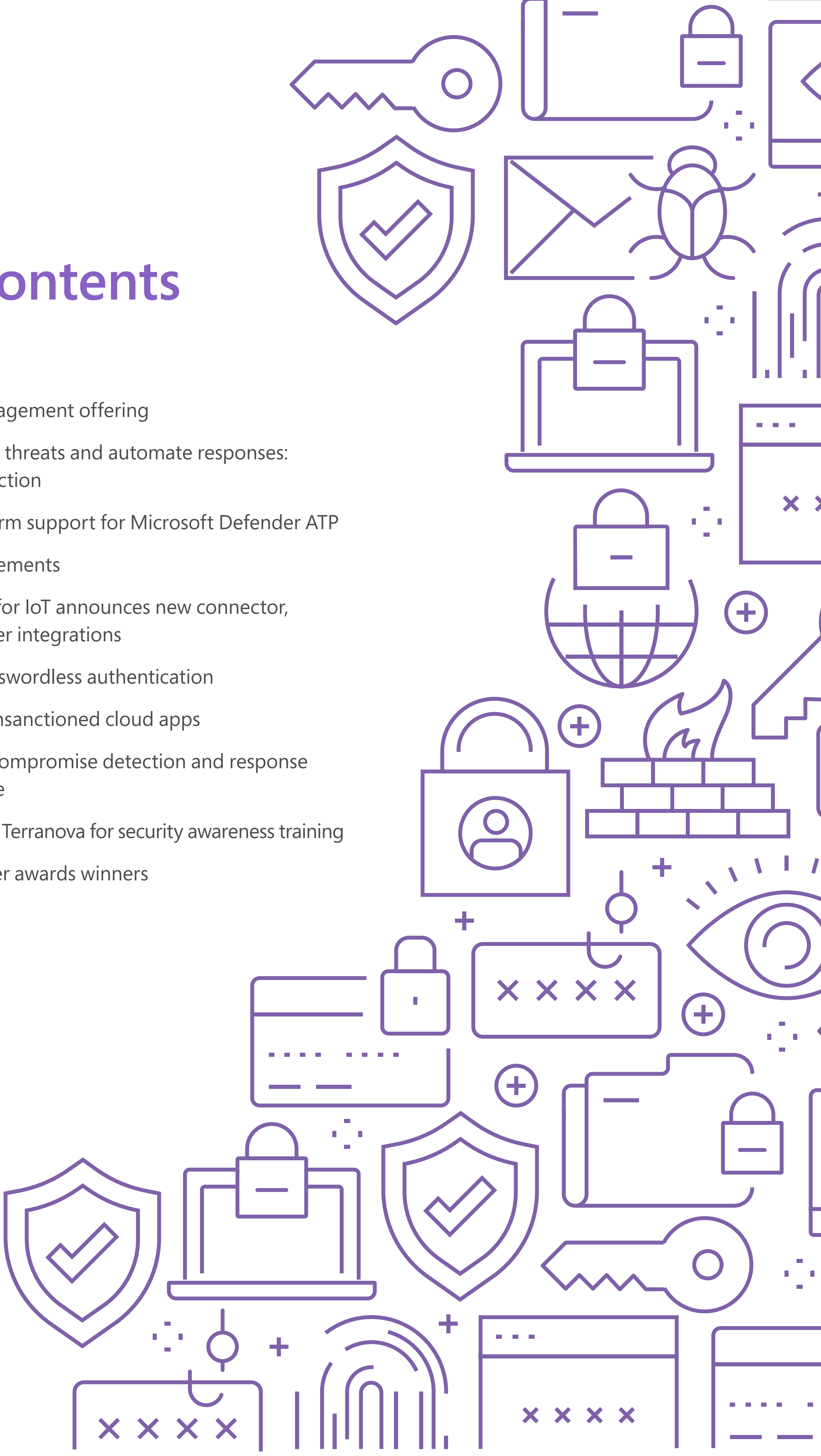
Microsoft

RSA Conference 2020

Book of news

Table of contents



Introduction

From protecting IoT devices in the field, to using AI in the hunt for insider threats, to extending security technologies well beyond the Microsoft platform, Microsoft is breaking new ground this year at the RSA Conference. This book of news is designed to help you navigate this week's announcements, highlighting new products and programs designed to support security operations professionals around the world.

