Ovum
TMT intelligence | informa

Microsoft's Expanded Horizons in Security

Securing Azure remains front and center, but hybrid and multicloud security is the way forward

Publication Date: 02 Apr 2019 | Product code: INT003-000345

Rik Turner

Summary

Catalyst

Microsoft's development of its security offerings has, until now, been designed to reinforce the appeal, first of its operating system, database, and office productivity software and more recently of its cloud services. While this remains the core driver of its activities in security, there are signs of a broadening of its approach of late as it moves to support heterogeneous environments and the environments of competing cloud service providers (CSPs).

Most significantly, in the run-up to the recent RSA Conference on cybersecurity, held in San Francisco March 4–7, 2019, the company launched Azure Sentinel, a security incident and event management (SIEM) platform it is offering as a cloud-based service, and a managed threat-hunting service called Microsoft Threat Experts.

The SIEM-as-a-service (SIEMaaS) offering in particular takes Microsoft into the world of heterogeneous security management.

Ovum view

Microsoft has already expanded successfully from being a vendor of software licenses to providing the whole spectrum of cloud services, which include infrastructure- and platform-as-a-service (IaaS and PaaS) with its Azure business and software-as-a-service (SaaS) with its Microsoft 365 portfolio. In making that journey, the vendor has also recognized that security is an integral part of being a CSP, and it has invested accordingly in both internal development and acquisitions.

However, if until now Microsoft's rationale for developing a robust security offering has been to make its Azure offerings worthy candidates for enterprise customers, Ovum has of late detected a slight change in its thinking. Of course, supporting the Azure sales pitch remains key to its security strategy, but as the enterprise world goes from private cloud to hybrid and on into multicloud infrastructures, it sees an opportunity. If one of the multiple CSPs used by an enterprise is Azure (and it is already second in the market behind AWS), Microsoft has a chance to provide security technologies into that account. And if it does so, it will need to support operating systems and platforms beyond the world of Windows, which it is already starting to do with its security offerings.

Ovum sees clear signs of Microsoft's taking this direction, most notably in its launch of the SIEMaaS offering, Azure Sentinel. This move not only moves the company in the direction of security management across multiple different environments (i.e., beyond Windows and Azure) but also positions the company to be a force for change in a SIEM market that is ripe for disruption at the moment.

Key messages

- Microsoft offers technology in four areas of security and is building a partner ecosystem.
- Active Directory is a market leader.
- Microsoft Threat Protection unites the advanced threat protection products.
- Data at rest, in motion, and in use is all protected.

- Azure Security Center combines cloud security posture management and cloud workload protection platform.

Recommendations

Recommendations for enterprises

If you are already an Azure customer, it is a no-brainer for you to consider all the security functionality Microsoft now offers around its IaaS and PaaS cloud services.

Perhaps more importantly, however, if you are already in, or planning to move to, a multicloud environment for your application infrastructure, and if Azure is in that mix, you should look at what Microsoft currently offers in terms of hybrid-cloud and cross-cloud security. You should also quiz it about where its roadmap for security is headed to see whether it matches the direction in which your own cloud infrastructure is evolving.

Microsoft has security platforms and partnerships

Microsoft offers technology in four areas of security

Microsoft has security products and services in four areas of technology: identity and access management (IAM), threat protection, information protection, and security management.

To protect its Azure services in the IaaS and, in particular, the PaaS arenas, the vendor also has its own next-generation firewall (NGFW), distributed denial-of-service (DDoS) mitigation, and web application firewall technologies, all of which are part of network security. However, it has not productized them and does not compete in that segment of the security market; that is, it does not offer those technologies for deployment outside of the Azure cloud.

Beyond that, Microsoft is building a security partner ecosystem

Instead, Microsoft partners with network security vendors such as Check Point, Fortinet, and Palo Alto Networks, developing an ecosystem that will become increasingly important as its offerings in threat protection and security management evolve further.

One key part of the ecosystem is called the Microsoft Intelligent Security Association (MISA) and was launched in April 2018 with an initial 19 vendors whose products integrate with Microsoft security platforms "to provide customers better protection, detection, and response." MISA has since expanded to 50 vendors.

This integration, frequently enabled by application programming interfaces (APIs), is designed to establish a bidirectional channel of communication so that the MISA members' products can send data to a Microsoft back end for aggregation, correlation, and analysis but also so that policy enforcement and remediation actions deriving from that analysis can be sent back to their devices to be carried out.

