Improve your security and insights with Azure Monitoring Services

Toni Pohl
CTO atwork, Azure and Office Dev MVP
@atwork | toni.pohl@atwork.at

NORTH AMERICAN COLLABORATION SUMMIT
2021
BRANSON MISSOURI

THANK YOU SPONSORS!

NORTH AMERICAN COLLABORATION SUMMIT

20 21

BRANSON MISSOURI

Diamond Sponsors

backupify
a datto company

tyGraph

Microsoft

AvePoint

Platinum Sponsors

Quest

NiCE
IT Management Solutions
www.nice.de

SC

KnowledgeLake
Intelligent Content Automation

WEBCON
LOW-CODE, BUT BETTER.

Gold Sponsors

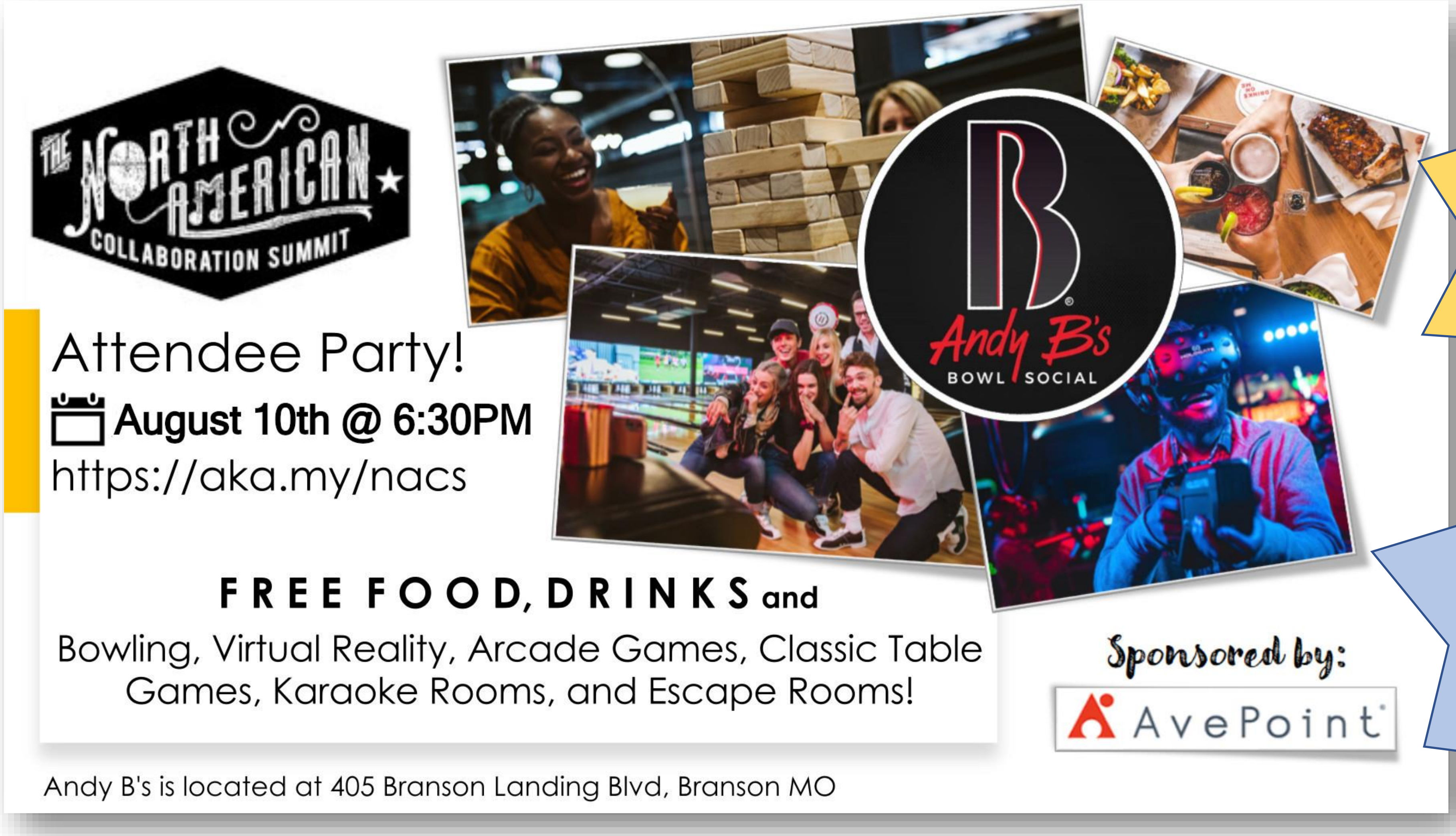
MARTELLO

ScriptRunner
The #1 for PowerShell Management

Hosted by:

PAIT GROUP

Be sure to visit each sponsor's channel in Microsoft Teams for prizes and extra entries in our big raffle prize drawing Wednesday!



THE NORTH AMERICAN COLLABORATION SUMMIT

Andy B's BOWL SOCIAL

Attendee Party!

August 10th @ 6:30PM

https://aka.my/nacs

FREE FOOD, DRINKS and

Bowling, Virtual Reality, Arcade Games, Classic Table Games, Karaoke Rooms, and Escape Rooms!

Sponsored by:

AvePoint

Andy B's is located at 405 Branson Landing Blvd, Branson MO

Just a short walk from the Convention Center!

Pick up free drink tickets during closing session Tuesday!

In order to attend, you must pick up wristbands during the end of day session on Tuesday at 4:15 in Taneycomo A

Join us for our end of day reception Wednesday starting at 3:45 in Taneycomo A for free food, drinks and raffle prizes!

NORTH AMERICAN COLLABORATION SUMMIT

20 21

BRANSON MISSOURI

*OPEN BAR

*Beer, wine, & soda

WIN PRIZES

WIN PRIZES

WIN PRIZES

Why monitoring?

Azure is **huge**!

Using the benefits of the cloud

Discover …
usage, cost, performance, **security**, and more

Find the scope to monitor

Is it a single app or service, or a group, or security, or performance, or costs, or … ?

Secure your services and get insights and monitor

App Insights

App Center

Network Watcher

Azure Monitor

Security Center

Azure Advisor

Azure Sentinel

Resource Graph

Cost manage ment

More…

App Insights + Log Analytics

“Create an Application Insights resource to monitor your live web application.”