1. A new insider risk management offering

The proliferation of devices means corporate data is on laptops, phones, even watches, and can be easily transported and accessed anywhere. In this environment, CISOs and IT departments need ways to identify, remediate and prevent insider risks to keep their organizations safe.

This week we are announcing the worldwide general availability of our Insider Risk Management offering to combat this difficult challenge. By gathering signals from across Microsoft 365 and other third-party systems, Insider Risk Management can identify anomalies in user behavior and flag high-risk activities. With privacy built in by design, the system leverages AI and machine learning to mitigate insider risks and better protect and govern the organization's data.

The offering also includes an IP Theft template and previews of our Harassment, Confidentiality, and Security templates. More information is available on the Microsoft blog, Leverage AI and machine learning to address insider risks.

2. A new tool to correlate threats and automate responses: Microsoft Threat Protection

Security teams often have an endless list of alerts coming their way from across the organization, making it difficult if not impossible to link those at speed, prioritize, and act swiftly on the most critical threats. To combat this problem, this week we are releasing the general availability of Microsoft Threat Protection, which correlates alerts across the threat landscape so security teams can focus on what matters most.

With Microsoft Threat Protection, SecOps teams get a correlated, incident-level view of threats, instead of managing individual alerts—and losing precious time mired in the noise or missing critical alerts that can wreak havoc. To help those teams be even more successful, Microsoft Threat Protection can investigate threats, respond to them, and restore affected assets to a secured state automatically, while simplifying hunting across the landscape for signs of attack.

Microsoft Threat Protection can also self-heal compromised user identities, endpoints, and mailboxes, allowing SecOps to focus on strategic projects and policies and put specialized knowledge to work across the threat landscape. Critical threat insights are shared in real time between Microsoft Threat Protection products to help stop the progression of an attack. The central Microsoft Threat Protection logic orchestrates and triggers actions on the individual products, like applying conditional-access policies when an identity-based threat is detected or cleaning impacted mailboxes.

The solution has been in preview to the tech community only. At the RSA Conference, we are releasing it more broadly so SecOps teams can get hands on and see the power of Microsoft Threat Protection.

3. Extending cross-platform support for Microsoft Defender ATP

Today's enterprises use a variety of devices and platforms, and attackers are targeting all of them. Customers want a single solution that can bring together alerts and threat insights from across all their devices and platforms for a unified view—with the ability to quickly remediate.

We have been listening to this customer feedback and are committed to delivering a best-in-class security solution that will help customers quickly detect and resolve threats across their enterprise. Microsoft is committed to delivering security solutions not just for Microsoft, but from Microsoft, and we demonstrated that commitment with our Microsoft Defender ATP for Mac announcements in December.

Last fall at Microsoft Ignite we previewed upcoming new capabilities for Linux, and this week at the RSA Conference we are progressing on those commitments, extending our capabilities to Linux and beyond. We are announcing the public preview of preventative protection capabilities from Microsoft Defender ATP on the following supported Linux server distributed versions: RHEL 7+, CentOS Linux 7+, Ubuntu 16 LTS, or higher LTS, SLES 12+, Debian 9+, and Oracle EL 7.

Our continued investments will also bring security from Microsoft into mobile platforms, and we plan to show a preview of the work we're doing there—new mobile security capabilities we expect to deliver in calendar year 2020.

On the client, the customer will get AV prevention and a full command line experience. In the Microsoft Defender Security Center, customers will see basic alerts and machine information. EDR functionality is forthcoming this year as well.

You can read more about our efforts to extend Microsoft Defender ATP to protect iOS, Linux, and Android on our Defender ATP blog.

4. Azure Sentinel enhancements

Announced last September, Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. With Azure Sentinel, enterprises worldwide can keep pace with the exponential growth in security data, improve security outcomes, and reduce hardware and operational costs.

