce that entitlement; if it notes that a lot of questionable traffic is coming at the workload via an API, it should have the ability to invoke the IaC to tighten up the rules against which it checks the legitimacy of API calls, and so on. Achieving these goals with tools from a disparate group of vendors may also be possible but would definitely take more work from the customer. With a CNAPP, such functionality should be available “out of the box” and operate seamlessly, offering unified visibility and contextual cloud-native security.

Microsoft is building out its CNAPP

Microsoft has an evolving CNAPP offering called **Microsoft Defender for Cloud**, which currently combines:

- cloud security posture management
- the vendor’s CWPP capability
- since October 2022, a security offering for DevOps, of which more later.

These three capabilities are presented as an integrated platform enabling customers to protect the lifecycle of an application from development to runtime, with the protection spanning the applications themselves, their infrastructure, and the underlying data.

CSPM

Defender for Cloud starts with the vendor’s CSPM technology, Defender Cloud Security Posture Management (CSPM), which can be agentless and comes with a contextual engine. While the agent-based version of the platform currently has extra functionality such as virus scanning, Microsoft is closing the gap and plans to bring the agentless one up to parity soon, though of course, remedial action is only possible with an agent-based approach.

The agentless deployment can already do vulnerability assessment and management, leveraging the Microsoft Defender Vulnerability Management, which is built into the platform. Meanwhile the agent-based alternative can also integrate with third-part tools for this purpose, such as Qualys.

Both versions do post facto alerting, with focused recommendations for the customer to act, with some issues resolvable from the CNAPP’s dashboard, such as blocking public access to a cloud storage instance.

Alerts can be correlated in Sentinel (Microsoft's own cloud-based SIEM) or in third-party SIEMs, the difference being that with Sentinel the communications as bi-directional. The CSPM platform's recommendations can also be used to populate SOAR platform.

Defender CSPM gains permission from the admin to perform its reconnaissance. It benchmarks a customer's cloud (or multi-cloud) estate, discovering all their assets, discovering all their data stores, and identifying which data is sensitive, then and performing attack path analysis to understand how malicious actors could get to them and map out potential lateral movement paths. It further highlights all the contextual cloud security insights associated with these paths, which enabling it to prioritize which are the most important issues the customer needs to address and make recommendations about remediation.

In this context, customers can query Defender CSPM's cloud security graph by vulnerability, resource type, etc., to further inform their prioritization decisions. The platform can also correlate its inside-out view of a customer's security posture with the external attack surface management (EASM) information provided by RiskIQ (acquired by Microsoft in August 2021)

CWPP

Defender for Cloud also has a CWPP component for runtime app protection, delivering remedial action via the vendor's Azure Arc agent on the workload. It protects:

- Compute—virtual machines (VMs), servers, app services, and Kubernetes.
- The Service Layer—Resource Manager, Key Vault, Azure DNS.
- Databases and Storage.

The vendor stresses that its CWPP capability works in Azure, AWS, GCP, and on-premises environments, with data being amassed via the Azure Log Collector and common management of the workloads as if they were all part of an Azure subscription.

The platform sends alerts, which are a summary of repetitive, suspicious events that the customer should investigate. These events can take place on databases, containers, Kubernetes, virtual machines, or on the cloud control plane, for example, in the DNS layer. They may also be a sequence of potentially malicious events involving the PowerShell task automation and configuration management program. Microsoft has implemented the MITRE ATT&CK Framework methodology for describing and understanding threats, enabling customers' security teams to work on these alerts, contextualizing and prioritizing them accordingly.

The CWPP component also feeds its insights into the CSPM part's cloud security graph to further inform analysis there, and workloads are scanned using the same agentless vulnerability scanning capability.

DevOps security was unveiled at Ignite 2022

However, Microsoft's CNAPP plans clearly go further than that. The vendor describes its CNAPP as both multi-cloud *and* multi-pipeline. This shows that, from the outset. it is thinking about cloud-native security from a proactive stance, including shifting left, for example, addressing any problems within an app in the development pipeline rather than after it has been put into the production environment.

It is in this context that the company announced Defender for DevOps, at the 2022 edition of its annual Ignite conference. The platform debuted supporting both the Azure DevOps (ADO) and GitHub environments, the latter of which was acquired by Microsoft in 2018. In other words, it has the ability to scan all new scripts coming into the repository, which includes looking for any secrets the developer may have inadvertently left in the code. Other major developer platforms are on the product's roadmap.

Defender for DevOps also performs IaC checking, supporting the two most widely used IaC platforms of Terraform and CloudFormation, as well as the Azure-specific Biceps language for deploying resources. The platform also comes with integrated workflows that make it possible for security issues to be addressed as a single procedure within the developer's preferred integrated development environment (IDE).

Still to come within Defender for DevOps is the ability to scan for vulnerabilities during the code-to-cloud contextualization process, for example, the point at which a generic workload, created according to a master image, is injected with instance-specific settings during the deployment phase. The idea is that, if a vulnerability is detected at that point and the platform identified it as critical, that will be reflected in the Microsoft Security Graph interface.

Omdia sees the inclusion of Defender for DevOps within the broader Microsoft Defender for Cloud as an important differentiator in the current stage of evolution of CNAPPs, many of which have so far focused only on runtime protection, for example, once the app is in production. By adding the DevOps dimension into its CNAPP, Microsoft is making it possible for organizations to connect insights coming from the "left side" (i.e., the development pipeline) and the "right side" (the production environment) of their application lifecycle. This should result in improved visibility and a reduction in the amount of time and cost required to remediate vulnerabilities and misconfigurations.

The vendor's avowed intent is to empower security teams, developers, and resource owners to collaborate toward security posture improvement, connecting disconnected worlds (code and cloud) that have different platforms, agendas, and taxonomy.

Permissions management is coming to the CNAPP

Having acquired the pioneer and market leader in CPM, CloudKnox, in mid-2021, Microsoft already offers the capability as a standalone service within Azure. The technology already supports multi-cloud environments, and the next step will be to integrate it into the broader CNAPP offering.

Conclusion

Defender for Cloud is Microsoft's cloud-native application protection platform (CNAPP), designed to deliver security throughout the lifecycle of an application, from the development phase on into its time in production. It offers both agentless and agent-based vulnerability scanning to underpin flexible protection strategies and provide efficient deployment of remediation, spanning both code and runtime.

CNAPP is clearly the direction of travel for technology that secures IaaS and PaaS workloads, and Microsoft has made a good start en route to a comprehensive CNAPP offering with Defender for Cloud. Clearly there is more to come: the vendor is already talking about "in-account scanning," (i.e. enabling customers to run all the scans the platform performs, but in their own environment), rather than needing to connect to the nearest Azure point of presence (PoP). Omdia expects to see further capabilities appearing within the Microsoft CNAPP in the near future.

Microsoft has made a commitment to heterogeneity in its cloud security offerings, recognizing that the multi-cloud world is by now a reality, and indeed that it represents an opportunity for the vendor to grow its own, already substantial, security business. As Defender for Cloud approaches the status of a fully-fledged CNAPP, it will be interesting to see how it fares in the market against CNAPPs from dedicated cybersecurity vendors who are not cloud service providers (CSP) as well. What is clear already is that, for existing Azure customers, it is a compelling offering, given that it can provide cloud-native security in a single dashboard across their Microsoft and third-party CSP environments.

Appendix

Further reading

2023 Trends to Watch: Infrastructure Security (November 2022)

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.

CONTACT US

omdia.com

askananalyst@omdia.com