Monitor desktop & web apps

- Usage, Failures, Availability, Performance, Application Map
- Tests
- App must not run in Azure
- Set alerts
- Continuous export for historic data

Kusto Query Language (aka KQL)

Applies to

- Azure Application Insights
- Azure Log Analytics
- Windows Defender Advanced Threat Protection
- Azure Security Center

```
requests
 | where timestamp > now(-1d)
 | summarize event_count=count() by bin(timestamp, 1h), client_CountryOrRegion
 | render piechart
```

Azure Monitor

“Get full stack visibility, find and fix problems, optimize your performance”

Overall monitoring system for multiple sources

Monitor data

- Azure Resources, Applications, VM Agents, Data collectors
- Log Analytics
- Metrics Explorer
- Create dashboards, insights, workbooks, and alerts

Network Watcher

“Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level.”

Find problems and troubleshoot

- Connections, IP flow, NSG, VPN, packets
- Tip for analyzing .cap: choco install wireshark

Azure Security Center

“Get continuous assessment and prioritized security recommendations with Azure secure score, and verify compliance with regulatory standards.”

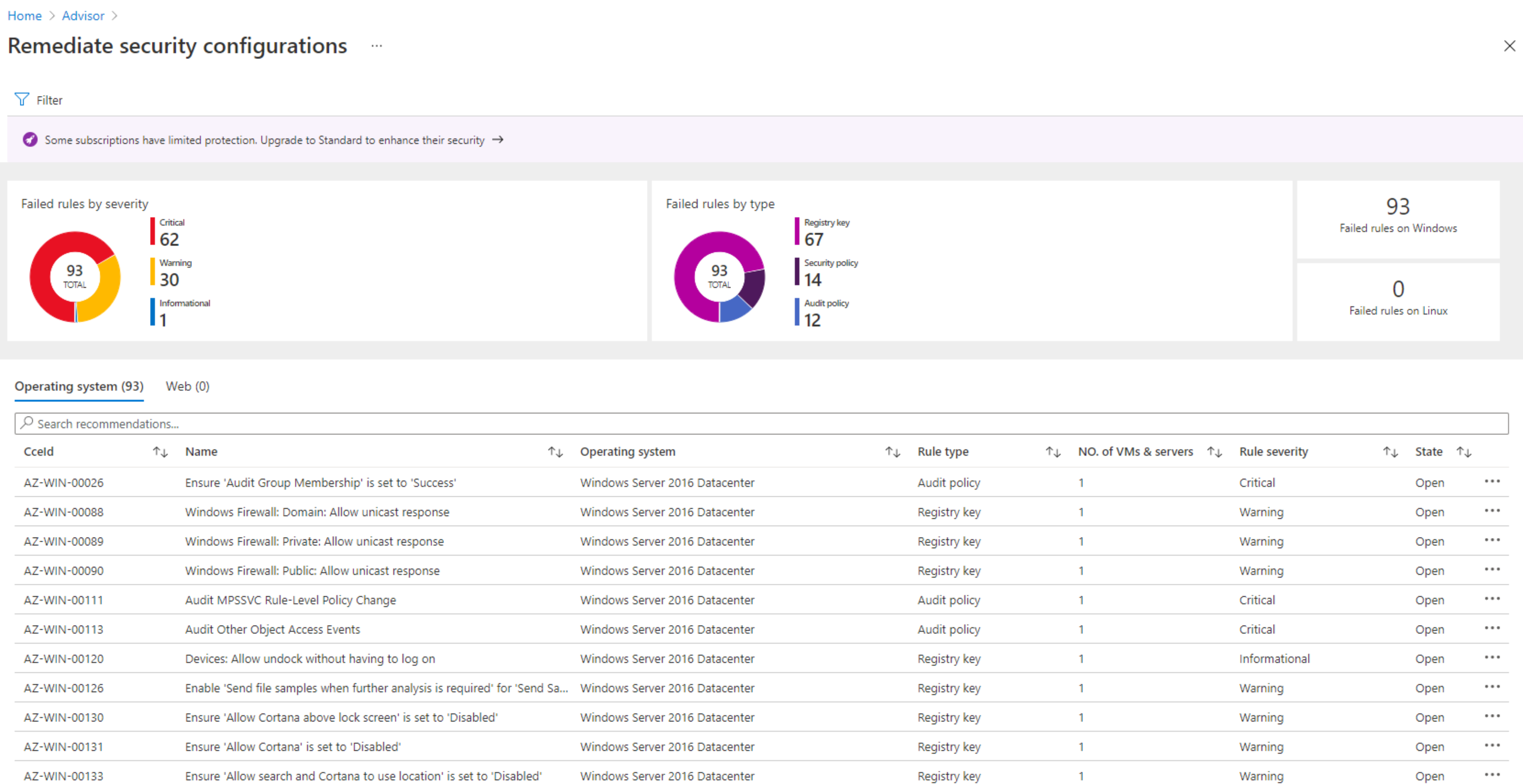
- Collect & Prevent *
- Detect incidents – Analytics & Hunting
- Investigate
- Respond

Azure Advisor

"…helps to identifying idle and underutilized resources, and delivers performance recommendations."

- Configuration defines what to check
- Cost (identify underutilized resources)
- Security (prevent, detect, and respond to threats)
- Performance issues (e.g. Upgrade)
- Advisor Score (new)

Typical recommendations for a VM



Home > Advisor >

Remediate security configurations ···

Filter

Some subscriptions have limited protection. Upgrade to Standard to enhance their security →

