OMDIA MARKET RADAR

Publication date
February 2022

Author
Rik Turner, Principal Analyst
Rob Bamforth, Associate Analyst

Omdia Market Radar: Cloud Permissions Management (CPM)

Brought to you by Informa Tech

Omdia view

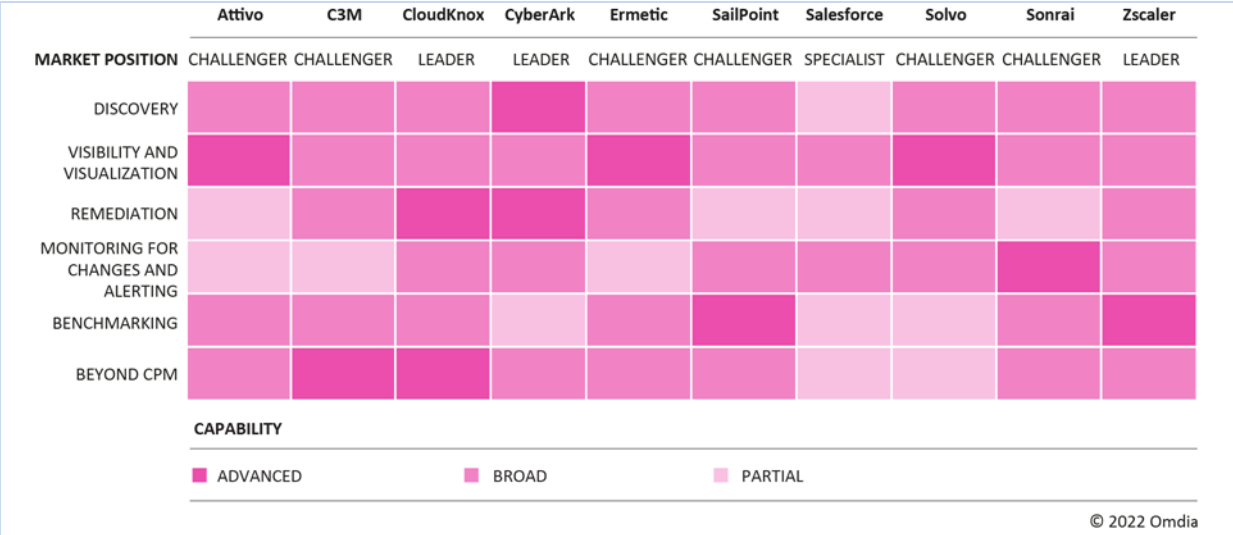
Summary

Securing the infrastructure- and platform-as-a-service (IaaS and PaaS) delivery modes for cloud computing is still very much an evolving art, not least because they themselves are still developing and changing. What is clear already, though, is that while one essential element of any defensive strategy is reactive (i.e., detecting and blocking attacks that are underway), there is increasing interest in proactive approaches, namely reducing the attack surface before any attack takes place.

CPM is an example of this mindset, and has gone from the preserve of dedicated start-ups as recently as early 2020, to a capability now offered by a range of tech sector heavyweights, including no less a player than Microsoft. This report looks at the evolution of this technology, considers the strengths and weaknesses of a number of the vendors in this space, and makes predictions as to where CPM is going over the next few years.

As such, it is of interest to any enterprise that is developing and/or using application code in IaaS and PaaS environments. CPM can help them shrink their attack surface in the cloud and free their security team to focus on attacks that make it through their defenses.

Figure 1: The cloud permissions management vendors covered in this report



Source: Omdia

IaaS and PaaS have overtaken the SaaS market in size

A history of cloud computing would probably consider its current stage of development as at least the second or third cycle. The first saw the explosion of software as a service (SaaS), which not only promised organizations a replacement of capital expenditure with operating expenditure (i.e., opex instead of capex), but also enchanted individual business units with the ease of adopting new applications without the need to work with, or even consult, their IT teams. No long provisioning processes for hardware or software were required: you just signed up, uploaded the relevant data, and were good to go.

The poster child for this phase of cloud adoption was, of course, Salesforce, back when it was still called Salesforce.com, but thousands more SaaS offerings have followed in its wake, not least the entire office productivity suite Microsoft now offers as a cloud service, called Microsoft 365.