Identity

Active Directory is a market-leading directory

Microsoft's presence in the IAM market stems from the strength of its Active Directory (AD) product, both in its original on-premises version and, more recently, as its cloud-based alternative, Azure AD. So widely used is AD in the enterprise market that all IAM vendors, whether from the on-premises world such as IBM, CA, and Oracle, or the cloud-native players such as Okta and Ping, trumpet their ability to use it as their source of authoritative identify information.

Indeed, the latter group of vendors has in recent years moved to develop so-called AD bridging capabilities, enabling their products to talk to an on-premises AD in order to manage access to applications and assets that remain in customers' own data centers, thus overcoming the perceived shortcoming of only being able to enable access to cloud-based applications and services.

Authentication fills out its IAM requirements

It is Ovum's contention that Microsoft has not traditionally been a fully fledged competitor in the IAM market, going up against the heavyweights in on-premises platforms such as IBM and Oracle. This is despite the fact that its Active Directory was very frequently the back-end source of the information on which these third-party IAM systems drew for authentication and authorization information. Now, however, the situation is different.

The change is, at least in part, enabled by the broader trend for IAM to move into the cloud and be delivered as a service with the emergence of a new acronym, IDaaS (identity-as-a-service). With AD able to handle the provisioning of identities and the moves, adds, and changes required for an IAM platform, Microsoft has lately added the ability to authenticate users when they first request access.

In this context, the company evangelizes about the trend toward password-less authentication, supporting biometrics and FIDO2-compliant secure keys in this context, and offering its Microsoft Authenticator mobile app to underpin multifactor authentication (MFA) scenarios by receiving a one-time password sent in an SMS message to a phone.

Beyond authentication, Microsoft touts its ability to grant conditional access, whereby, after being authenticated and authorized to proceed, a user is monitored throughout their time on a company's infrastructure (the session), enabling the system to present additional authentication requirements on an ad hoc basis. It can, for instance, require the user to provide additional information to access particularly sensitive data or perform a financial transaction. Equally, if it picks up what it considers to be particularly risky behavior, it can simply terminate the session altogether.

Microsoft Cloud App Security is the company's CASB

As a result of its 2015 acquisition of Israeli developer Adallom, Microsoft has a cloud access security broker (CASB) in its portfolio, bearing the name Microsoft Cloud App Security. CASBs grew up for two main reasons:

- to provide corporate security teams with visibility into the SaaS functions in use within their organization, given the ease with which new services can be adopted by end users without their IT department's knowledge (a phenomenon commonly known as "shadow IT")

- to enable those same teams to exert control over SaaS services, blocking those that they decide not to sanction and enforcing corporate security policy on the use of those that they do, via techniques such as read-only access, blocks on downloading, and encryption, for example.

Microsoft Cloud App Security actually contributes to the company's overall security proposition in various ways. In the context of identity, for instance, the product integrates with Azure AD so that customers can perform identity-centric monitoring of users on their infrastructure and can control their actions via the conditional access facility and the vendor's reverse proxy.

Threat protection

Microsoft Threat Protection unites the ATP products

Microsoft has offered anti-virus software since its acquisition of Romanian developer GeCAD in 2003. However, in more recent times, the vendor has expanded its ability to defend customers' infrastructure from cyberthreats. On the endpoint, it augmented its Windows Defender product with the acquisition in 2017 of Hexadite, an Israeli developer of endpoint detection and response (EDR) technology, which is now part of the Windows Defender Advanced Threat Protection (WDATP) product.

Identities, endpoints, user data, cloud apps, and infrastructure are protected

The ATP tag has since been applied elsewhere in its portfolio; Microsoft now offers Azure ATP for identities and Office 365 ATP for email. Even more recently, the three ATP products have been offered together under the name of Microsoft Threat Protection (MTP), which is designed to cover detection and response requirements across

- identities
- endpoints
- user data (emails, messages, and documents)
- cloud applications (SaaS and cloud storage)
- infrastructure (servers, virtual machines, databases, and networks).

MTP learns what constitutes normal user behavior, leveraging the behavioral analytics capability with the platform, so as to detect anomalies and prioritize investigations in accordance with the risk profile of the individual users.

