REPORT REPRINT

Microsoft's security focus becomes a first-class citizen among Ignite announcements

FERNANDO MONTENEGRO, PATRICK DALY, SCOTT CRAWFORD

30 OCT 2018

While some in the security industry roll their eyes at references to 'security is our most important goal' and similar platitudes from some organizations, they'd be wrong to do so when considering Microsoft. The company revealed several new security offerings aimed at improving the security experience for practitioners and users alike.

 |

As roughly 20,000 professionals descended on this year's Microsoft Ignite event, they were treated to dozens of new product and service announcements across the company's portfolio, including AI, IoT, edge computing and updates to the Azure infrastructure itself. However, it was the breadth of security offerings and announcements that could differentiate Microsoft from its competitors. Microsoft revealed a slew of new security offerings, including password-less authentication features, a new threat protection offering, enhancements to its Secure Score offering and a new confidential computing architecture available within Azure to protect data in use.

THE 451 TAKE

Few companies are as embedded into the fabric of modern enterprise computing as Microsoft. As organizations modernize their environments, it is only natural for Microsoft to be a significant technology choice across a number of disciplines. All Microsoft's announcements from Ignite seem to touch on a theme that we are seeing across the security industry. The Threat Protection and Secure Score speak to enterprises moving toward a continuous evaluation of their security posture and also include increased automation and orchestration capabilities for the practitioner. Password-less security also speaks to a move away from passwords as a means of user authentication and a shift in security products developed to optimize the user experience. While none of these offerings are unique, the combination of these new products with Microsoft's existing security assets and the level of intelligence it is able to aggregate across a customer's devices, identities and cloud infrastructure gives the company a formidable security portfolio, not only compared with other cloud providers but also among security vendors. The challenge for Microsoft is twofold: to continue executing on this wholesale transformation and to come to market with offerings that, while working best together, are flexible enough to operate independently as they attempt to ease the migration paths through which its core enterprise customers are going.

CONTEXT

Ignite is Microsoft's main user-focused event, bringing about 20,000 professionals to Florida for a week filled with thousands of distinct activities ranging from broad keynotes to breakout sessions, certification exams and community meetups. The message from the conference is anchored around keynotes from CEO Satya Nadella and president Brad Smith, and further distilled by dozens of other executives targeting their specific areas.

STRATEGY

Nadella framed Microsoft's broader strategy as a move toward a model embracing the duality of centralized and decentralized technology. Nadella indicated that Microsoft is looking to provide offerings to implement what it called Intelligent Cloud and Intelligent Edge. On one hand, centralized cloud capabilities such as artificial intelligence and data processing – running on Azure, of course – provide the transformative analytics that organizations are looking for as they embark on digital transformations. In parallel to this, Microsoft looks to provide increased capabilities at the edge, including IoT in various forms as well as traditional edge compute now enhanced for the cloud (meaning, in Microsoft's case, Azure Stack or the traditional Windows server offerings).

To support this vision, security is naturally an integral component of all offerings. As it relates to its security strategy, Microsoft highlighted three core pillars: operations, technology and partnerships. From an operations perspective, the company is already protecting over 100 datacenters worldwide and employs 3,500 security professionals that act as extensions to their clients' existing security personnel. In terms of technology, Microsoft classifies its security products under four umbrellas: identity and access management (which is primarily Azure Active Directory), information protection, threat protection and security management. Last, Microsoft actively pursues partnerships with peer vendors and participates in industry and government alliances. Most notably, the Microsoft

Intelligent Security Association that was announced at the RSA Conference allows partners to come together to share security intelligence and the company is also a FIDO alliance member. Each of the announcements at Ignite falls under at least one of the above pillars.

ANNOUNCEMENTS

Indirectly, Microsoft provided further evidence that security is indeed one of its primary concerns by listing it as the very first section of announcements in some of its media collateral. Other topics listed were, in order: artificial intelligence and data, Internet of Things and edge computing, Azure topics and Microsoft 365 topics.

Microsoft started off with the reveal of a new password-less login capability via the Microsoft Authenticator app for Azure AD, bringing enterprises a more seamless MFA experience. Once users have initiated the login process with their username or email address, they are redirected to a page displaying a number, telling them to open the Microsoft authenticator app on their mobile device and tap the number shown on the screen. This establishes the 'something I have' factor of the MFA process, since the authenticator app on their device is linked to their unique username. From there, users then prove the device belongs to them with a biometric factor provided through FaceID or a fingerprint, establishing the 'who I am' factor. This system is not only more secure than a typical password login, but it also seems to remove some of the friction associated with SMS-based MFA schemes in which users have to type in the numbers sent to their mobile device manually to authenticate themselves to the application.

The company also expanded its Secure Score offering to include intelligence gathered across its identity controls, data, devices, applications and infrastructure, providing a more holistic view of an organization's full security posture than the product provided previously. The result is a score that acts as a report card, allowing enterprises to view their overall status and gain insight into how they can improve. The ability to initiate workflows that implement Microsoft's recommendations, such as applying MFA to admin accounts or reconfiguring an application, is embedded within the Secure Score UI, making it easier for security and IT teams to improve their security profile. Trend lines also show how the organization's score has changed over time and compare their security posture to enterprises in the same industry or of a similar size.