However, as organizations have become more comfortable with the cloud, their ambitions have grown, and rather than just consuming readymade cloud applications, a growing number of them have taken to developing their own code for the cloud. In that scenario, they can choose the option of:

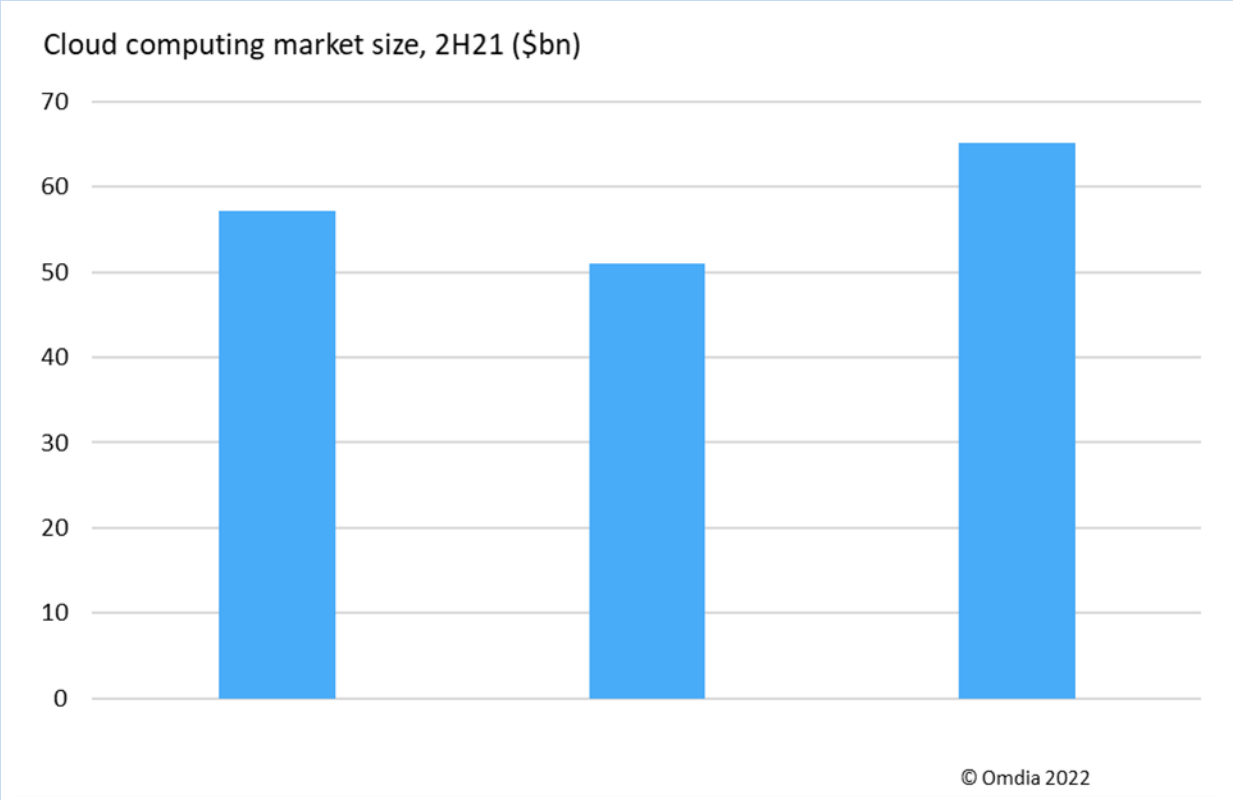
- Being responsible for the application “stack” from the operating system on up, thereby maintaining a greater degree of independence from their cloud service provider (CSP). This is IaaS route, or
- Taking responsibility for the data and applications in the stack, relying on the CSP for everything up to and including the runtime environment, thereby trading independence from the CSP for greater ease and speed of development. This is the PaaS route.

Microservices accelerate code production

What IaaS and PaaS have in common, of course, is that the organization adopting them has a deeper engagement with the cloud service: in other words, its responsibility goes beyond the data, to the actual application code that it is using in the cloud. Some of this code will come from an independent software vendor (ISV) such as SAP or Oracle, with the application having been migrated from an on-premises deployment into the cloud. However, a growing number of organizations are also developing their own code for the cloud, and doing so at an increasing rate, thanks to procedural trends such as Agile development and the adoption of DevOps methodologies.

Omdia's market sizing had SaaS as the largest part of the overall cloud services market through the latter years of the 2010s, with both IaaS and PaaS growing at a faster rate but from smaller bases. The impact of the coronavirus pandemic, when companies were suddenly forced to accelerate digital transformation projects to address the sudden changes it imposed, has accelerated still further their expansion, to the point that together they have now overtaken SaaS in total market size.

Figure 2: Omdia's estimate for the size of the IaaS, PaaS, and SaaS markets



Source: Omdia's Cloud Colocation Services Market Tracker, 2H21

If the adoption of IaaS and PaaS constitutes the second wave of cloud computing, then a third wave—happening in tandem with the second in recent years—has seen the emergence of cloud workload formats beyond virtual machines (VMs). These new formats coming in over the last few years are, in the first instance, containers, and thereafter, serverless computing. Their adoption marks a shift from coarse-grained units of code and apps to fine-grained ones, resulting in a huge increase in scale and variety of sources, but thus also increasing supply chain complexity.

Collectively referred to as microservices, these new formats tend to accelerate still further the application development (AppDev) process. However, with this speed of innovation comes increased risk.