Failed rules by severity

93 TOTAL

Critical 62

Warning 30

Informational 1

Failed rules by type

93 TOTAL

Registry key 67

Security policy 14

Audit policy 12

93 Failed rules on Windows

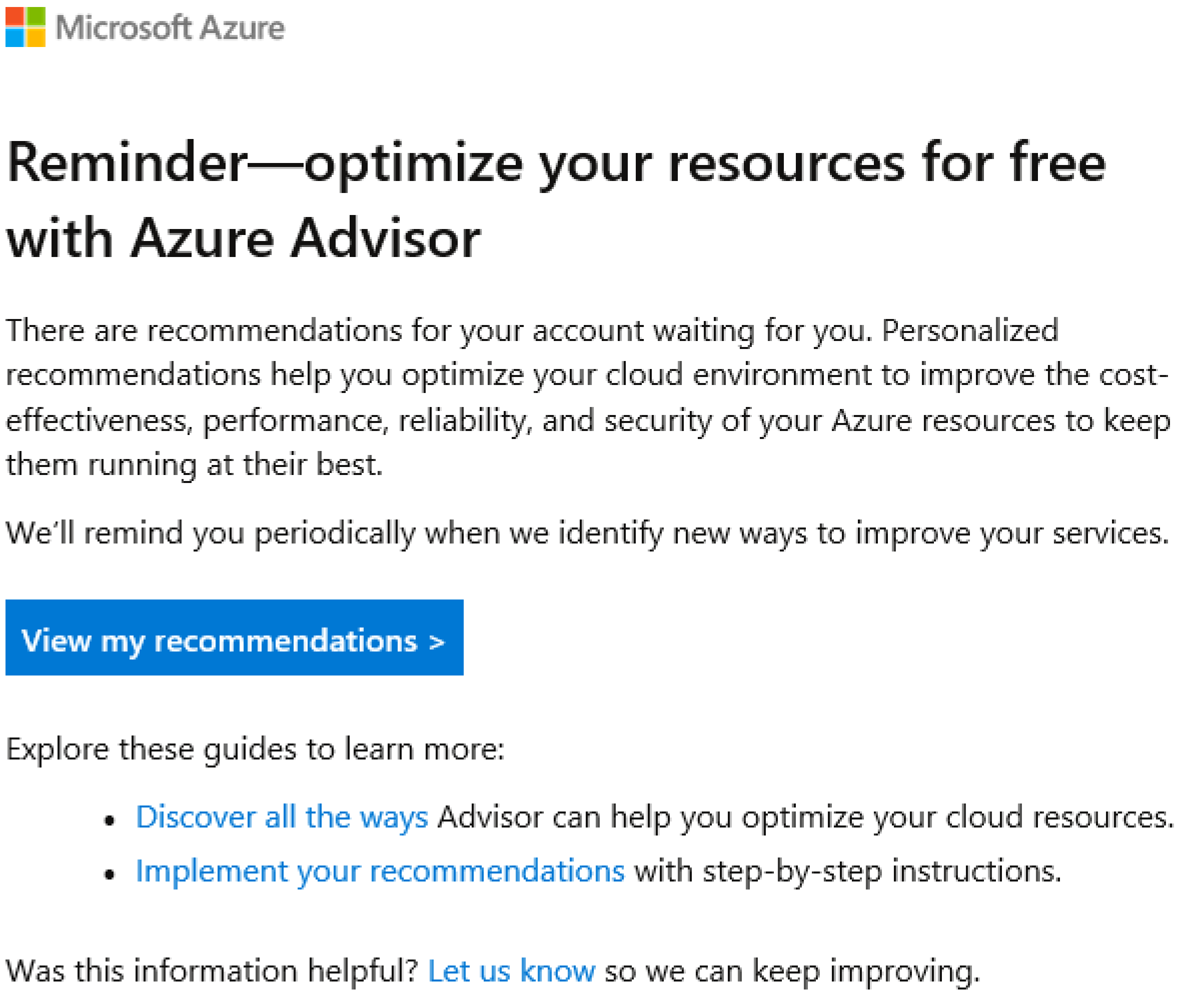
0 Failed rules on Linux

Operating system (93) Web (0)

Search recommendations...

CceId ↑↓	Name ↑↓	Operating system ↑↓	Rule type ↑↓	NO. of VMs & servers ↑↓	Rule severity ↑↓	State ↑↓	
AZ-WIN-00026	Ensure 'Audit Group Membership' is set to 'Success'	Windows Server 2016 Datacenter	Audit policy	1	Critical	Open	···
AZ-WIN-00088	Windows Firewall: Domain: Allow unicast response	Windows Server 2016 Datacenter	Registry key	1	Warning	Open	···
AZ-WIN-00089	Windows Firewall: Private: Allow unicast response	Windows Server 2016 Datacenter	Registry key	1	Warning	Open	···
AZ-WIN-00090	Windows Firewall: Public: Allow unicast response	Windows Server 2016 Datacenter	Registry key	1	Warning	Open	···
AZ-WIN-00111	Audit MPSSVC Rule-Level Policy Change	Windows Server 2016 Datacenter	Audit policy	1	Critical	Open	···
AZ-WIN-00113	Audit Other Object Access Events	Windows Server 2016 Datacenter	Audit policy	1	Critical	Open	···
AZ-WIN-00120	Devices: Allow undock without having to log on	Windows Server 2016 Datacenter	Registry key	1	Informational	Open	···
AZ-WIN-00126	Enable 'Send file samples when further analysis is required' for 'Send Sa...	Windows Server 2016 Datacenter	Registry key	1	Warning	Open	···
AZ-WIN-00130	Ensure 'Allow Cortana above lock screen' is set to 'Disabled'	Windows Server 2016 Datacenter	Registry key	1	Warning	Open	···
AZ-WIN-00131	Ensure 'Allow Cortana' is set to 'Disabled'	Windows Server 2016 Datacenter	Registry key	1	Warning	Open	···
AZ-WIN-00133	Ensure 'Allow search and Cortana to use location' is set to 'Disabled'	Windows Server 2016 Datacenter	Registry key	1	Warning	Open	···

Azure Advisor recommendations



Microsoft Azure

Reminder—optimize your resources for free with Azure Advisor

There are recommendations for your account waiting for you. Personalized recommendations help you optimize your cloud environment to improve the cost-effectiveness, performance, reliability, and security of your Azure resources to keep them running at their best.

