Improve your security and insights with Azure monitoring services

Toni Pohl | MVP | @atwork

atwork

Sponsored by

Microsoft Teams Microsoft Tech Community

Why monitoring?

Azure is huge!

Using the benefits of the cloud

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

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 management

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
- App must not run in Azure (but it helps to simply enable the svc)
- 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 to monitor data

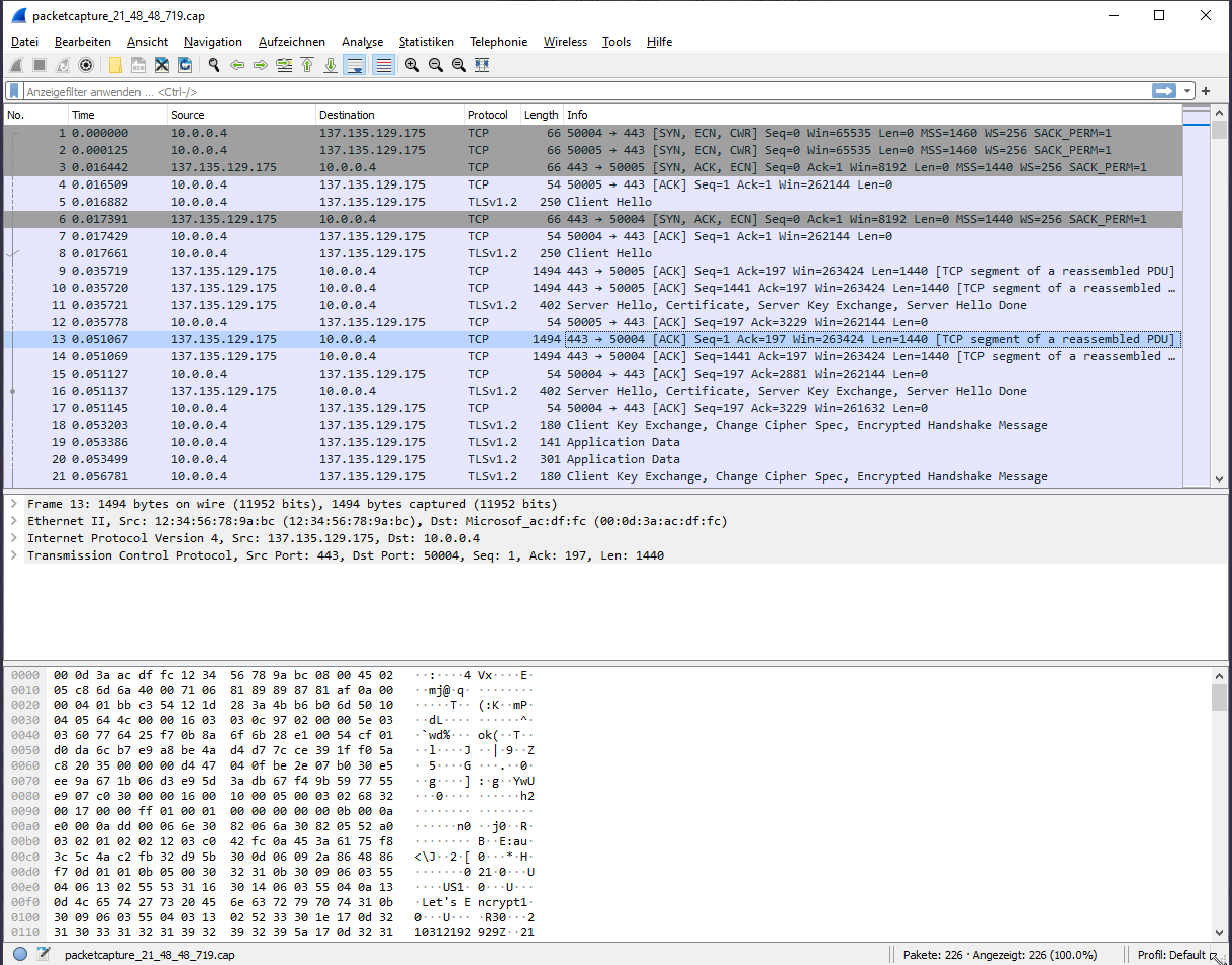
- Azure Resources, Applications, VM Agents,
  Data collectors
- Log Analytics
- Metrics Explorer
- Create dashboards, insights, workbooks, and alerts