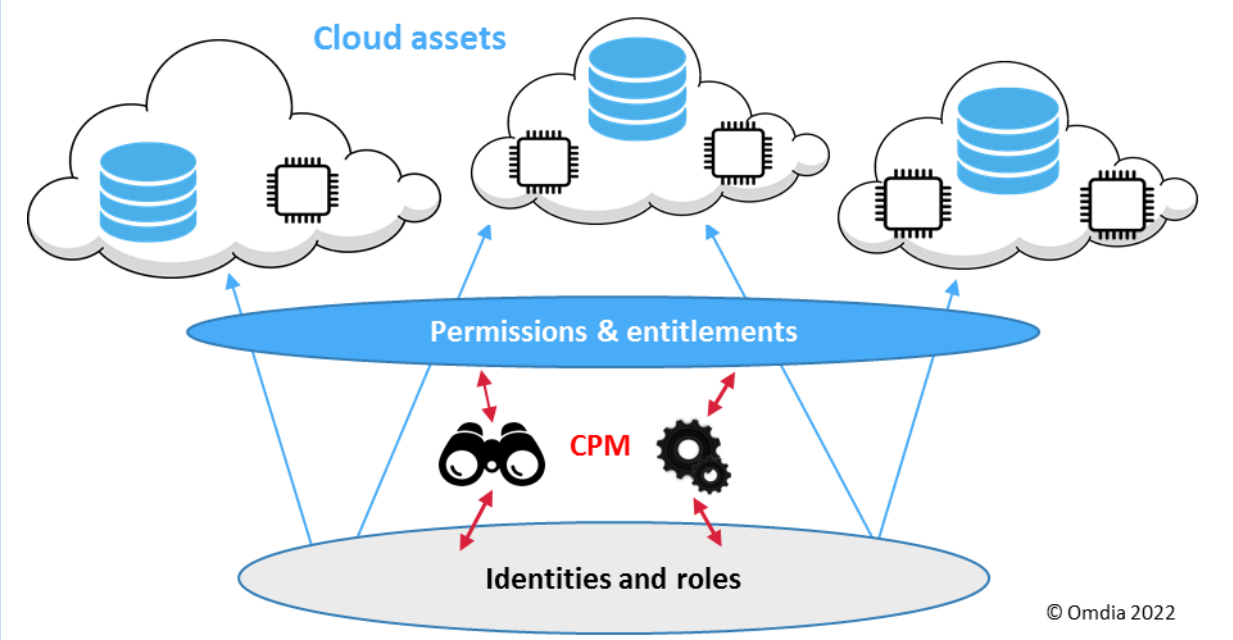
CPM is part of the proactive trend in cloud security

From a security standpoint, the acceleration in AppDev means more code to protect, with less time to do it before another update—and thus another version—goes into production. Obviously, part of that protection must involve defending the code against the attacks that will inevitably come.

However, given the burgeoning volumes of code going into production and the finite resources (particularly of the human variety) that organizations have at their disposal to mount those defenses, Omdia detects a growing interest in proactive measures that can reduce attack surfaces before any exploits can take place. In other words, if potential “holes” in an organization’s defenses can be detected as early as possible, ideally even before an attack has taken place, the work of its security can be reduced, enabling a greater focus to be given to the assaults that do still happen against the smaller attack surface.

CPM is one such proactive approach.

Figure 3: How CPM reins-in cloud permissions



Source: Omdia

CPM sets out to impose the principle of "least privilege" on an organization's cloud permissions estate (i.e., the extant access rights to cloud assets), looking at all the human identities within its corporate directory, as well as any non-human identities such as service accounts. Having created an inventory of all these permissions (also known as access rights or entitlements), it analyzes them to determine which are excessive or indeed completely unnecessary, then recommends how they can be curtailed. Some CPM platforms can even go further and perform that curtailment in an automated fashion if the customer is comfortable with that.

CPM aims to address permission sprawl in cloud computing

The rationale for such activity is the so-called "permission sprawl" that characterizes most organizations' cloud estates. For instance, with development teams busy writing and delivering new code, it is frequently the case that access rights to a given cloud asset (i.e., a workload or data store) are granted to a developer while they are working on an application, but are not revoked when the app goes into production. Workloads themselves may also be granted rights at certain points in the lifecycle, which should be curtailed prior to going into production.

Another such issue is when a developer leaves an organization, some permissions may not be deactivated because the security team is not even aware of their full extent. And sometimes a developer inherits access rights they don't need simply by joining a team working on a particular project.

In other words, the DevOps environment is often overly permissive, leaving security holes that a threat actor can exploit if they manage to penetrate the infrastructure and carry out reconnaissance on who can access what. Similarly, one system can often access other systems, and many of these permissions may not be necessary, creating another vulnerability within the infrastructure.

