Securing the hybrid cloud with Azure Security Center and Azure Sentinel

Posted on June 4, 2019

Gilad Elyashar
Principal Group PM Manager, Azure Security Center

Infrastructure security is top of mind for organizations managing workloads on-premises, in the cloud, or hybrid. Keeping on top of an ever-changing security landscape presents a major challenge. Fortunately, the power and scale of the public cloud has unlocked powerful new capabilities for helping security operations stay ahead of the changing threat landscape. Microsoft has developed a number of popular cloud based security technologies that continue to evolve as we gather input from customers. Today we'd like to break down a few key Azure security capabilities and explain how they work together to provide layers of protection.

Azure Security Center (https://azure.microsoft.com/en-us/services/security-center/) provides unified security management by identifying and fixing misconfigurations and providing visibility into threats to quickly remediate them. Security Center has grown rapidly in usage and capabilities, and allowed us to pilot many new solutions, including a security information and event management (SIEM)-like functionality called investigations. While the response to the investigations experience was positive, customers asked us to build out more capabilities. At the

same time, the traditional business model of Security Center, which is priced per resource such as per virtual machine (VM), doesn't necessarily fit for SIEM. We realized that our customers needed a full-fledged standalone SIEM solution that stood apart from and integrated with Security Center, so we created Azure Sentinel. This blog post clarifies what each product does and how Azure Security Center relates to Azure Sentinel.

Going forward, Security Center will continue to develop capabilities in three main areas:

1. **Cloud security posture management**: Security Center provides you with a bird's eye security posture view across your Azure environment, enabling you to continuously monitor and improve your security posture using the Azure secure score (https://docs.microsoft.com/en-us/azure/security-center/security-center-secure-score). Security Center helps you identify and perform the hardening tasks recommended as security best practices and implement them across your machines, data services, and apps. This includes managing and enforcing your security policies and making sure your Azure Virtual Machine instances, non-Azure servers, and Azure PaaS services are compliant. With newly added IoT capabilities, you can now reduce attack surface for your Azure IoT solution and remediate issues before they can be exploited. We will continue to expand our resource coverage and the depth insights that are available in security posture management. In addition to providing full visibility into the security posture of your environment, Security Center also provides visibility into the compliance (https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard) state of your Azure environment against common regulatory standards.

2. **Cloud workload protection**: Security Center's threat protection enables you to detect (https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities) and prevent threats at the infrastructure-as-a-service (IaaS) layer (https://docs.microsoft.com/en-us/azure/security-center/security-center-os-coverage) as well as in platform-as-a-service (PaaS) resources like Azure IoT and Azure App Service and on-premises virtual machines. Key features of Security Center threat protection include config monitoring, server endpoint detection and response (EDR), application control, network segmentation, and is extending to support container and serverless workloads.

3. **Data security**: Security Center includes capabilities that identify breaches and anomalous activities against your SQL databases, data warehouse, and storage accounts, and will be extending to other data services. In addition, Security Center helps you perform automatic classification of your data in Azure SQL database.

When it comes to cloud workload protection, the goal is to present the information to users within Security Center in an easy-to-consume manner so that you can address individual threats. Security Center is not intended for advanced security operations (SecOps) hunting scenarios or to be a SIEM tool.

Going forward SIEM and security orchestration and automated response (SOAR) capabilities will be delivered in Azure Sentinel. Azure Sentinel delivers intelligent security analytics and threat

intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

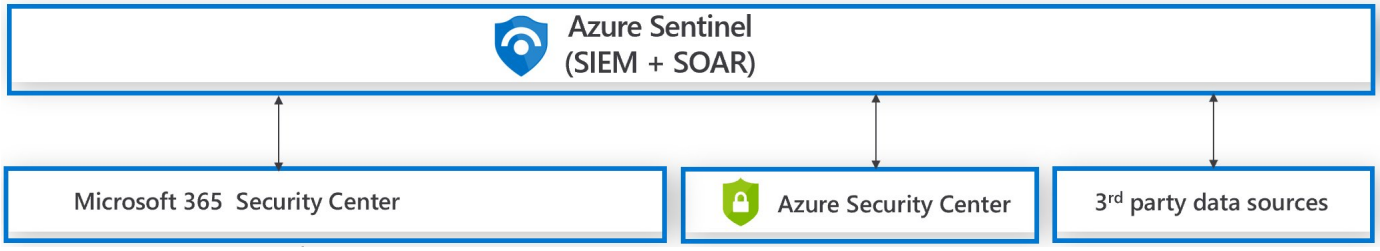
Azure Sentinel is your service operations center (SOC) view across the enterprise, alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution timeframes. With Azure Sentinel you can:

- **Collect data at cloud scale** across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
- **Integrate curated alerts** from Microsoft's security products like Security Center, Microsoft Threat Protection, and from your non-Microsoft security solutions.
- **Detect previously undetected threats** and minimize false positives using Microsoft Intelligent Security Graph, which uses trillions of signals from Microsoft services and systems around the globe to identify new and evolving threats. Investigate threats with artificial intelligence and hunt for suspicious activities at scale, tapping into years of cyber security experience at Microsoft.
- **Respond to incidents rapidly** with built-in orchestration and automation of common tasks.