This week we are announcing new enhancements for Azure Sentinel that will deliver instant value and new efficiency to security operations teams, making it easier to collect data across diverse sources and get security insights across the enterprise:

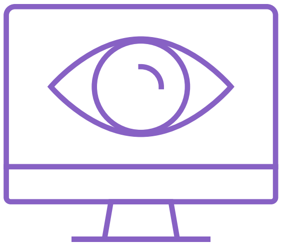
- **New built-in connectors for easier data collection:** We are introducing new data connectors and workbooks from partners like Forcepoint, Zimperium, Quest, CyberArk, and Squadra. The new connector for Azure Security Center for IoT provides onboarding of IoT data workloads into Azure Sentinel from Azure IoT Hub-managed deployments. With this new announcement Azure Sentinel is the first SIEM with native IoT support, allowing SecOps andanalysts to identify threats in the complex converged networks.

- **Augment security operations center teams with a community-driven approach:** We are offering a rewards program for community contributions to develop dashboards, orchestration workflows, notebooks for advanced hunting scenarios, and much more.

- **New resources for security teams:** We're also announcing the availability of new developer docs, guides, samples, validation criteria, and updated GitHub Wiki, and support codified contributions for data connectors on GitHub.

- **Import AWS CloudTrail logs for no additional cost from February 24, 2020 until June 30, 2020:** Azure Sentinel provides security insights across the entire enterprise, not just on Microsoft workloads. Customers can already ingest Microsoft Azure activity logs, Office 365 audit logs, and Microsoft 365 security alerts for free with Azure Sentinel. We are announcing import of AWS CloudTrail logs into Azure Sentinel for no additional cost from February 24, 2020 until June 30, 2020, for new and existing Azure Sentinel customers. With this offer, AWS customers who adopt Azure Sentinel can also now have seamless access to the best-in-class cloud-native SIEM technology from a major cloud provider.

All these features are currently available as of February 24.
See the Microsoft Security blog for more information.



5a. Azure Security Center for IoT announces new connector, OS support, and partner integrations

Azure Security Center for IoT has been ramping up several new products and programs, which are being announced this week at the RSA Conference:

Azure Sentinel connector for IoT
This week Azure Security Center for IoT is announcing the availability of an Azure Sentinel connector that provides onboarding of IoT data workloads into Sentinel from Azure IoT Hub-managed deployments. This integration provides investigation capabilities on IoT assets from Azure Sentinel, allowing security pros to combine IoT security data with data from across the organization for artificial intelligence or advanced analysis.

With Azure Sentinel connector, SecOps teams can now monitor alerts across all IoT Hub deployments, act upon potential risks, inspect and triage IoT Incidents, and run investigations to track an attacker's lateral movement within the network.

New operating system support
Azure Security Center for IoT is extending support for Azure real-time operating systems in addition to Linux (Ubuntu, Debian) and Windows 10 IoT core operating systems. Real-time OS support provides the capability to detect malicious network activities, to baseline device behavior based on custom alerts, and to identify when identical authentication credentials are used by multiple devices.

Partner integrations
By partnering with members of Microsoft Intelligent Security Association, Microsoft can leverage a vast knowledge pool to defend against a world of increasing IoT threats in enterprise, healthcare, manufacturing, energy, building management systems, transportation, smart cities, smart homes, and more.

Azure Security Center for IoT's partner integration capabilities enable partner security alerts to be displayed on the Azure Security Center user interface. Customers can use Azure Security Center as a single pane of glass to see their security posture recommendations.

(CONT)

5b. Azure Security Center for IoT announces new connector, OS support, and partner integrations

(CONT)

Azure Security Center for IoT's simple onboarding flow connects solutions from vendors like Attivo Networks, CyberMDX, CyberX, Firedome, and SecuriThings, enabling SecOps teams to protect managed and unmanaged IoT devices, view all security alerts, reduce the attack surface with security posture recommendations, and run unified reports.

To learn more, read the Microsoft blog, Azure Security Center for IoT RSA Conference 2020 Announcements.

Azure US Gov support

Also, starting in March, Azure Security Center for IoT will be available in the Azure US Gov Virginia and Azure US Gov Arizona regions. US Gov support is expected to be available by March 1, 2020.

6. A new step toward passwordless authentication

Back in July we announced the public preview for passwordless authentication in cloud-based environments. This week we're announcing the expansion of our preview of FIDO2 security key support in Azure Active Directory to hybrid environments—enabling even more customers to take an important step in their journey toward passwordless authentication.