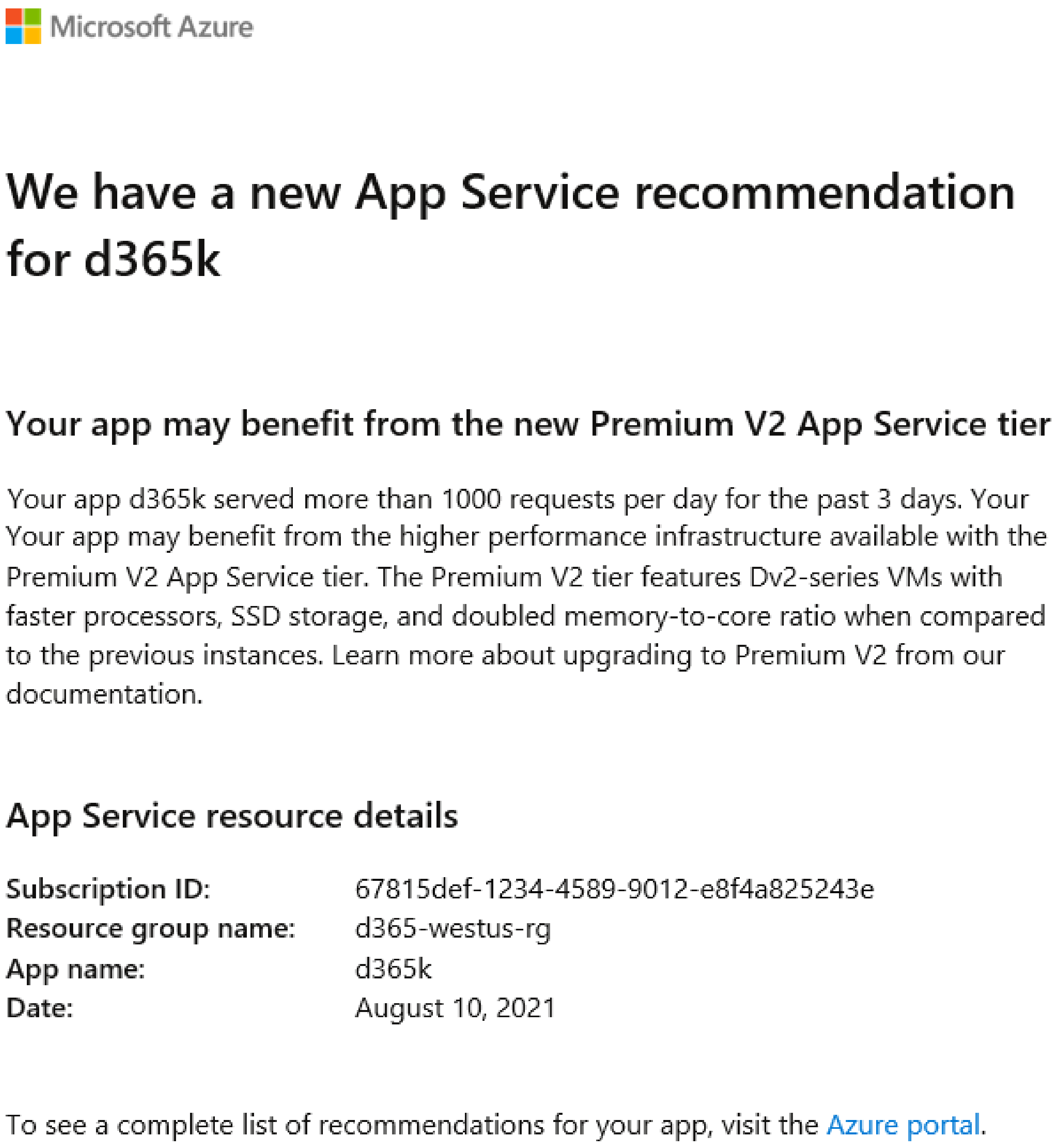
We'll remind you periodically when we identify new ways to improve your services.

Explore these guides to learn more:

- Discover all the ways Advisor can help you optimize your cloud resources.
- Implement your recommendations with step-by-step instructions.

Was this information helpful? Let us know so we can keep improving.

Azure Advisor



Microsoft Azure

We have a new App Service recommendation for d365k

Your app may benefit from the new Premium V2 App Service tier

Your app d365k served more than 1000 requests per day for the past 3 days. Your Your app may benefit from the higher performance infrastructure available with the Premium V2 App Service tier. The Premium V2 tier features Dv2-series VMs with faster processors, SSD storage, and doubled memory-to-core ratio when compared to the previous instances. Learn more about upgrading to Premium V2 from our documentation.

App Service resource details

Subscription ID:	67815def-1234-4589-9012-e8f4a825243e
Resource group name:	d365-westus-rg
App name:	d365k
Date:	August 10, 2021

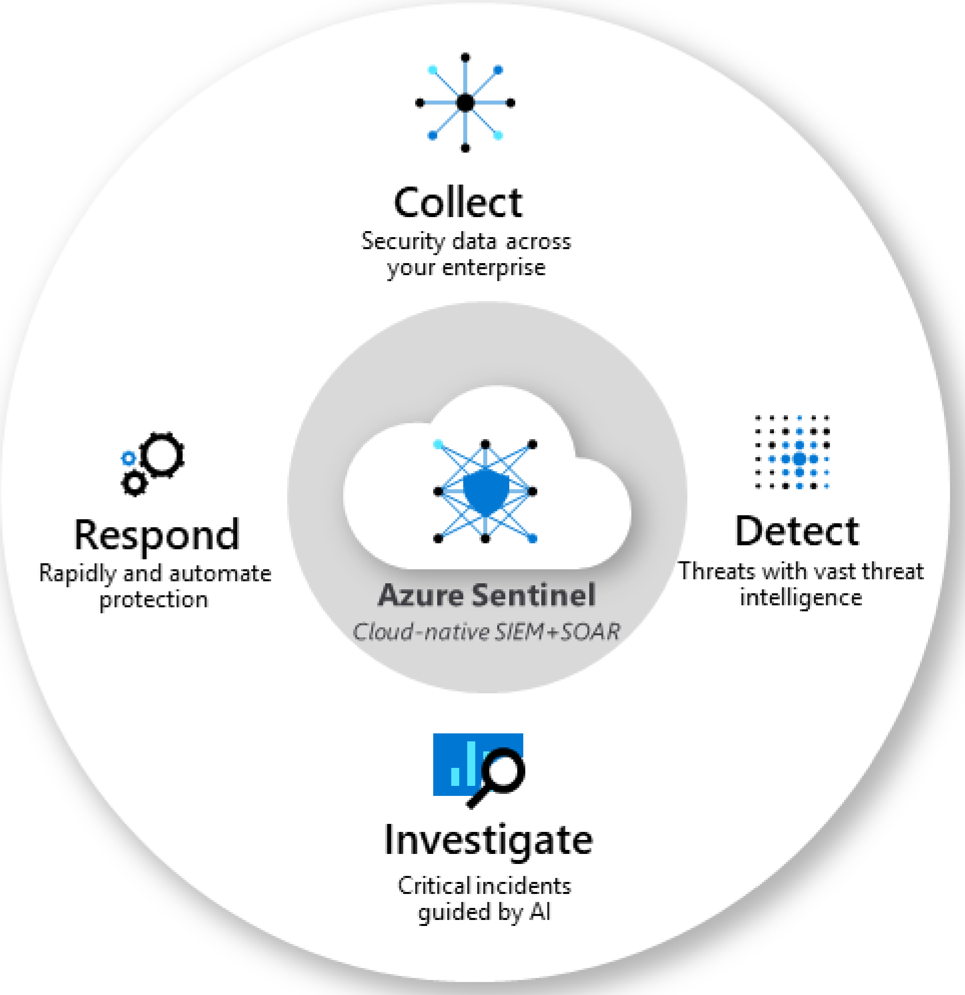
To see a complete list of recommendations for your app, visit the Azure portal.