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 files: choco install wireshark



```
No.   Time      Source           Destination      Protocol Length Info
    1 0.000000  10.0.0.4         137.135.129.175  TCP        66 50004 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
    2 0.000125  10.0.0.4         137.135.129.175  TCP        66 50005 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
    3 0.016442  137.135.129.175  10.0.0.4         TCP        66 443 → 50005 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
    4 0.016509  10.0.0.4         137.135.129.175  TCP        54 50005 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
    5 0.016882  10.0.0.4         137.135.129.175  TLSv1.2   250 Client Hello
    6 0.017391  137.135.129.175  10.0.0.4         TCP        66 443 → 50004 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
    7 0.017429  10.0.0.4         137.135.129.175  TCP        54 50004 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
    8 0.017661  10.0.0.4         137.135.129.175  TLSv1.2   250 Client Hello
    9 0.035719  137.135.129.175  10.0.0.4         TCP      1494 443 → 50005 [ACK] Seq=1 Ack=197 Win=263424 Len=1440 [TCP segment of a reassembled PDU]
   10 0.035720  137.135.129.175  10.0.0.4         TCP      1494 443 → 50005 [ACK] Seq=1441 Ack=197 Win=263424 Len=1440 [TCP segment of a reassembled …
   11 0.035721  137.135.129.175  10.0.0.4         TLSv1.2   402 Server Hello, Certificate, Server Key Exchange, Server Hello Done
   12 0.035778  10.0.0.4         137.135.129.175  TCP        54 50005 → 443 [ACK] Seq=197 Ack=3229 Win=262144 Len=0
   13 0.051067  137.135.129.175  10.0.0.4         TCP      1494 443 → 50004 [ACK] Seq=1 Ack=197 Win=263424 Len=1440 [TCP segment of a reassembled PDU]
   14 0.051069  137.135.129.175  10.0.0.4         TCP      1494 443 → 50004 [ACK] Seq=1441 Ack=197 Win=263424 Len=1440 [TCP segment of a reassembled …
   15 0.051127  10.0.0.4         137.135.129.175  TCP        54 50004 → 443 [ACK] Seq=197 Ack=2881 Win=262144 Len=0
   16 0.051137  137.135.129.175  10.0.0.4         TLSv1.2   402 Server Hello, Certificate, Server Key Exchange, Server Hello Done
   17 0.051145  10.0.0.4         137.135.129.175  TCP        54 50004 → 443 [ACK] Seq=197 Ack=3229 Win=261632 Len=0
   18 0.053203  10.0.0.4         137.135.129.175  TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   19 0.053386  10.0.0.4         137.135.129.175  TLSv1.2   141 Application Data
   20 0.053499  10.0.0.4         137.135.129.175  TLSv1.2   301 Application Data
   21 0.056781  10.0.0.4         137.135.129.175  TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
```

```
> Frame 13: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits)
> Ethernet II, Src: 12:34:56:78:9a:bc (12:34:56:78:9a:bc), Dst: Microsof_ac:df:fc (00:0d:3a:ac:df:fc)
> Internet Protocol Version 4, Src: 137.135.129.175, Dst: 10.0.0.4
> Transmission Control Protocol, Src Port: 443, Dst Port: 50004, Seq: 1, Ack: 197, Len: 1440
```

```
0000  00 0d 3a ac df fc 12 34  56 78 9a bc 08 00 45 02   ··:····4 Vx····E·
0010  05 c8 6d 6a 40 00 71 06  81 89 89 87 81 af 0a 00   ··mj@·q· ········
0020  00 04 01 bb c3 54 12 1d  28 3a 4b b6 b0 6d 50 10   ·····T·· (:K··mP·
0030  04 05 64 4c 00 00 16 03  03 0c 97 02 00 00 5e 03   ··dL···· ······^·
0040  03 60 77 64 25 f7 0b 8a  6f 6b 28 e1 00 54 cf 01   ·`wd%··· ok(··T··
0050  d0 da 6c b7 e9 a8 be 4a  d4 d7 7c ce 39 1f f0 5a   ··l····J ··|·9··Z
0060  c8 20 35 00 00 00 d4 47  04 0f be 2e 07 b0 30 e5   · 5····G ···.··0·
0070  ee 9a 67 1b 06 d3 e9 5d  3a db 67 f4 9b 59 77 55   ··g····] :·g··YwU
0080  e9 07 c0 30 00 00 16 00  10 00 05 00 03 02 68 32   ···0···· ······h2
0090  00 17 00 00 ff 01 00 01  00 00 00 00 00 0b 00 0a   ········ ········
00a0  e0 00 0a dd 00 06 6e 30  82 06 6a 30 82 05 52 a0   ······n0 ··j0··R·
00b0  03 02 01 02 02 12 03 c0  42 fc 0a 45 3a 61 75 f8   ········ B··E:au·
00c0  3c 5c 4a c2 fb 32 d9 5b  30 0d 06 09 2a 86 48 86   <\J··2·[ 0···*·H·
00d0  f7 0d 01 01 0b 05 00 30  32 31 0b 30 09 06 03 55   ·······0 21·0···U
00e0  04 06 13 02 55 53 31 16  30 14 06 03 55 04 0a 13   ····US1· 0···U···
00f0  0d 4c 65 74 27 73 20 45  6e 63 72 79 70 74 31 0b   ·Let's E ncrypt1·
0100  30 09 06 03 55 04 03 13  02 52 33 30 1e 17 0d 32   0···U··· ·R30···2
0110  31 30 33 31 32 31 39 32  39 32 39 5a 17 0d 32 31   10312192 929Z··21
```

packetcapture_21_48_48_719.cap
Pakete: 226 · Angezeigt: 226 (100.0%)
Profil: Default