SIEMs typically integrate with a broad range of applications including threat intelligence applications for specific workloads, and the same is true for Azure Sentinel. SecOps has the full power of querying against the raw data, using AI models, even building your own model.

So how does Azure Security Center relate to Azure Sentinel?

Security Center is one of the many sources of threat protection information that Azure Sentinel collects data from, to create a view for the entire organization. Microsoft recommends that customers using Azure use Azure Security Center for threat protection of workloads such as VMs, SQL, Storage, and IoT, in just a few clicks can connect Azure Security Center to Azure Sentinel (https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center). Once the Security Center data is in Azure Sentinel, customers can combine that data with other sources like firewalls, users, and devices, for proactive hunting and threat mitigation with advanced querying and the power of artificial intelligence.



(https://azurecomcdn.azureedge.net/mediahandler/acomblog/media/Default/blog/05db1e19-d44f-44ca-9ee5-74e8d99b4ec6.png)

Are there any changes to Security Center as a result of this strategy?

To reduce confusion and simplify the user experience, two of the early SIEM-like features in Security Center, namely investigation flow in security alerts and custom alerts (https://docs.microsoft.com/en-us/azure/security-center/security-center-features-retirement-july2019) will be removed in the near future. Individual alerts remain in Security center, and there are equivalents for both security alerts and custom alerts in Azure Sentinel.

Going forward, Microsoft will continue to invest in both Azure Security Center and Azure Sentinel. Azure Security Center will continue to be the unified infrastructure security management system for cloud security posture management and cloud workload protection. Azure Sentinel will continue to focus on SIEM.

To learn more about both products, please visit the Azure Sentinel home page (https://azure.microsoft.com/en-us/services/azure-sentinel/) or Azure Security Center home page (https://azure.microsoft.com/en-us/services/security-center/).

Security (/en-us/blog/topics/security/) Azure Security Center (/en-us/blog/tag/azure-security-center/) Azure Sentinel (/en-us/blog/tag/azure-sentinel/)

Explore

See where we're heading. Check out upcoming changes to Azure products

Azure updates (/en-us/updates/)

Let us know if you have any additional questions about Azure

Ask questions (https://aka.ms/azureqa)

Topics

Announcements (/en-us/blog/topics/announcements/) (2323)

API Management (/en-us/blog/topics/api-management/) (38)

Artificial Intelligence (/en-us/blog/topics/artificial-intelligence/) (244)

Azure Maps (/en-us/blog/topics/azure-maps/) (30)

Azure Marketplace (/en-us/blog/topics/azure-marketplace/) (145)

Azure Stream Analytics (/en-us/blog/topics/azure-stream-analytics/) (36)

Big Data (/en-us/blog/topics/big-data/) (649)

Blockchain (/en-us/blog/topics/blockchain/) (89)

Business Intelligence (/en-us/blog/topics/business-intelligence/) (119)

Cloud Strategy (/en-us/blog/topics/cloud-strategy/) (691)

Cognitive Services (/en-us/blog/topics/cognitive-services/) (126)

Data Science (/en-us/blog/topics/datascience/) (113)

Data Warehouse (/en-us/blog/topics/data-warehouse/) (222)

Database (/en-us/blog/topics/database/) (626)

Developer (/en-us/blog/topics/developer/) (1197)

DevOps (/en-us/blog/topics/devops/) (86)

Events (/en-us/blog/topics/events/) (249)

Government (/en-us/blog/topics/government/) (77)

Hybrid (/en-us/blog/topics/hybrid/) (83)

Identity & Access Management (/en-us/blog/topics/identity-access-management/) (88)

Internet of Things (/en-us/blog/topics/internet-of-things/) (383)

IT Pro (/en-us/blog/topics/it-pro/) (601)

Last week in Azure (/en-us/blog/topics/last-week-in-azure/) (92)

Machine Learning (/en-us/blog/topics/machine-learning/) (49)

Management (/en-us/blog/topics/management/) (386)

Media Services & CDN (/en-us/blog/topics/media-services/) (207)

Migration (/en-us/blog/topics/migration/) (36)

Mobile (/en-us/blog/topics/mobile/) (159)

Monitoring (/en-us/blog/topics/monitor/) (150)

Networking (/en-us/blog/topics/networking/) (231)

Partner (/en-us/blog/topics/partner/) (134)

Security (/en-us/blog/topics/security/) (405)

Serverless (/en-us/blog/topics/serverless/) (80)

Storage, Backup & Recovery (/en-us/blog/topics/storage-backup-and-recovery/) (697)

Supportability (/en-us/blog/topics/supportability/) (47)

Updates (/en-us/blog/topics/updates/) (580)

Virtual Machines (/en-us/blog/topics/virtual-machines/) (724)

Web (/en-us/blog/topics/web/) (371)

Articles by date

September 2021 (/en-us/blog/2021/09/)

August 2021 (/en-us/blog/2021/08/)

July 2021 (/en-us/blog/2021/07/)

June 2021 (/en-us/blog/2021/06/)

May 2021 (/en-us/blog/2021/05/)

April 2021 (/en-us/blog/2021/04/)

Full archive (/en-us/blog/archives/)