Azure Sentinel

"Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise."

- A scalable, cloud-native, **security information event management (SIEM)** &
- A **Security orchestration automated response (SOAR)** solution

SIEM & SOAR? Features of Azure Sentinel



Collect

Security data across your enterprise

Respond

Rapidly and automate protection

Azure Sentinel

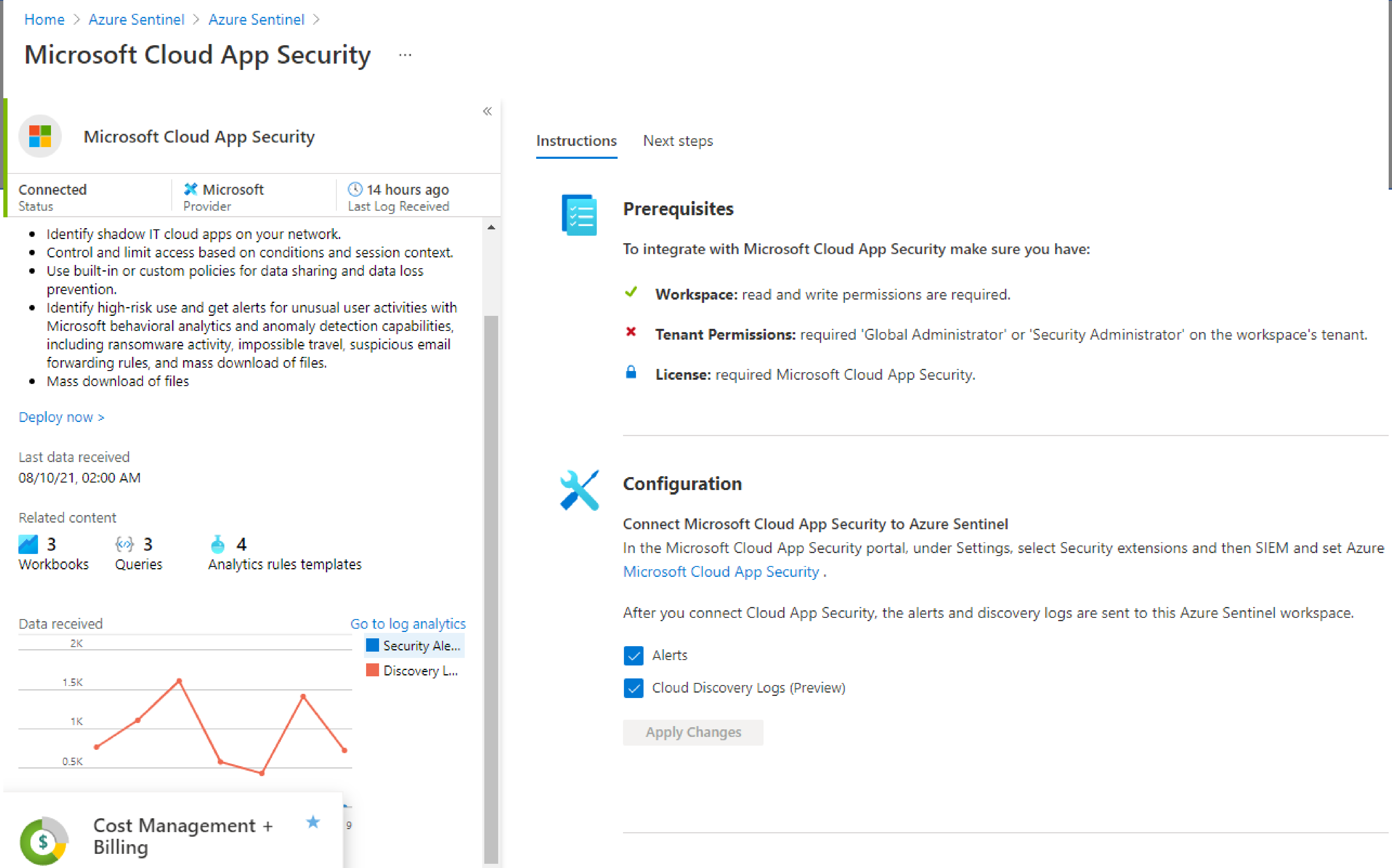
Cloud-native SIEM+SOAR

Detect

Threats with vast threat intelligence

Investigate

Critical incidents guided by AI



Home > Azure Sentinel > Azure Sentinel >

Microsoft Cloud App Security ···

Microsoft Cloud App Security

Connected	Microsoft	14 hours ago
Status	Provider	Last Log Received

- Identify shadow IT cloud apps on your network.
- Control and limit access based on conditions and session context.
- Use built-in or custom policies for data sharing and data loss prevention.
- Identify high-risk use and get alerts for unusual user activities with Microsoft behavioral analytics and anomaly detection capabilities, including ransomware activity, impossible travel, suspicious email forwarding rules, and mass download of files.
- Mass download of files

Deploy now >

Last data received
08/10/21, 02:00 AM

Related content

3 Workbooks | 3 Queries | 4 Analytics rules templates

Data received | Go to log analytics

Cost Management + Billing ★

Instructions | Next steps

Prerequisites

To integrate with Microsoft Cloud App Security make sure you have:

✓ **Workspace:** read and write permissions are required.

✗ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.

🔒 **License:** required Microsoft Cloud App Security.

Configuration

Connect Microsoft Cloud App Security to Azure Sentinel

In the Microsoft Cloud App Security portal, under Settings, select Security extensions and then SIEM and set Azure Microsoft Cloud App Security .