Thus, imposing a least-privilege stance in the environment can significantly reduce bad actors' opportunities to launch attacks. This proactive approach on the part of CPM platforms places the technology in the category of zero-trust zeitgeist currently sweeping through different areas of cybersecurity.

Other names for CPM

It is worth noting here that CPM is known by other names at different analyst firms. One leading house came up with cloud infrastructure entitlements management (CIEM) after Omdia had coined CPM. The CIEM name has various negative aspects:

- In its full form, it is longwinded, and CPM perfectly encapsulates the essence of what this technology does.
- In its acronym form, it is confusingly similar to another staple of the cybersecurity market, namely security information and event management (SIEM).
- Because SIEM is often pronounced "sim," this leaves people wanting to talk about CIEM scratching around for an alternative. Omdia has heard it pronounced as "kim," which may work in Gaelic, which has a hard C before both I and E, but is counterintuitive in English.

For all these reasons, Omdia shuns CIEM, but we highlight its existence here because it has been widely adopted, and indeed will appear in a couple of the vendors' illustrations later in this report.

Another analyst house calls this technology cloud identity governance (CIG), which certainly points to its affinities with identity governance and administration (IGA); a sector whose leader, SailPoint, has, of course, ventured into CPM. However, we consider this appellation insufficiently precise, nay woolly, in that it has no explicit reference to access rights, entitlements, or permissions.

The scope of this Market Radar

CPM as a technology category traces its origins back to the second half of the 2010s, when various start-ups were founded to deliver this capability:

- The pioneer was CloudKnox, which was founded in 2016, while
- Sonrai was founded in 2017,
- C3M in 2018,
- Ermetic and Trustdome in 2019, and
- Solvo in 2020.

All these vendors are featured in this report, although two of them were acquired by larger tech industry players in 2021: Zscaler acquired Trustdome, while Microsoft bought CloudKnox. Meanwhile, SailPoint, the market leader in IGA, bought two companies, Orkus and OverwatchID, in October 2019, merging their technology to become its Cloud Access Management product, launched in March 2020.

In addition, as the need for and desirability of CPM became apparent across the security sector, other industry heavyweights have joined the fray with technology they developed in house, namely

- Privileged access management (PAM) market leader CyberArk, in 2020, and
- SaaS and PaaS giant Salesforce, also in 2020.

Also entering the market was a smaller security vendor, Attivo, which made its name in deception technology in the 2010s and has since broadened its offering into Active Directory and endpoint security.

Criteria for scoring CPM vendors

Discovery

This is about how the platform builds an inventory of identities and entitlements. We consider the degree to which it finds every identity, human or non-human, native and federated, and all related resources and entitlements, as well as account activity.

Visibility and visualization

With so much information to understand, this looks at how the product helps users to visualize the problem. Does it provide a graph view, mapping identities to resources? Can security team users query entitlements via a natural query language, or is there a dashboard to track entitlement usage, user behavior, and so on? Scores are awarded on the clarity of visualization, its comprehensiveness, range of viewpoints, and the ease with which users can switch between different viewpoints.

Remediation

This criterion judges the product on its remediation capabilities. How much information and detail are provided to guide customers? How well does it build or fit into existing workflows? Is there is any prioritization of remediation suggestions? Does the platform offer automation of the remediation process, and how can users feel confident in the automated approach?

Monitoring for changes and alerting

After an initial rightsizing effort, a CPM platform should also deliver continuous monitoring of a customer's permissions estate to detect and track any further signs of sprawl initiated via changes to their settings, alerting on such risks and again providing remediation suggestions in the form of JSON code. This criterion scores the vendor on how well developed this capability already is in the platform.

Benchmarking re industry peers and best practices

This criterion looks at the product's ability to make comparisons, either with other organizations or with identified best practices and industry benchmarks. Some vendors will include templates, workflows, and other models to allow users to see how compliant they are with industry and broader initiatives.

Beyond CPM

This criterion scores vendors from two perspectives:

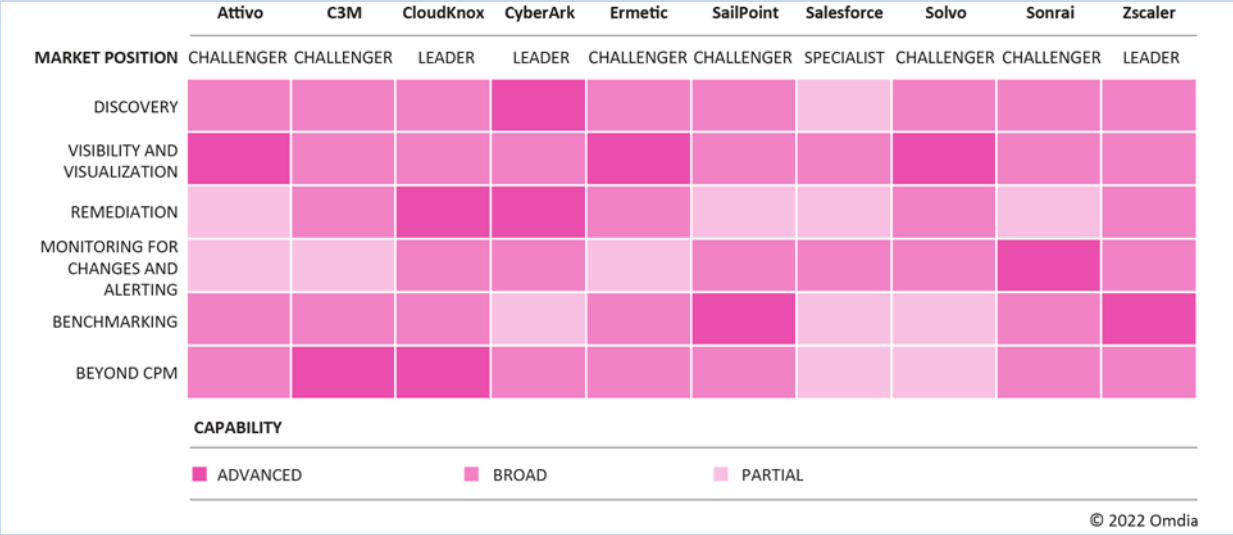
- First: On the breadth of their existing integrations with other security tools. Examples are IGA, PAM, cloud security posture management (CSPM), or endpoint security.
- Second: On the vendor's plans to develop their own technology in contiguous areas of security.

Omdia Market Radars represent a benchmarking exercise, which is usually performed on less mature markets, while sectors that have been in existence and have developed for longer, such as firewalls or identity management platforms, are considered in a different type of report, namely an Omdia Universe.

As such, a Market Radar uses more coarse-grained criteria to provide an early look at how a sector is evolving and who Omdia considers the current frontrunners are. It does not include a facility for weighting the individual criteria. If it did, we would have given extra weight to Beyond CPM because

- The range of technical capabilities of each platform is fairly standard, and most of the products under consideration meet the majority of these requirements, which means stark differentiation between them is difficult, and
- Omdia believes CPM will not remain a standalone capability within cloud security for very long. Indeed, there are already signs that it is merging into broader portfolios. We consider this a desirable outcome, given the breadth of organizations' requirements for securing their cloud assets, and so have sought to reward those vendors whose roadmap and vision impressed us in this context.

Figure 4: The CPM vendors in this report



Source: Omdia

As the above figure shows, we have scored the vendors on a range of criteria, resulting in a ranking where we have three Leaders, six Challengers, and one Specialist. It is worth noting, however, that

the technical differences between the groups were minimal, in that any CPM platform must bring a certain set of capabilities to the table, such that one or two of our Challengers were very close to being Leaders. That said, here is our rationale for the rankings:

CloudKnox (now part of **Microsoft**) is the clear Leader, for a couple of reasons. Firstly, because CloudKnox itself was the first start-up devoted to the development of this technology and had built a considerable reputation in the field as a result: the exact sizes of customer bases are difficult to judge in a largely privately-held sector, but we believe it has the largest, or at least a leading share. Secondly, we were impressed by the company's vision for where it wants to take its tech offering (i.e., the "Beyond CPM" criterion).

Thirdly, because it now has the market clout and resources of Microsoft behind it, yet the new owner has stressed that it does not intend to make the CloudKnox technology work only on the Azure cloud platform. In other words, it will continue to support all the leading cloud providers, which we consider essential for CloudKnox, but also a winning strategy from Microsoft, in that heterogeneous security is a powerful argument when preaching the benefits of multicloud and so persuading customers of market leader Amazon Web Services (AWS) to consider trying other providers.

CyberArk is also a Leader here, not only because of its technical capabilities but also thanks to the way it is taking its CPM technology to market. In other words, it can be acquired as a standalone, independent of its flagship PAM platform, but is also a logical add-on for any PAM customers. Given CyberArk's dominant position in PAM, this bodes well for its ability to corner a significant share of the emerging CPM market.

Finally, **Zscaler** is ranked as a Leader. Even though it bought a less mature technology platform with Trustdome, Omdia was impressed by the vendor's vision for where it wants to take its cloud security offerings. In addition, its existing strength in cloud-delivered security leads us to believe it will build the customer base, at the very least through the upsell opportunity.

As for the dedicated start-ups, it should be said that they all ticked all the relevant boxes for CPM functionality, and their Challenger status relates not to their technical capabilities, but their ability to execute on the global scale that is now warranted by the entry into the market of big guns like Microsoft.