The updated Microsoft Threat Protection is the company's most ambitious release of this offering to date. The new product includes a greater emphasis on automation and combines protection for email, identities, endpoints, user data, devices, cloud apps and infrastructure. Microsoft Threat Protection surfaces the signal from the different security services into a single console. The dashboard highlights ongoing incidents, including the users, devices, apps and email accounts that are at greatest risk within the organization. Rather than individual alerts, however, Threat Protection automatically consolidates multiple alerts into a single incident, providing security teams with a step-by-step report of how an attack was carried out and the action taken to respond to the incident. Following the initial auto-remediation capabilities first introduced in Windows Defender ATP, Microsoft Threat Protection is fully integrated with automated remediation capabilities to aid security operations teams in breach containment, investigation and response. When an investigation begins, SecOps teams can take advantage of the advanced threat hunting functionality embedded in Threat Protection, including a community of hunters at other organizations that have developed queries to check for specific threats in their environment. This allows SecOps teams to simply run queries, which can be shared through a GitHub repository, to check if the same threat has affected their environment (and yet another example of Microsoft's leveraging of the advantages of GitHub).

To improve data security on Azure public cloud, Microsoft also revealed the public preview of Azure confidential computing, an effort to protect customer data in use. The service is offered as a new series of VMs in Azure and uses secure enclaves on Intel SGX technology to run customer workloads in a trusted execution environment, protecting data while it is being processed in the cloud. Microsoft released an open source SDK along with the new DC series VMs to support the confidential computing vision for customer development teams to begin building TEE-based applications.

Security was also a key factor in several other announcements, such as the availability of Windows Server 2019, now with more secure container support, better integration with Windows Defender ATP, support for exploit protection technology and availability of Shielded VMs for Linux. Microsoft's 'Azure Sphere' initiative of creating a newer generation of control silicon for IoT use cases is also heavily dependent on security functionality.

One of Microsoft's key strengths is its ability to understand what security concerns may impede its customers' cloud transformation journeys and provide resources to alleviate those concerns. This was evident with the release of features such as additional compliance information related to the GDPR, the availability of Azure Blueprints to optimize creation of safe Azure environments and a smattering of network-focused announcements, including support for virtual network taps. A feature that enterprise network security teams have long relied on for gathering data on-premises, the technology has been announced in preview mode and partners such as ExtraHop, Gigamon and others have announced support for it in future releases.

LOOKING AHEAD

We expect Microsoft to continue to focus on optimizing how enterprise customers can use its myriad security offerings to ease digital transformation efforts. This includes deeper integration with identity technologies as well as automation and security operations, especially pertaining to simplifying the threat detection, investigation and remediation process. These are among the areas most heavily affected by the security expertise shortage in the enterprise, due to the number of alerts that hit enterprise SOCs every day and the level of experience and technical skill required to be a threat hunting analyst. Microsoft's Secure Score and Threat Protection announcements are both intended to tackle this problem and will likely be well received by enterprise security teams that struggle to keep up with alerts and conduct investigations on a regular basis.

Aside from making the practitioner's job easier, we would also expect Microsoft to keep focusing on improving the user experience in security, much as its password-less MFA offering is intended to do. Security vendors make a habit of blaming user behaviors when incidents occur (see: weak passwords) but if vendors truly want to improve their clients' security posture, then a far more realistic embrace of actual human behavior needs to be factored into a product's design rather than used as a scapegoat. Actions like removing passwords in favor of a more secure MFA process are one way to accomplish this but Microsoft will have to continue thinking of ways to incentivize people to act in a more secure manner when interacting with Office, Windows and Azure.

COMPETITION

With Azure being a key component of Microsoft's strategy, it is no surprise that the other hyperscale cloud providers – Amazon Web Services and Google, primarily – are direct and clear competition. Both offer a range of cloud services that rival Microsoft's. Other large-scale cloud providers such as AliCloud, IBM and Oracle also compete across a range of services.

In large part, competition to Microsoft, particularly in enterprise environments, occurs at both strategic and tactical levels. On the strategic front, a customer may choose alignment with competitors such as IBM, Oracle, SAP, which may offer alignment with existing strategic investments or platforms (such as databases or ERP in the latter cases). At more tactical levels, customers may choose a provider that can fulfill requirements for specific projects or technologies. Competition for Microsoft can be paradoxical. On the one hand, it stems from, among other places, the paradigm that Microsoft may offer a third-party option that may be preferred over leveraging existing features from other vendors.

On the other hand, Microsoft's forays into security, for example, highlight the advantage the company brings as the provider of broadly penetrated offerings, from Windows to Microsoft 365 to Azure. In security, Microsoft competes against numerous vendors in different areas. On email security, Microsoft is seen competing with Symantec, Mimecast and Proofpoint, among others. On the endpoint security front, Microsoft is up against Symantec, McAfee, Trend Micro, Carbon Black, Crowdstrike, FireEye, Bitdefender and numerous others. Announcements such as Security Score and Threat Protection bring in competition from security analytics vendors including Splunk, Bitsight and others. Microsoft can leverage its advantage in offering competing technologies integrated with its products, as long as those offerings are effective in countering the competitive advantage others may have by specializing in targeted domains.

SWOT ANALYSIS

STRENGTHS
Microsoft is a cornerstone of the IT industry and makes a credible claim to giving proper importance to security as a critical part of its offerings. The company also has a deep understanding of enterprise use cases and mind-set.

WEAKNESSES
Microsoft products often deliver better results working together, which means that organizations may balk at the potential complexity of having to adopt more than one Microsoft product to achieve a given set of functionalities.

OPPORTUNITIES
Microsoft can likely make further strides with cloud and security use cases if it can capture not only the cloud transition for existing enterprises, but better handle the needs of cloud-native organizations.

THREATS
The largest threat to Microsoft stems from long-term industry shifts to technology patterns that may not favor it as much. These can include alternate models for user identity, IoT devices, AI/ML or endpoint platforms.