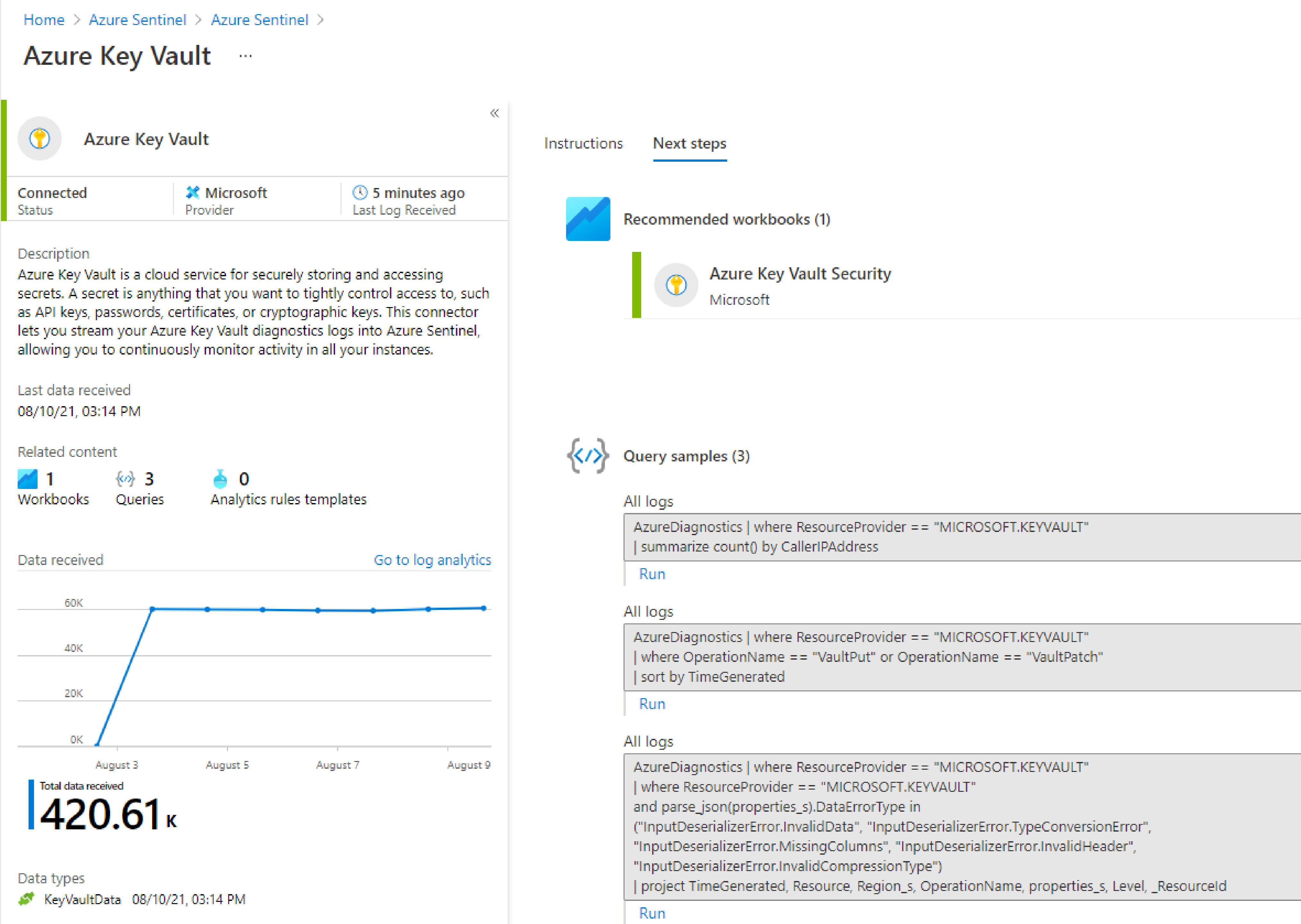
After you connect Cloud App Security, the alerts and discovery logs are sent to this Azure Sentinel workspace.

☑ Alerts

☑ Cloud Discovery Logs (Preview)

Apply Changes

Sample



Azure Key Vault

Azure Key Vault

Connected Status	Microsoft Provider	5 minutes ago Last Log Received

Description

Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys. This connector lets you stream your Azure Key Vault diagnostics logs into Azure Sentinel, allowing you to continuously monitor activity in all your instances.

Last data received

08/10/21, 03:14 PM

Related content

1 Workbooks	3 Queries	0 Analytics rules templates

Data received

Total data received

420.61 K

Data types

KeyVaultData 08/10/21, 03:14 PM

Recommended workbooks (1)

Azure Key Vault Security

Microsoft

Query samples (3)

All logs

```
AzureDiagnostics | where ResourceProvider == "MICROSOFT.KEYVAULT"
| summarize count() by CallerIPAddress
```

All logs

```
AzureDiagnostics | where ResourceProvider == "MICROSOFT.KEYVAULT"
| where OperationName == "VaultPut" or OperationName == "VaultPatch"
| sort by TimeGenerated
```

All logs

```
AzureDiagnostics | where ResourceProvider == "MICROSOFT.KEYVAULT"
| where ResourceProvider == "MICROSOFT.KEYVAULT"
and parse_json(properties_s).DataErrorType in
("InputDeserializerError.InvalidData", "InputDeserializerError.TypeConversionError",
"InputDeserializerError.MissingColumns", "InputDeserializerError.InvalidHeader",
"InputDeserializerError.InvalidCompressionType")
| project TimeGenerated, Resource, Region_s, OperationName, properties_s, Level, _ResourceId
```

App Center

“Continuously build, test, release, and monitor apps for every platform.”

- Integrate
- Test
- Distribute
- Security:
  - Multi-Tenant, Hosted in the US
  - App Center Test hosted in US+Denmark
  - CDNs
  - TLS 1.2
  - Encryption at rest (incl. Azure Storage, Azure SQL and Cosmos DB)

