MICROLAND®
Extraordinary. Everyday.

AZURE SECURITY CENTER

SOLUTION PAPER

Abstract

The number of enterprises moving their workloads onto cloud is on the rise, given the flexibility and inherent advantages of cloud and its impact on business efficiencies. However due to the number of services hosted and updates being released regularly, cloud environments have become more vulnerable.
The Azure Security Center, offered as service in the Azure cloud, provides a reliable answer to these technical blockades on the security front. Azure Security Center offers integrated security monitoring and policy management across Azure subscriptions, helps detect threats that might otherwise go unnoticed and works with a broad ecosystem of security solutions.
Microland can set up and monitor things from a security, management and network standpoint for a customer to reap benefits of Azure (to apply security policies across hybrid cloud workloads to ensure compliance with security standards and collect, search and analyse security data from a variety of sources, including firewalls and other partner solutions. Microland can at the same time secure the client's IT environment from real time threats.

Azure Security Center

Security management is critical part of every organization's security and compliance strategy. Azure Security Center offered as Azure cloud service helps enterprises prevent, detect and respond to threats with increased visibility and control over the resources deployed within Azure. One of the best reasons to use Microsoft Azure cloud for enterprise applications and services is to take advantage of the wide array of security tools and capabilities available and make it possible to create secure solutions in a secure platform.

Azure Security Center can also be onboarded on VMs and computers running on-premises and in other clouds by simply installing the Microsoft Monitoring Agent on target machines.

Security challenges in Cloud

Cloud computing is the provisioning of computing services—servers, storage, databases, networking, software, analytics and more-over the Internet as on-demand service. The seller responding to all these computing requests is called as 'cloud provider'. Cloud computing services can be private, public or hybrid.

Faster implementations, lack of up-front cost, instant scalability and anywhere access—drives the push towards cloud computing across organizations. However, the security of data in the cloud is a key concern holding back cloud adoption for IT departments. Security threats may be classified as

- **Data Breach** is a security event when sensitive, protected or confidential data has potentially been viewed, stolen or used by an unauthorized source. If a data breach results in identity theft and/or a violation of government or industry compliance mandates, the offending organization may face fines or other civil or criminal prosecution.
- **Poor Identity Management** exposes customer records, which results in stolen user credentials. Organizations, planning to federate identity with cloud provider should understand the security used by provider to protect the identity platform. Organizational teams in charge of authenticating user identities and managing access to corporate resources must create a fine line, ensuring that the enterprise has robust security controls in place while integrating authentication procedures with cloud provider.
- **Insecure APIs** used by Web and cloud services to identify third-party applications do not adequately secure the keys to the cloud and their data. APIs handle everything "from authentication and access control to encryption and activity monitoring", as these APIs are the public front door to your Cloud application, an attacker with access to the API keys can cause a denial-of-service or rack up fees on behalf of the victim. Cloud and Web service developers must first follow best practices in opening their APIs to third parties.
- **System Vulnerabilities** are the system flaws or weaknesses that could be exploited to compromise the security of the cloud resource. Vulnerabilities have been found in every major operating system including Windows, macOS, various forms of Unix and Linux, OpenVMS, and others. The only way to reduce the chance of a vulnerability being used against a system is through constant compliance process, including system maintenance (e.g. applying software patches), implementing best practices in deployment (e.g. use of firewalls and access controls) and auditing (both during development and throughout the deployment lifecycle).
- **Malicious insiders** may be current or former employee, contractor, or other business partner who could create risk of a data breach, or data loss. Sometimes malicious instances could be the case of human error like people uploading sensitive files on unsanctioned applications, copying confidential information on cloud file sharing apps or making print screens of critical data and publishing it on unauthorized online services.
- **Advanced Persistent Threats** (APTs) refer to network attack in which an unauthorized person gains access to a network and stays there undetected for an extended period. Generally, APT hackers employ familiar methods, using phishing emails or other tricks to fool users into downloading malware. Once they gain access to the network, hacker will be more interested in stealing data and causing damage to the organization.