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

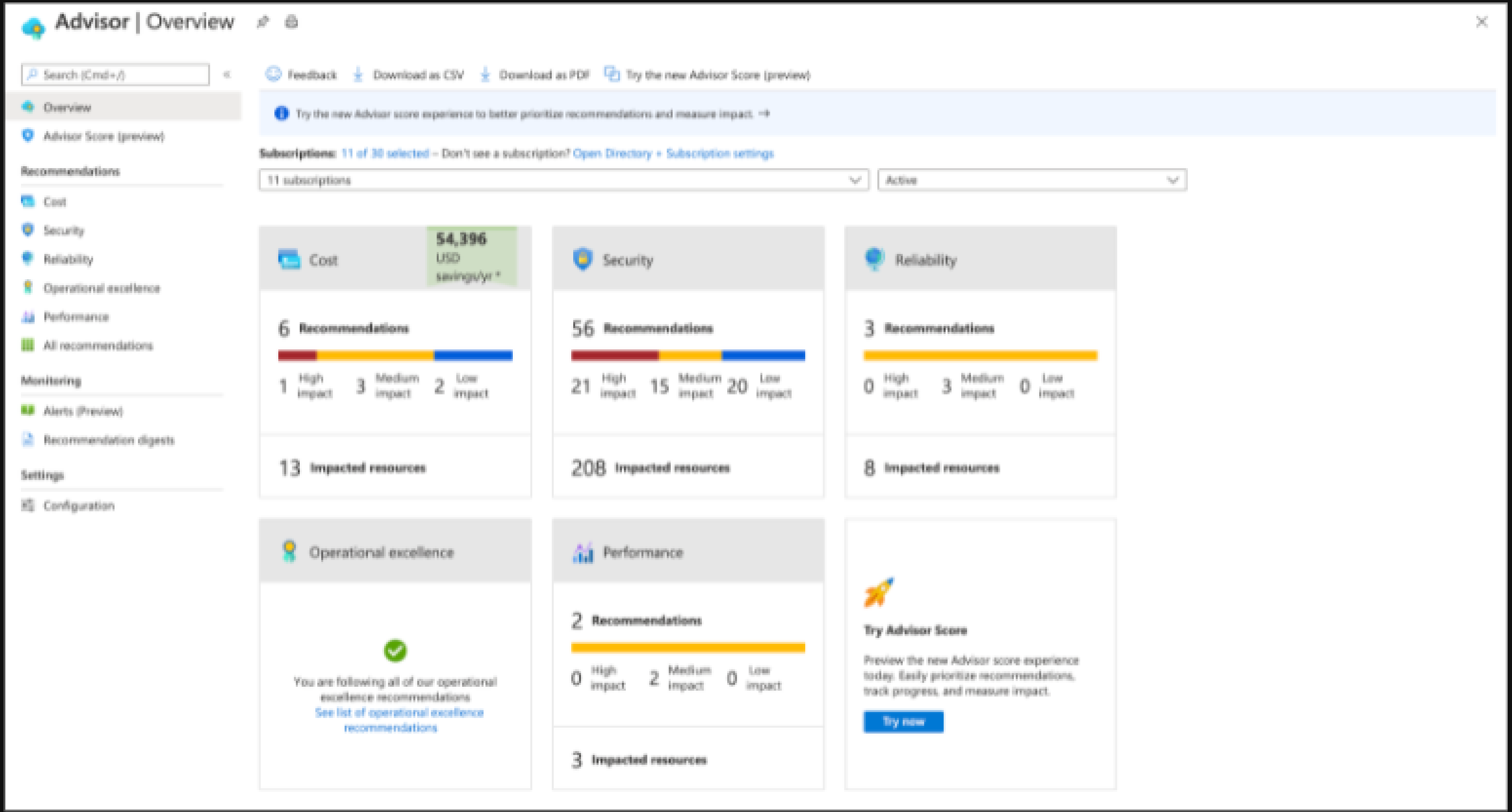
Azure Advisor

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

- Configuration defines what to check
- Cost
- Security
- Performance, e.g. Upgrade
- Advisor Score (new)