The Intelligent Security Graph is Microsoft's threat intel play

MTP is also backed by the company's Microsoft Intelligent Security Graph. This is a repository of threat information from millions of Microsoft and customer-deployed systems around the world to which artificial intelligence and machine learning is applied to generate threat intelligence that can be used to improve investigations and speed up response.

The Microsoft CASB helps pinpoint anomalous and high-risk behaviors

As with the company's identity technologies, Microsoft Cloud App Security has a role to play in the context of threat protection, this time in identifying high-risk usage and detecting unusual user behavior, drawing on the threat intelligence from the Intelligent Security Graph.

Information protection

Data at rest, in motion, and in use is all protected

Microsoft identifies the need to protect data via obfuscation techniques such as encryption as well as via data leak prevention rules, outlining three situations that together constitute complete protection:

- data at rest in databases and/or on storage devices, as well as on end user devices such as laptops
- data in motion, (i.e., traversing network connections, where SSL/TLS creates an encrypted tunnel through which data can travel securely)
- data in use.

The data-in-use scenario is covered by a capability announced last year called Azure Confidential Computing, whereby data that is in cleartext for processing purposes is kept within a trusted execution environment (TEE), also known as a secure enclave, a facility that is enabled by Intel's SGX technology.

TEEs prevent data or the operations going on inside the enclave being viewed from the outside, even with a debugger, and make sure that only authorized code is permitted to access data. If the code is altered or tampered with, the operations are denied and the environment disabled. The TEE enforces these protections throughout the execution of code within it.

The platform provides discovery, classification, protection, and monitoring

Building on its 2015 acquisition of another Israeli startup, Secure Islands, the company has recently announced Microsoft Information Protection, an integrated set of technologies that cover four key requirements of such technology.

Discovery

This is the ability to locate all the data assets that a company has, whether they be on storage devices in its infrastructure, in cloud storage environments such as OneDrive, or on end users' laptops. Increasingly, given the size and complexity of this task, the vendor is introducing the ability to perform discovery in an automated fashion.

Classification with a common taxonomy

This is the critical phase of determining how data should be categorized for handling purposes, receiving designations such as "confidential," "secret," and "top secret," for example, with enterprise-wide agreement on what each of these descriptions means in terms of access controls, the need for encryption, and retention/deletion policies, for example.

Protection

This part of the portfolio is where protection mechanisms such as encryption and tokenization are put in place, as well as the level of obfuscation mandated by the data's classification (AES 256, 512, and so on).

Monitoring

This is the ongoing process of keeping watch over the protected assets, logging attempts to access them, and determining whether they are legitimate or not, with reports to the relevant people within the organization.

Microsoft Information Protection is made up of constituent parts, namely Windows Information Protection, which was introduced with Windows 10, and Azure Information Protection. It offers a software development kit (SDK) for third parties to integrate it into their technology platforms.

Microsoft will shortly add an analytics capability called Information Protection Analytics, with which customers will be able to use Microsoft's Keyword Query Language (KQL) to interrogate the system for insights into how protected data is being used and by whom. The company is also adding optical character reading for discovery and classification of data within images.

Microsoft Cloud App Security helps with information protection

As for the CASB's role in information protection, it enables customers to enforce granular control policies and perform single-click remediation actions such as document quarantine and sharing restrictions.

Security management

Azure Security Center combines CSPM and CWPP

Microsoft's main offering in this area is currently its Azure Security Center platform, designed to address the challenges posed by

- rapidly changing workloads: IaaS and PaaS environments are inherently dynamic, which requires a speedy response to changing business requirements and also carries the potential for security provision to lag behind the current state of the infrastructure
- increasingly sophisticated attacks, as threat actors seek to exploit new vulnerabilities and find new ways of doing so
- lack of available skilled security staffers, making the ability to automate detection, response, and remedial actions a vital component of security systems.

Azure Security Center is an interesting product, because it combines two distinct sets of functionality, operating in both the cloud security posture management (CSPM) and cloud workload protection platform (CWPP) segments of this still-emerging market.

CSPM

CSPM is a recently named category of products that assess a company's cloud infrastructure to ensure compliance with regulations and identify security vulnerabilities. They report on how compliant

the infrastructure is with whatever are the appropriate regulatory requirements for the company's sector of activity (e.g., MiFID for the financial sector, HIPAA in healthcare, PCI DSS for any e-commerce infrastructure, and so on). They can also take action to right any noncompliance, thereby offering continuous and ongoing verification, and take corrective action to ensure that there is never any of the kind of drift that is endemic to cloud estates.