- **Denial of Service** typically performed by flooding a server say, the server of a web site - so much that it's unable to provide its services to legitimate users. Security techniques must be used in case of a DoS attack, such as deep packet inspection and application hardware placed on the network to analyze packets. These measures must be designed to scale to the level of attack, so they are not overwhelmed by malicious traffic.
- **Shared Technology** Cloud service providers share infrastructure, platforms, and applications, and if a vulnerability arises in any of these layers, it affects the whole setup. If security requirements and protocols are not integrated into the shared infrastructure at multiple levels (i.e. computing resources, storage, and networking) then vulnerabilities could exist.

Key modules in Azure Security Center

Security policy and data collection

Security policy is the defined set of controls recommended for resources within the specified subscription or resource group. Security policy classification can be varied as per the type of applications or sensitivity of the data in each subscription

Figure 1 Security Policy applied at Subscription and Resource Group level

Azure Security Center basically collects data from the following source,

Azure Service | Partner Solutions | Network Traffic | Virtual Machines

Roles and access controls

Security Center tasks can be distributed into individuals or teams as per the structure of your organization. Below infographic gives you general view on roles and security responsibilities assigned to individuals and teams:
Security Center helps enabling responsibilities for individuals and teams. Sample distribution of Security Center roles,

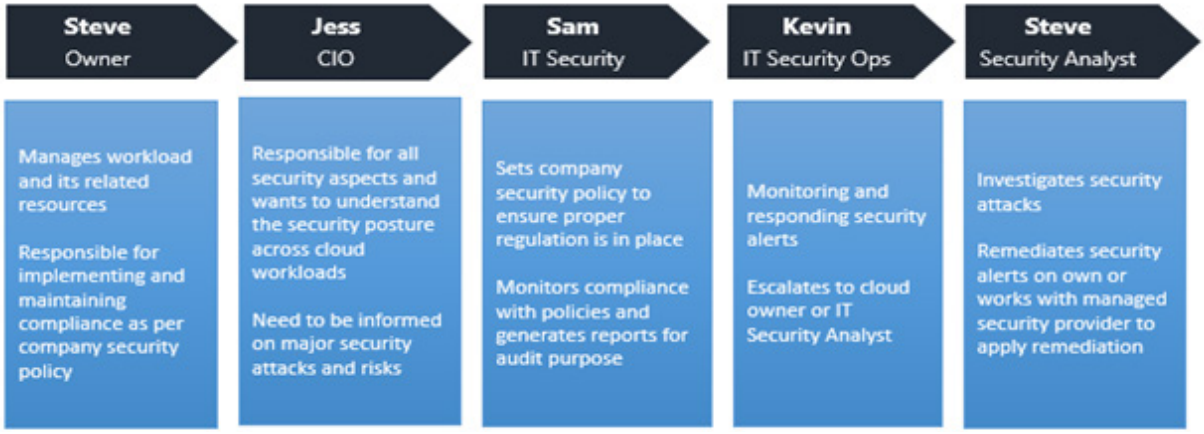

Figure 2 Azure Security Center Roles

Role-Based Access Control (RBAC) integrated with Security Center allows users roles to be assigned as per security actions executed. Also, assessing what types of tasks users will be performing in Security Center will help cloud administrators to configure RBAC accordingly.

Monitoring and recommendations

Monitoring is often believed to be as watching and waiting for an event to occur so that the customer can react to the situation. Security Center monitoring refers to taking a proactive strategy to audits cloud resources and identify systems that do not meet organizational standards or best practices.

Once security policies are enabled on the subscription or resource groups, Security Center analyzes the security of cloud resources to identify potential vulnerabilities. Information about cloud network configuration is available instantly while, it may take an hour or more for information about virtual machine configuration, such as security update status and operating system configuration, to become available.

Security Center monitoring is applicable to the below listed cloud resources,

- Virtual machines (VMs) (including Cloud Services)
- Azure Virtual Networks • Azure SQL service • Azure SQL service
- Partner solutions integrated with Azure subscription such as a web application firewall on VMs and on App Service Environment