C3M, for instance, ranked as a Challenger, though it was close to making it into the Leader category. Omdia liked where the company has come from with its CPM offering and very much appreciated where it is going with its product roadmap. Similarly, the dedicated CPM start-ups **Ermetic**, **Solvo**, and **Sonrai** also ranked as Challengers, with the colors in the heatmap explaining what we considered to be their greatest strengths. As start-ups, however, all these companies need to redouble their efforts to gain and retain visibility in the market, particularly as CPM goes more mainstream with the entry of tech heavyweights.

The other Challengers were **Attivo** and **SailPoint**. Both are established vendors in other areas of the security market, and both have upsell opportunities for CPM in their respective customer bases.

Salesforce is classed as a Specialist vendor here, the reason being that it has no intention of offering its CPM technology for use on third-party clouds (i.e., it will only be offered to customers of any of the multiple Salesforce services). That is not an insignificant potential market, however, as the

vendor has some 150,000 customers globally, representing a massive upsell opportunity. That said, organizations whose cloud estate spans multiple clouds won't be able to use Salesforce's CPM platform there, even if they are using it on any Salesforce instances they may have. Thus we do not see Salesforce as a "player" in the CPM market per se.

Honorable mentions

While the Leaders in this report have already been highlighted for their market clout and growth potential, we would also like to call out for honorable mention three of the other vendors covered, in each case for different reasons.

Attivo: Ploughing its own furrow with CPM

Attivo comes at CPM from a completely different perspective. It is not a start-up and neither is it a cloud-native vendor. Instead, it has an established background in the on-premises world, a situation which naturally leads it to focus on securing the hybrid world that will predominate in enterprise infrastructure, at least for many years. Rather than pursuing a CNAPP strategy (see below), it offers CPM for integration with its existing security capabilities for hybrid environments.

Omdia applauds this approach, not only as a sensible extension of the existing Attivo portfolio, but also as a smart move, for as Omdia never tires of reminding its subscribers—if the future is cloud, the foreseeable future is definitely hybrid.

C3M: Clarity of cloud security vision

C3M impressed us with its clarity of vision for CPM, firstly because it had already developed CSPM and so added CPM to enhance that capability, and secondly because it started out with a broader roadmap that includes other essential cloud security capabilities. In short, it was talking about a CNAPP offering (see the next section) even before that acronym had been coined.

As such, Omdia expects C3M to do well in the cloud security market provided it can raise awareness of its brand and product offering in this increasingly crowded space, where it must compete with vendors with considerably deeper pockets to fund their marketing activities.

SailPoint: Using CPM to differentiate its IGA offering

SailPoint is the recognized market leader in identity governance and administration (IGA), one pillar of which is entitlements management, so the vendor's extension of that capability into cloud permissions management was both a sensible move and a differentiator vis-à-vis its leading IGA competitors, who are mostly exploring partnerships with one or other of the dedicated CPM vendors.

Thus, having CPM as an extension of its own entitlements management capabilities sets SailPoint apart in the current IGA landscape. While it may not focus on winning many greenfield CPM deals, the vendor should certainly enhance its position with its existing IGA customers, with CPM as a logical upsell opportunity there.

Where the CPM market is headed

Before we pass to the profiles of the individual vendors in this report, a word about where Omdia sees the CPM market going.

Firstly, we do not see CPM as a product category that will remain standalone in the long run. Just in terms of IaaS and PaaS security, there are already a handful of disparate products, such as:

- Cloud workload protection platforms (CWPP): Providing runtime security for workloads by detecting and blocking attacks that are underway.
- CSPM: Adopting a more proactive stance of surveying an organization's cloud assets, detecting where one or other of them has strayed outside the bounds of compliance with particular regulations (e.g., PCI DSS, HIPAA, or GDPR) or has undergone any configuration change that has introduced vulnerability, then recommending how the asset should be returned to "factory settings," bringing its configuration back into line with what it had when it left the development pipeline.
- Infrastructure-as-code (IaC) checking: As the runtime environment for a given workload can now be created by code, this capability checks that the coding has not introduced any additional vulnerabilities and sends an alert if it has.
- API security, providing both code checking in the development pipeline to make sure the API is secure, and inspection of all API calls in runtime to detect and block any security exploits against the interface once it is live.

Each of these security tools started life in isolation (i.e., developed and marketed by dedicated start-ups). However, there has been extensive M&A activity already in this market segment, such that, while some single-product vendors continue to exist, there is a growing trend for vendors to offer some or all of these capabilities as part of a comprehensive portfolio. There is even a name for such portfolios: **cloud-native application protection platforms** (**CNAPP**s).

CPM is definitely another capability within the spectrum of a CNAPP, and indeed, while some M&A activity such as Zscaler's acquisition of Trustdome already points in this direction, other vendors in this report, such as C3M, are going it alone, developing a whole range of products to underpin a CNAPP offering.