App Center is great for …

iOS apps
Swift and Objective-C

Android apps
Java and Kotlin

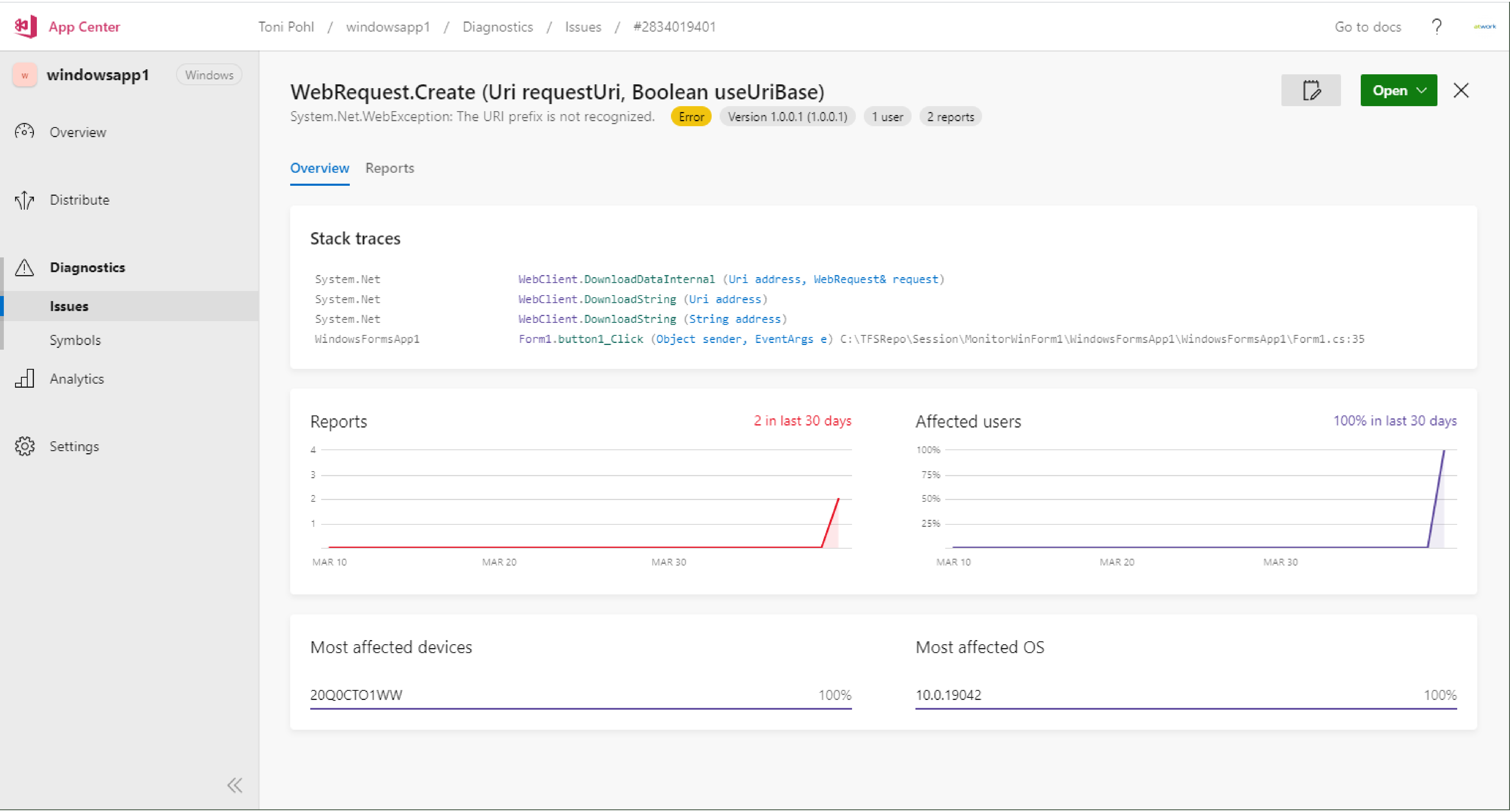
Windows apps
UWP, WPF and WinForms

React Native apps
iOS and Android

Xamarin apps
iOS and Android

Even more!
macOS, tvOS and Unity

Test your app (native and hybrid mobile apps)



WebRequest.Create (Uri requestUri, Boolean useUriBase)

System.Net.WebException: The URI prefix is not recognized. Error Version 1.0.0.1 (1.0.0.1) 1 user 2 reports

Stack traces

```
System.Net           WebClient.DownloadDataInternal (Uri address, WebRequest& request)
System.Net           WebClient.DownloadString (Uri address)
System.Net           WebClient.DownloadString (String address)
WindowsFormsApp1     Form1.button1_Click (Object sender, EventArgs e) C:\TFSRepo\Session\MonitorWinForm1\WindowsFormsApp1\WindowsFormsApp1\Form1.cs:35
```

Reports 2 in last 30 days

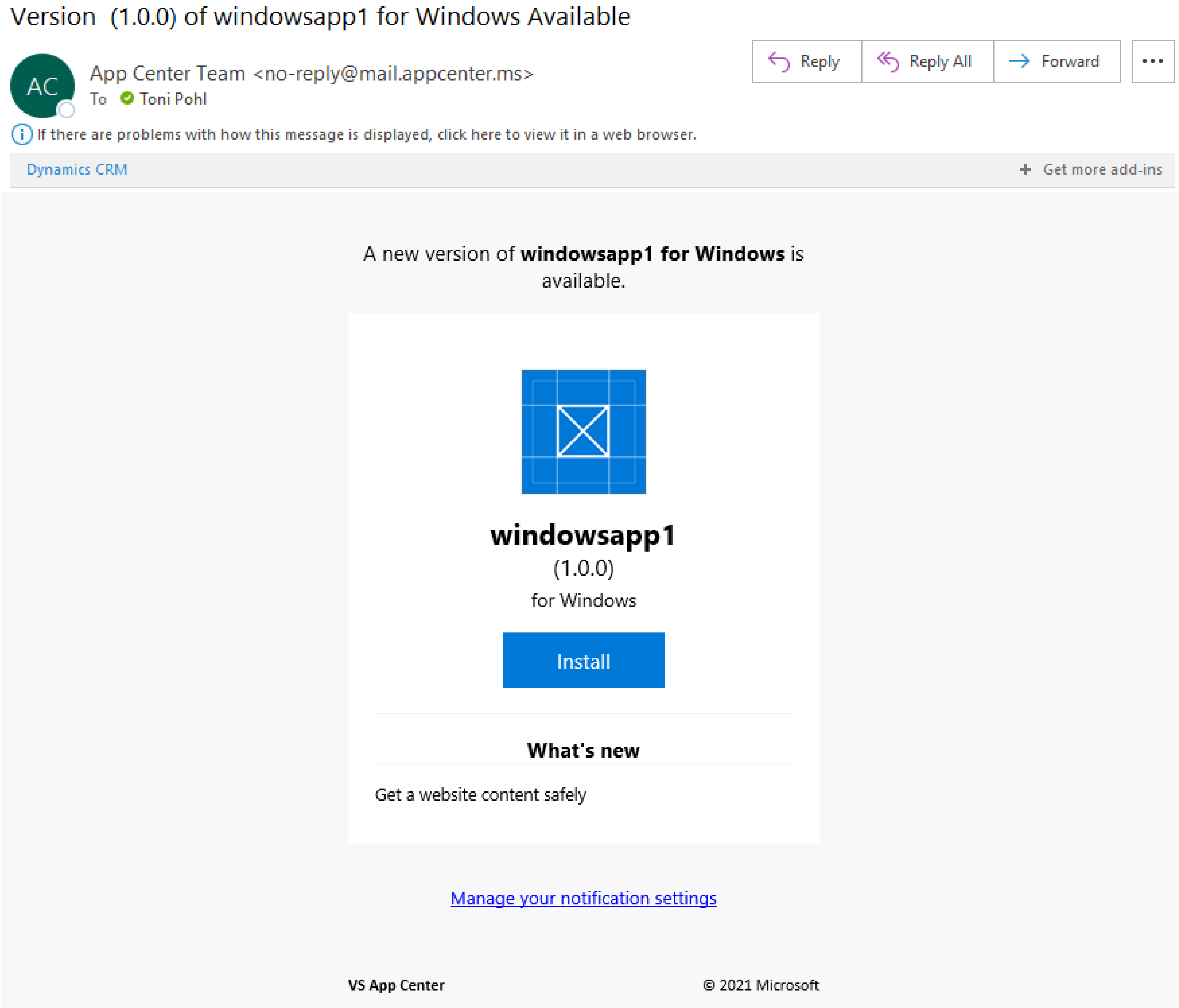
Affected users 100% in last 30 days

Most affected devices

20Q0CTO1WW	100%

Most affected OS

10.0.19042	100%



Version (1.0.0) of windowsapp1 for Windows Available

App Center Team <no-reply@mail.appcenter.ms>
To Toni Pohl

If there are problems with how this message is displayed, click here to view it in a web browser.