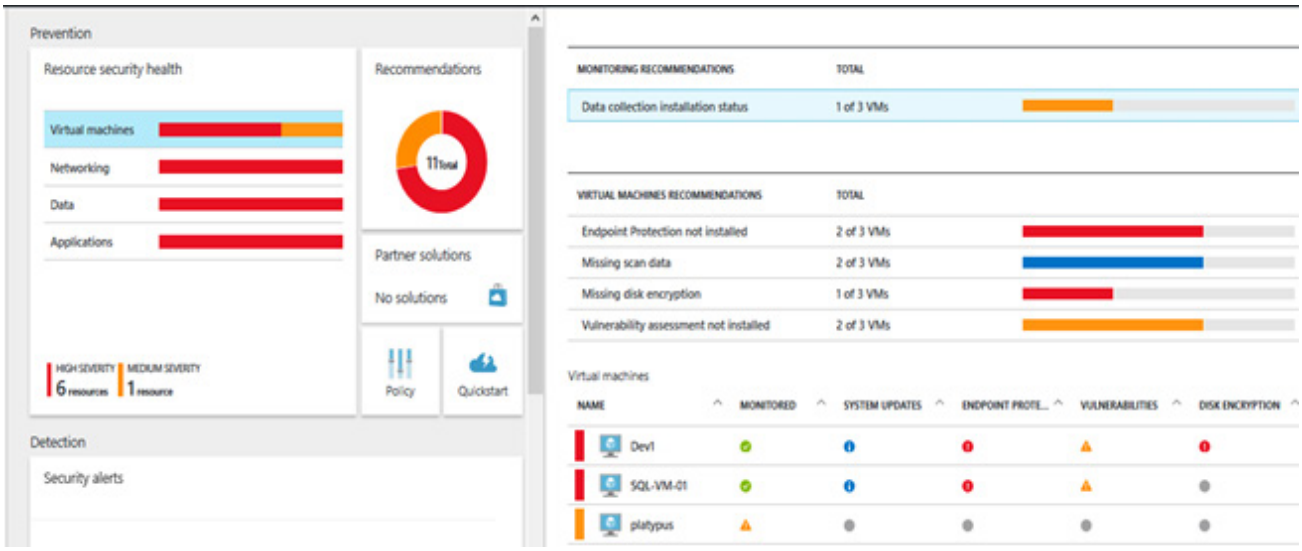

Figure 3 Monitoring status from Azure console

Operating Systems supported by Azure Security Center,

Windows VMs	Linux VMs
Windows Server 2008 R2	Ubuntu versions 12.04, 14.04, 16.04
Windows Server 2012	Debian versions 7, 8
Windows Server 2012 R2	CentOS versions 6.*, 7.*
	Red Hat Enterprise Linux (RHEL) versions 6.*, 7.*
	SUSE Linux Enterprise Server (SLES) versions 11.*, 12.*
	Oracle Linux versions 6.*, 7.*

Security Center recommends action for the cloud resources when vulnerabilities are identified.
Recommendations guides you configuring the required governance. Few sample from recommendations,

- Provisioning of antimalware to help identify and remove malicious software
- Provisioning web application firewall to help defend against attacks targeting your web applications
- Deploying missing system updates
- Addressing OS configurations that do not match the recommended baselines

DESCRIPTION	RE	STATE	SEVERITY	
Enable advanced security for subscriptions	1 s	Resolved	High	...
Enable data collection for subscriptions	1 s	Resolved	High	...
Provide security contact details	1 s	Resolved	Medium	...
Add a Next Generation Firewall	2 ı	Open	High	...
Enable Network Security Groups on subnets	2 :	Open	High	...
Install Endpoint Protection	2 ı	Open	High	...
Add a vulnerability assessment solution	2 ı	Open	Medium	...
Add a web application firewall	de	Open	High	...
Enable Network Security Groups on virtual ...	D(	Open	High	...
Apply disk encryption	D(	Open	High	...
Enable Auditing & Threat detection on SQL ...	m	Open	High	...
Enable Auditing & Threat detection on SQL ...	M	Open	High	...
Enable Transparent Data Encryption	M	Open	Medium	...
Restrict access through Internet facing endp...	SC	Open	Medium	...

Figure 4 Recommendations from Security Center

Managing and responding to security alerts

Azure Security Center automatically collects, analyzes and fuses log data from Azure resources and partner solutions like anti malware and firewalls. When threats are detected, a security alert is created.
Alert detection examples are,

- Compromised virtual machines communicating with known malicious IP addresses
- Advanced malware detected using Windows error reporting
- Brute force attacks against virtual machines
- Security alerts from integrated partner security solutions such as Anti-Malware or Web Application Firewalls.