It is a moot point whether CNAPP offerings will, or indeed should, extend beyond IaaS and PaaS to include SaaS security also. That would entail adding other capabilities such as the well-established **cloud access security broker** (**CASB**) technology, as well as the newly emerging category of **SaaS security posture management** (**SSPM**), which is akin to CSPM but for SaaS instead of IaaS and PaaS.

What is clear, however, is that CPM is an integral part of a comprehensive CNAPP offering, and Omdia predicts that few CPM vendors will be able to plow the CPM furrow in isolation for much longer.

The vendors

The report covers ten vendors in the CPM market, six of whom are start-ups that came into existence specifically to create the technology (one actually started in CSPM and expanded into CPM), while the other four are larger technology vendors who have added a CPM capability. And to complicate matters further, one of the six start-ups was itself acquired by a tech giant last year (Microsoft bought CloudKnox), while one of the four industry majors added CPM through the acquisition of a start-up that was so new in the market that its name has not survived under the new management (Zscaler bought Trustdome).

CloudKnox (now part of Microsoft)

CloudKnox was the first entrant in the nascent CPM market and was acquired by Microsoft in July 2021. Its Permissions Management platform manages the entire privilege lifecycle across any private or public cloud infrastructure.

Why put CloudKnox on your radar?

CloudKnox Permissions Management continually monitors the actions of every identity (both users and workloads) on every resource across any cloud and enables customers to implement the principle of least privilege with one unified operating model across clouds. It also alerts customers to the first signs of potential danger for anomalies and suspicious behavior. Features such as rapid deployment and one-click remediation make CloudKnox a serious contender for IaaS and PaaS security projects, especially now that it is part of the Microsoft fold, which adds presence, depth of support, and enhanced route to market options.

Product/service overview

CloudKnox Permissions Management is a SaaS offering. It is comprised of two components: a collector service and a SaaS service.

CloudKnox collector service

The main purpose of this is to collect activity and attribute data (from the clouds and identity providers) and act as a controller to make the necessary changes. There are two ways a customer can deploy it:

- In the form of a small Linux VM installed in the customer's cloud infrastructure environment, with one appliance required per cloud platform, such as AWS, Microsoft Azure, GCP, and VMware vSphere.
- By configuring the CloudKnox platform to connect directly to the customer's public cloud infrastructure environment (AWS, Azure, and GCP).

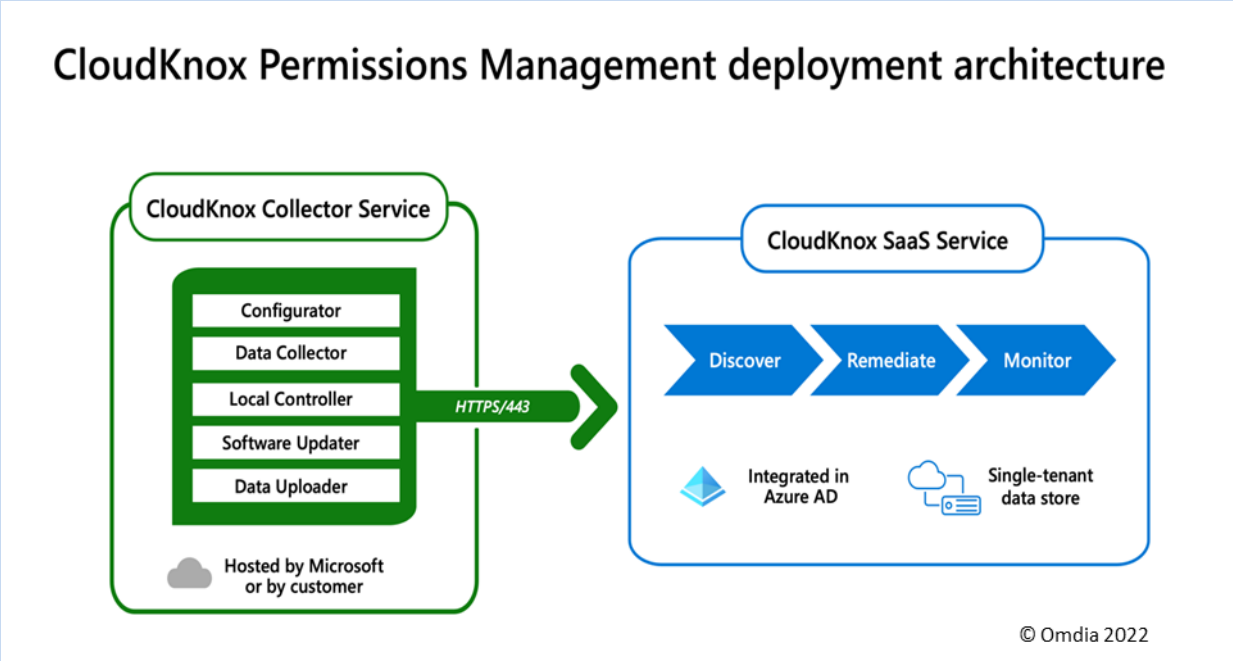
CloudKnox SaaS service

This is the main interface for customers to manage permissions (visibility, remediation, and monitoring) of all identities across the cloud infrastructure.