Thus, Azure Security Center enables customers to strengthen their security posture, helping them identify and perform the hardening tasks recommended as best practices and implement them across machines, data services, and applications. This includes identifying shadow IT subscriptions, which come up as "not covered" in the platform's dashboard, and tracking and managing compliance and governance over time, with the platform providing an "overall compliance" status report, giving the customer a measure of the degree to which their subscriptions are compliant with the policies associated with a given workload.

CWPP

Beyond the corrective functionality of CSPM, however, Azure Security Center also comes with CWPP capabilities for securing workloads.

CWPP platforms are designed to detect and block threats, which usually arise from the use of agents embedded in the workload. Azure Security Center also makes it possible for customers to automate application control policies on server environments. Adaptive application controls in Security Center enable end-to-end app whitelisting across Windows servers without the need to create the rules or check violations.

Azure Security Center is natively part of Azure, and a free version of the platform, which provides basic functionality, is enabled as part of a customer's Azure subscription. There is also a standard pricing tier, for which Microsoft offers a free trial for all users. The fact that it is Azure native also means Azure Security Center monitors and protects PaaS functions within Azure such as service fabric, SQL databases, and storage accounts by default.

In addition, Azure Security Center protects non-Azure servers and virtual machines in the cloud or on premises (Windows and Linux servers) via the installation of the Microsoft Monitoring Agent on them. Azure virtual machines are auto-provisioned in Azure Security Center.

Another out-of-the-box feature of Azure Security Center is integration with Windows Defender ATP, Microsoft's EDR product. This means that, without any configuration, Windows virtual machines and servers are integrated with Azure Security Center's recommendations and assessments. Advanced threat detection is also offered out of the box for Linux virtual machines and servers.

Aware of the need to provide multicloud security, the vendor plans to extend Azure Security Center beyond Azure, starting this year with AWS and adding Google Cloud Platform (GCP) later.

CASB contributes to security management

Microsoft Cloud App Security also has a role to play in security management, enabling customers to identify cloud apps on their network and gain visibility into shadow IT as well as providing ongoing detection of abnormal usage patterns, upload/download traffic, and transactions.

Secure Score helps raise awareness and visibility

One of the most interesting parts of Microsoft's security offering is Secure Score, which started life in the Office 365 world and is now increasingly being applied across the company's entire portfolio. Secure Score is a dashboard that presents a graphical view of how a company is progressing with regard to its security or, as practitioners in this sector like to say, how its attack surface is faring (i.e., whether it is expanding or contracting). While it is not, per se, part of the vendor's security management portfolio, it clearly helps increase the visibility of the latter.

Secure Score reviews the security recommendations generated by Azure Security Center and prioritizes them for the customer so that they know which recommendations to act on first. This helps them find the most serious security vulnerabilities and prioritize investigation. It is a tool designed to help Microsoft business customers assess and improve their security posture.

While it can be used by the security team to optimize its workflow, its straightforward dashboarding makes it readily understandable by board-level executives who lack a technical understanding of security but who must nonetheless keep an eye on how the company in their charge is addressing security challenges.

Further opportunities in security management

SIEM is a market in transformation

In Ovum's opinion, the broader security management market provides Microsoft with the scope to disrupt the security market, because this segment is itself in a state of flux.

The SIEM market is a well-established sector where a range of vendors offer platforms for the aggregation and correlation of network logs in a single repository, from which they can be analyzed, enabling customers' security teams to detect suspicious activity and determine what remedial action to take. In recent times, SIEMs have been enhanced with products that bring extra analytical capabilities in the form of user and event behavior analysis (UEBA), as well as ones that enable remediation operations to be orchestrated and, wherever possible and appropriate, automated, namely security orchestration and automated response (SOAR) platforms.

Predictably, the more proactive of the SIEM vendors have engaged in M&A activity to add these capabilities to their portfolios (Splunk bought Caspida for UEBA and Phantom Cyber for SOAR, while IBM acquired Resilient for incident response even before the SOAR acronym had been created). Meanwhile, some of the pure-play UEBA vendors such as Exabeam and Securonix now position themselves as SIEM vendors in their own right.