Azure Security Center only has visibility into anti malware installed through Azure extensions and antimalware installed through pre-installed image or own manual process will be out of Security Center assessment.

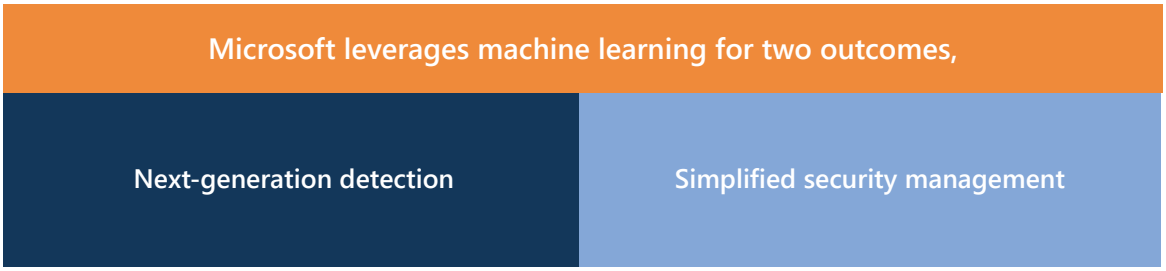

Figure 5 Machine learning influence in Security Center

Security Center has three categories of alerts,

- Virtual Machine Behavioral Analysis (VMBA)
- Network Analysis
- Resource Analysis

Once the detected threats are published as security alerts with priority along with recommendations on how to remediate the threat.

Security Center deploys advanced security analytics and machine learning technologies to evaluate events across the entire cloud fabric – detecting threats that would be impossible to identify using manual approaches and predicting the evolution of attacks. Security analytics include,

- Integrated Threat Intelligence
- Behavioral Analytics • Anomaly Detection

Vulnerability assessment in Azure Security Center

Vulnerability assessment in Azure Security Center is part of the virtual machine recommendations.

Security flaws are constantly being discovered and fixed by vendors, making it hard for organizations to keep up with security patches. Missing security updates are easy targets for attackers and can compromise the security of the entire network.

Azure Security Center offers integrated vulnerability assessment with Qualys cloud agents (preview) as part of the Virtual Machine recommendations. If a Virtual Machine is not deployed with vulnerability assessment solution, Security Center recommends that it be installed.

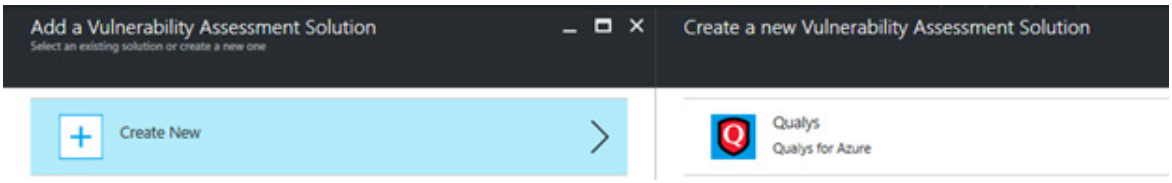

Figure 6 VA Solutions available in Security Center

Secure your deployments with your preferred partner

With on-premise environments expanding to hybrid cloud, customers often prefer to bring their trusted partners into cloud deployment. Azure Marketplace provides a variety of security solutions from leading vendors. Azure Security Center takes this additional step, by partnering with these vendors to provide an integrated experience in Azure, while relying on Marketplace for partner certification and billing. Deployment process may vary accordingly to the type of solution and partner.