CloudKnox Permissions Management prides itself on its quick and easy setup. The collector service builds activity profiles for each identity, resources, and action based on the historical 90-day data

set, which it then maintains on a rolling basis, and customers can implement the principle of least privilege for all identities and resources in their cloud infrastructures. Organizations can then automate and simplify the provisioning and right-sizing of permissions.

Figure 5: The CloudKnox architecture



Source: CloudKnox

Permission Creep Index

The Permission Creep Index scores a customer's risk posture to help evaluate risks associated with the identities in its infrastructure. The index has a range from 0 (low risk) to 100 (high risk), where scoring 100 means that there are many unused permissions and high risk. The number can be adjusted based on what permissions are being used, enabling customers to enforce the principle of least privilege, regardless of the infrastructure being used.

Acquisition by Microsoft has opened up a number of avenues for integration, including Microsoft's SIEM, Sentinel, and endpoint protection, Defender, as well as other systems. It also increases positive sentiments towards the adoption of automation. CloudKnox has noted that the time it takes customers to switch over from manual to automated remediation has been falling, but in its early years, it would generally take around a year of consideration to build trust and comfort in the approach. The Microsoft brand adds significant big-name credibility, which should embolden and encourage more customers to move more quickly to automation.

Company information

Background

CloudKnox was founded in 2016 and formally launched in 2017 by CEO Balaji Parimi. Parimi was previously VP of engineering and operations at CloudPhysics, a SaaS platform for optimizing IT management in data centers. CloudKnox's VP of engineering is Ravi Adusumilli, who was previously VP of engineering at CloudPhysics. Raj Mallempati joined CloudKnox Security as COO, where he is responsible for CloudKnox's overall business and go-to-market strategies. Prior to joining CloudKnox, Mallempati was most recently the SVP of marketing at Malwarebytes. John Donnelly completes the executive team as VP of sales. Before joining CloudKnox, Donnelly served as a partner at Wing; a purpose-built venture capital firm focused on early-stage long-term investments.

In June 2021, CloudKnox was selected as one of the World Economic Forum's 2021 "Technology Pioneers," which is where the Forum identifies early to growth-stage companies involved in the use of new technologies and innovation that is expected to have a significant impact on business and society.

CloudKnox was acquired by Microsoft in July 2021.

Current position

CloudKnox launched its SaaS offering, CloudKnox Permissions Management Platform, in October 2018. The platform was launched for on-premises VMware-based ESX deployments and the three big public clouds (AWS, Azure, and GCP). It helps enterprises implement and enforce the principle of least privilege across clouds by removing the complexity associated with managing the exponential growth of machine identities, services, privileges, and resources.

CloudKnox charges an annual subscription, which is based on the size of the customer's cloud deployment (the number of compute or RDS instances it is operating). CPM is still at an early stage in its evolution, as is the competitive landscape, although notable competitors include Prima from Palo Alto Networks, CyberArk, Ermetic, and Sonrai Security. CloudKnox believes one of its key differentiators is its remediation mechanism along with Permission on Demand / Just In Time Permission, something it does not see from the competition. CloudKnox also developed the Activities-Based Authorization protocol on which its platform operates, and it has patents in this area.

Prior to acquisition, CloudKnox had several F100 companies deployed at scale for AWS, Azure, GCP, and VMware vSphere across different verticals as paying customers, ranging from large to midsize enterprises, mainly in the US. It went to market entirely through channel partners. Now, as part of Microsoft, it has global scale and expects to grow its presence and sales in other parts of the world, especially in Europe.

Key facts

Table 1: Datasheet—CloudKnox

Product/service name	CloudKnox Permissions Management Platform	Product classification	Cloud permissions management
Version number	n/a (SaaS platform)	Release date	October 2018
Industries covered	Financial services, healthcare, telecoms, professional services, pharma/medical devices, energy, and technology verticals	Geographies covered	Global
Relevant company sizes	Enterprise and large enterprise customers that have public and/or private cloud infrastructure	Licensing options	subscription
URL	Cloudknox.io	Routes to market	Through Microsoft and channels
Company headquarters	Sunnyvale, California, US* *HQ and employee count are pre-acquisition and will be subject to change	Number of employees	50*

Source: Omdia

Appendix

Further reading

Fundamentals of Cloud Permissions Management (CPM) (January 2022)

Omdia Market Radar for Next-Generation Application Security: Pipeline (Pipeline NGAS) (July 2021)

Cloud security – IaaS and PaaS (December 2019)

Author

Rik Turner, Principal Analyst, Cybersecurity

Rob Bamforth, Associate 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

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