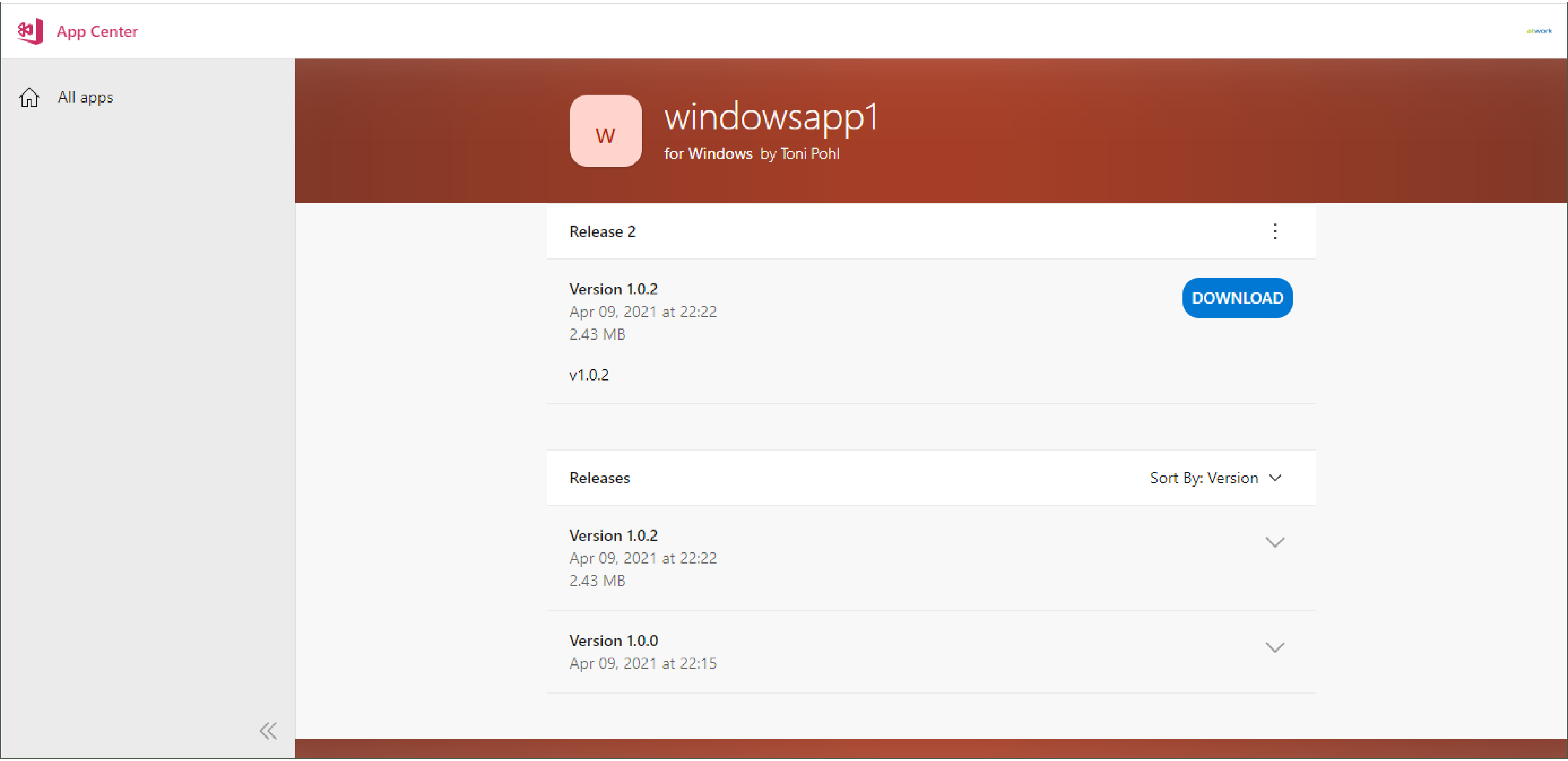
A new version of **windowsapp1 for Windows** is available.

windowsapp1
(1.0.0)
for Windows

What's new

Get a website content safely

VS App Center © 2021 Microsoft



windowsapp1

for Windows by Toni Pohl

Release 2

Version 1.0.2
Apr 09, 2021 at 22:22
2.43 MB

v1.0.2

Releases

Version 1.0.2
Apr 09, 2021 at 22:22
2.43 MB

Version 1.0.0
Apr 09, 2021 at 22:15

Resource Graph (Explorer + Queries)

“Get ad-hoc data from Azure Resource Manager”

- Answer queries with current data

Cost Management

“See the costs and get alerts.”

- Set alerts for cost limits

More

“Configure and develop your custom solutions.”

Standardize business processes

- Security Graph, Azure Logic Apps, Automation Accounts, Azure Functions, etc.
- Teams App Cloud Hub
  https://www.atwork-it.com/solutions/cloudhub/
- Governance Toolkit 365
  https://www.atwork-it.com/solutions/gt365/
- More third-party solutions

When to use what service

Task	App Insights	Network Watcher	Azure Monitor	Security Center	Azure Advisor	Azure Sentinel	App Center	Resource Graph	Cost Management
Monitor an app	🟢						🟠		
Inspect network traffic + diagn.		🟢							
Overview of multiple services			🟢		🟠				
Check security issues				🟢					
Actionable recommendations					🟢				
Investigate security issues				🟠		🟢			
Monitor & test mobile apps	🟢						🟢		
Get current resource data								🟢	
Cost management									🟢

Thank you!

Check out samples and links about Azure Monitoring on my GitHub repo toni.pohl

NORTH AMERICAN
COLLABORATION
SUMMIT
2021
BRANSON MISSOURI

https://www.collabsummit.org