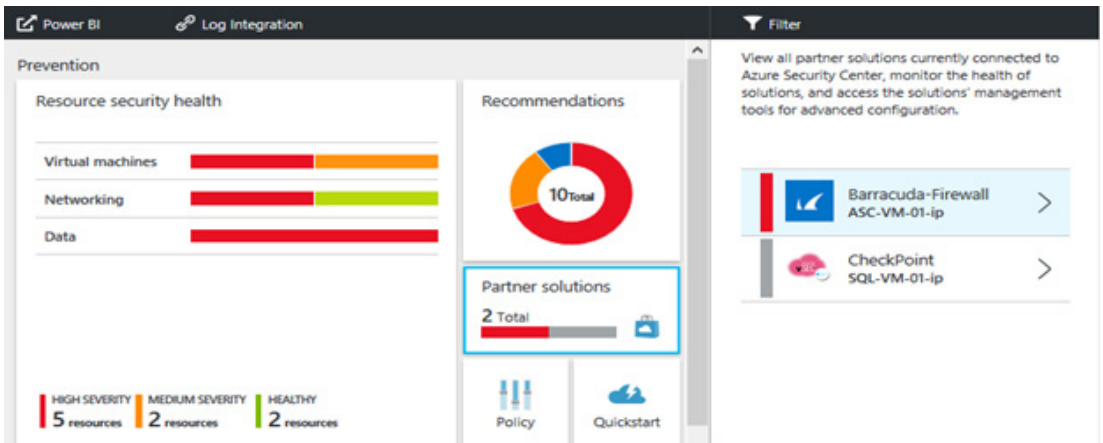

Figure 7 Partner Solutions integrated with Security Center

Security Center integrates with following partner solutions,

- Endpoint Protection (Trend Micro)
- Web Application Firewall (Barracuda, F5, Imperva and soon Microsoft WAF and Fortinet)
- Next Generation Firewall (Check Point, Barracuda and soon Fortinet and Cisco) solutions.
- Vulnerability Assessment (Qualys - preview) solutions.

Currently, Security Center integration works only for partner solutions that deployed from Security Center, by following a recommendation. Partner packages that are deployed directly from the Azure Marketplace through automation, are not yet supported. This support would be added over the next year where partner solutions will be auto discovered and connected to Security Center, regardless of their mode of deployment.

Using Azure Security Center for an incident response

Organizations think of security incident response only after witnessing a security attack. In Security Center, a security incident is an aggregation of all alerts for a resource that align with kill chain patterns.
Incident response not only warns you of premature attack, but it also brings costs and damage control to your resources in the cloud or on premise.

To be more effective, Incident planning should cover **protect, detect and respond** to threats as the core capabilities. Protect means preventing incidents, detect means detecting incidents in early stage and response is about evicting the attacker and restoring systems to mitigate the impacts of a breach.

Security Center can be used in detect, assess and diagnose stages of security incident life cycle.
Below example will explain how Security Center brings value during the three stages of initial incident response

- Detect: review the first indication of an alert investigation and review the initial verification that a high-priority security alert was raised in the Security Center dashboard.
- Assess: perform the initial assessment to obtain more information about the suspicious activity.
  Example: obtain more information about the security alert.
- Diagnose: conduct a technical investigation and identify containment, mitigation, and workaround strategies.

Visualize with Power BI

Azure Security Center offers increased visibility and insights into Azure resources and Azure workload security. Power BI content pack enables you to visualize, analyze, and filter recommendations and security alerts. To establish connection with content pack customer must provide Azure subscription ID and Azure Security account credentials. Once integrated, Power BI helps to visualize and analyze everything in one place so you can focus on what matters to you.

Figure 8 Security Center Insights from Power BI

Azure Security Center log integration

Every enterprise security operations and incident response teams rely on a Security Information and Event Management (SIEM) solution as the initial point for investigating security alerts. Azure log integration allows you to integrate raw logs from your Azure resources into your on-premises Security Information and Event Management (SIEM) systems. Azure log integration collects Azure Diagnostics from your Windows (WAD) virtual machines, Azure Activity Logs, Azure security center alerts and Azure Resource Provider logs.

Log integration provides a unified dashboard for all your assets, on-premises or in the cloud, so that you can aggregate, correlate, analyze, and alert for security events.
Azure log integration works with HP ArcSight, Splunk, IBM QRadar, and others.