Support for hybrid identity environments was a blocker for 90 percent of customers in adopting passwordless authentication, and with this announcement, we are expanding the preview for 10 times more people, supporting both on-premises and cloud applications. Organizations with Windows Server Active Directory can now enable passwordless authentication using FIDO2 security keys for Hybrid Azure Active Directory-Joined Windows 10 devices and get a single sign-on experience for their cloud and on-premises applications.

This demo video shows how the feature works. As soon as the user signs in with her security key, she is automatically connected to Azure Active Directory using Azure AD Domain Join or Azure AD Hybrid Domain Join and does not need to sign in again. When the user navigates to Office, she's already signed in and good to go.

This feature is available now in public preview with the latest Windows Insider build and Azure Active Directory. The integration was tested for compatibility with these Microsoft Intelligent Security Associations partners: Yubico, HID, Global, Feitian Technologies, eWBM, Ensurity, and AuthenTrend. (See documentation for more information.)

General availability of this capability is expected sometime in the next 4-6 months. More information is available on our Identity blog.

7. Endpoint control for unsanctioned cloud apps

Shadow IT discovery is a significant challenge for customers, as is controlling unauthorized use of cloud applications. By bringing together our cloud access security broker (CASB) and endpoint protection capabilities, we can offer a unique solution to customers to address both these concerns.

At the RSA Conference, we are announcing an integration between Microsoft Cloud App Security and Microsoft Defender ATP that provides endpoint-based enforcement of access control and blocks the upload of sensitive files to unsanctioned cloud apps. After deploying Cloud App Security and Defender ATP, it is as simple as one switch to toggle on and configure the policies to apply and enforce.

Read more about this new capability in our RSA Conference Security Announcements blog.

8. Campaign views and Compromise detection and response now generally available

Campaign views GA: The wildly popular campaign views we announced a few months ago is now generally available. Since we first previewed this feature, we've further streamlined the experience and made it easy to search across campaigns. We've seen customers across the globe use and love it. Campaign views gives security teams an all-encompassing view of email attack campaigns targeted at their organizations, along with making it very easy to spot vulnerable users or configuration issues that enabled the campaign to succeed.

Compromise detection and response GA: Since we launched this feature in preview a few months ago, compromise detection and response has enabled customers to detect and recover from compromised accounts—with its Office 365 activity base anomaly alerting and automatic investigation capabilities. We've also enhanced the anomaly detection to look for suspicious inbox rules that look to forward or delete sensitive data—a common attack pattern. Early detection and response to compromised users is critical to ensuring that attacks are thwarted early on and the impact of the breach is minimized. We're excited to announce that this feature is now in general availability.

You can read more about the general availability of these capabilities on the Microsoft blog, Introducing campaign views in Office 365 Advanced Threat Protection.

9. Microsoft partners with Terranova for security awareness training

Microsoft has entered into a partnership with Terranova, a market leader in computer-based training, to include Terranova's entire phishing-related training set into Office 365 Advanced Threat Protection Plan 2. This security awareness training, coupled with Microsoft's **security solutions** and risk analytics, will enable Office 365 Advanced Threat Protection to provide customized user learning paths that enable **organizations to create governance around organizational risk and maintain a stronger security posture.**

Until now, our Attack Simulator functionality has lacked a computer-based training component. With the addition of Terranova's security awareness training **incorporated with our security solutions** and risk analytics, we will provide a complete solution for the first time, and one that is highly differentiated from a training perspective. This differentiation will materialize where it matters the most—achieving results in training efficacy.

We partnered with Terranova because of its market-leading training content created by expert educators. This allows us to focus on developing advanced targeting mechanisms that will achieve the best possible **security** training with the right level of content at the right time based on demonstrated risk levels.

The system provides the ability **to help prevent insider threats** and, based on the risks that users demonstrate while using their devices, assign appropriate training content to help reduce those risk levels to the organization. The training can also be assigned manually or be based on a combination of both manual assignments and analytics. See our blog for more information.

10. Microsoft 20/20 partner awards

Security is a team sport, and our customers need us to work together to help them be more secure. To recognize outstanding efforts across the ecosystems, on February 23, the night before the RSA Conference begins, Microsoft is hosting its inaugural security partner awards event, Microsoft Security 20/20, to celebrate our ecosystem partners.

Winners were voted on by Microsoft employees and will be announced at the event. A preview of the event from earlier this month is available on the Microsoft Security blog.