At the same time, newer players, such as Jask, have entered the fray, many of them riding the cloud wave to offer SIEM or SIEM-like functionality as a service from the outset, where traditional SIEM providers started life as purveyors of on-premises software. Add to this the evolution of threat intelligence platforms and gateways (TIGs) and the fact that several security industry mainstays such as Symantec, Cisco, and McAfee are offering "platforms" for receiving threat alerts and coordinating responses, and it becomes clear that the whole security management space is evolving and changing.

There is also the potential for disruption in pricing models. Many enterprises complain that the storage of their logs, particularly if they require long-term retention for compliance or research purposes, ends up being a very expensive proposition with the leading SIEM providers. Indeed, a number of managed security service providers that deliver SIEM as a service to multiple customers tell Ovum they are engaged in developing their own alternative to the commercially available platforms for reasons of cost as well as of functionality.

Azure Sentinel is a cloud-based SIEM service

It is into this environment that Microsoft has launched its SIEM-as-a-service offering, Azure Sentinel.

It collects a customer's Office cloud data and combines it with security information, and in this context, Azure Sentinel's support for the common event format (CEF) enables it to draw threat data and alerts from systems from MISA members such as Check Point, Cisco, F5, Fortinet, Palo Alto Networks, and Symantec as well as from other Microsoft technology partners such as ServiceNow.

The SIEM platform collects all this data to find threats, using artificial intelligence (AI) to reduce noise and cut alert fatigue by what the company claims to be up to 90% based on the experience of its beta customers.

Even before launching Azure Sentinel service, Microsoft offered customers the ability to store the logs from their Azure instances (a service called Azure Log Analytics), so they can now be analyzed within Azure Sentinel, which is classic SIEM functionality. The difference is that, by applying AI, the vendor aims to simplify and streamline the analytical process, easing the burden on overworked security analysts.

Microsoft Threat Experts comes with a panic button

Meanwhile, the new Microsoft Threat Experts service analyzes a company's security data and pulls out the most important threats, such as human adversary intrusions, hands-on-keyboard attacks, and cyber-espionage, to help security teams prioritize risks and respond to the most important ones more quickly.

The service comes with a new "Ask a Threat Expert" button within Windows Defender ATP, which allows security operations teams to submit questions to Microsoft's own security specialists directly from the product console.

Both new services are designed to be labor saving

The market opportunity for both Azure Sentinel and Microsoft Threat Experts comes not only from the challenges faced by classic SIEM vendors right now but also from the worsening shortage of skilled cybersecurity professionals. The latest predictions are of a shortfall of as many as 3 million people, (i.e., 3 million unfilled positions within the cybersecurity sector by 2021), and in this context, clearly any technology that promises to simplify the lives of the analysts in the frontline is to be welcomed.

Expect to see Microsoft raise its profile in security

Mobile security shows where Microsoft is going

Mobile security is in some ways a harbinger of the change in Microsoft's approach to the security market as a whole. By virtue of its abandonment in 2017 of the Windows Phone OS, Microsoft has been obliged to support its erstwhile rivals iOS and Android with the Windows Defender ATP product, and now this heterogeneity is expanding to the laptop world, where Mac devices are supported, and into servers, where Linux is also protected by the endpoint security platform.

Meanwhile, for cloud environments, MTP will be extended to AWS in 2019 and to GCP sometime thereafter.

Partial Azure shops are in scope for a security play

Hybrid and multicloud environments are the target

Microsoft's positioning in the security market is changing thanks to heterogeneity, but the company acknowledges that it will not be competing across the board. It has no ambitions in network security beyond Azure, for example. Equally, enterprises that are mainly AWS shops when it comes to their IaaS/PaaS provider are not targets for any of Microsoft's cloud security technologies.

Wherever Azure is in the mix, however, and that includes both hybrid (cloud and on premises) and multicloud (i.e., using two or more CSPs) environments, Microsoft will be marketing its security offerings as comprehensive services that can cover its own and third-party operating systems. And of course, it has the huge advantage that the majority of enterprises on the planet will have some Microsoft products in their infrastructure. Many of them will now be looking to cloudify their application infrastructure as part of a broader digital transformation project, thereby opening the door for cloud and security conversations with all their IT providers.

Appendix

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

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

Copyright notice and disclaimer

CONTACT US

ovum.informa.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Boston
Chicago
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
Paris
San Francisco
Sao Paulo
Shanghai
Singapore
Sydney
Tokyo