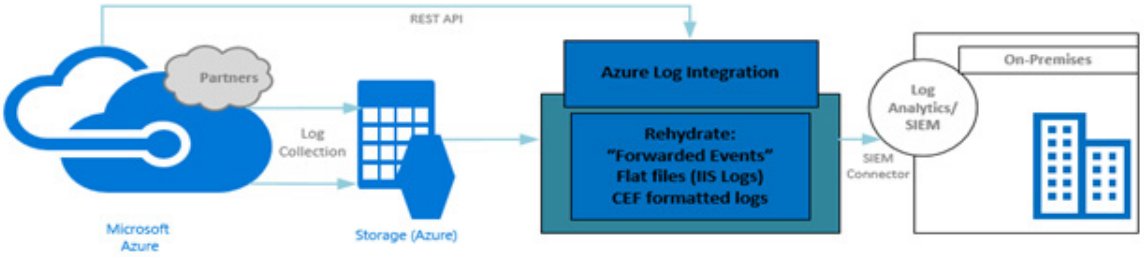

Figure 9 On-premise integration with Azure Security Center

Azure produces extensive logging for every service. Azure log integration currently supports the integration of Azure VM logs, Azure Audit Logs and Azure Security Center alerts.
The Azure log integration service collects telemetry data from the machine on which it is installed.

How Microland can help the customer

From an IT perspective, Microland can enable Azure Security Center on customers Azure subscription and monitor Azure services from a security, management and network standpoint.

For each subscription Microland can work according to each security policy on:

Turn on Data Collection

- Collect information from virtual machines about security health
- Check the configuration of Azure virtual machines
- Get security-event logs.

Integrate Partner Solutions

- Enable third-party applications for enhanced threat detection and vulnerability assessments
- Connect on premise SIEM systems using Microsoft Azure Log Integration

Get Visibility

- Cloud Security health status through security center APIs
- Power BI dashboard to view security state across Azure subscriptions

For customers using Azure subscription, Microland's Cloud Consultants can perform security audit of Azure services status using Security Center. Microland Consultants will help the customer in enabling the Security Center policy which will inspect following information through Azure Security Center and give the recommendations to IT Operations/ Security Teams for taking appropriate action.

- System updates
- Endpoint protection
- Network security groups
- Next generation firewall
- Storage encryption
- SQL auditing & Threat detection
- OS Vulnerabilities
- Disk encryption
- Web application firewall
- Vulnerability Assessment
- JIT Network Access
- SQL encryption

Having the above key aspects of Azure cloud services in safe and secure state using Security Center will ensure the customers that their cloud security landscape is standing tall against real time threats.

Conclusion

Security, in general, has been a concern for businesses entering cloud platform. This is largely because public cloud providers have a multi-tenant architecture and many vendors have evolved security tools and methods, such as encryption, identity access management and authentication, for public cloud deployments. Azure Security Center brings more value to customer by centralizing security event monitoring across resources. Because it looks at both – the security posture of each resource and gathers, analyzes, and correlates events, it has potential to be your single view of all Azure security data.

References

- Introduction to Azure Security Center
  https://docs.microsoft.com/en-us/azure/security-center/security-center-intro

- Azure Security Center for partner security solutions
  https://azure.microsoft.com/en-us/blog/top-4-reasons-for-using-azure-security-center-for-partner-security-solutions

- Azure Security Center on Microsoft mechanics
  https://blogs.msdn.microsoft.com/azuresecurity/2016/03/03/azure-security-center-on-microsoft-mechanics/

About the author

Anand Saravanan
LEAD ARCHITECT – Cloud Practice

Anand Saravanan is an Azure Certified Professional. He has 10 years of experience with strong skills on Azure architecting, design and deployment; solutions and migrating enterprise workload/ applications to Azure cloud. He has conducted several PoC on Azure Site Recovery and Assessments, architected cloud migration solutions and enterprise applications for various organizations across industry verticals in multiple geos. Anand has good experience on Microsoft System Center Suite, Active Directory, Microsoft Exchange, Lync and Blackberry (BES). Anand also focuses on research and evaluation of new technologies and tools that helps to migrating applications on Azure cloud.

For further information
Contact us at: + **201 793 7052** or Email us at : **cloud@microland.com**

About Microland

Microland is a leading Hybrid IT Infrastructure Service Provider and a trusted partner to enterprises in their IT-as-a-Service journey. Incorporated in 1989 and headquartered in Bangalore, India, Microland has more than 3,700 professionals across its offices in Australia, Europe, India, Middle East and United States. Microland enables global enterprises to become more agile and innovative through a comprehensive portfolio of services that addresses hybrid IT transformation, workspace transformation, service transformation and end-to-end IT infrastructure management.

Learn more about us at:

www.microland.com