Optimize your cloud workloads with personalized recommendations

With your Azure account, you get free, personalized recommendations to help you optimize your cloud workloads. Start with Azure Advisor recommendations—based on an analysis of your Azure usage—to improve cost-efficiency, security, reliability, performance, and operational excellence. Learn more



Try the new Advisor score experience to better prioritize recommendations and measure impact. →

Subscriptions: 11 of 30 selected – Don't see a subscription? Open Directory + Subscription settings

11 subscriptions

Active

Cost — 54,396 USD savings/yr *
6 Recommendations
1 High impact 3 Medium impact 2 Low impact
13 Impacted resources

Security
56 Recommendations
21 High impact 15 Medium impact 20 Low impact
208 Impacted resources

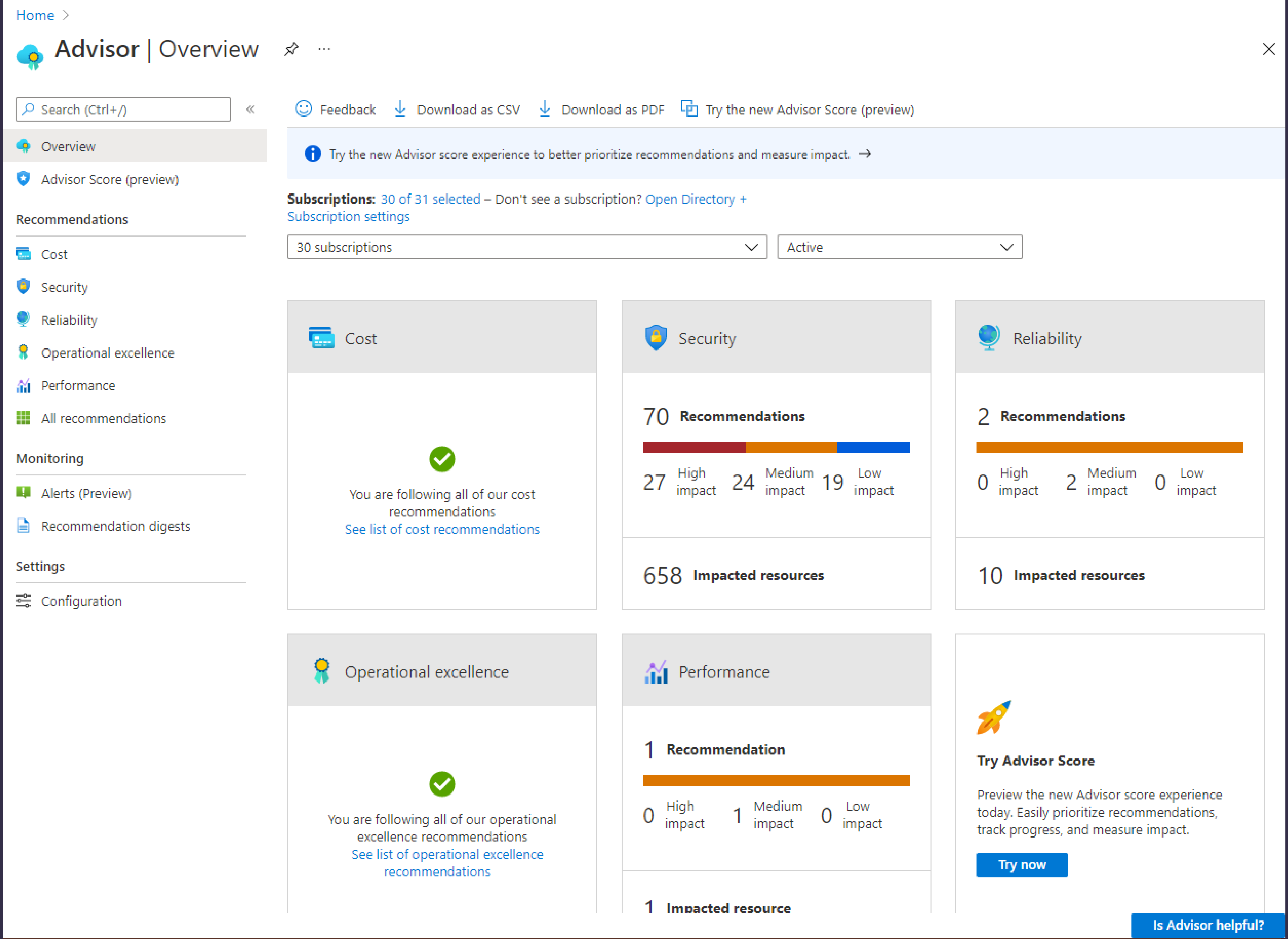
Reliability
3 Recommendations
0 High impact 3 Medium impact 0 Low impact
8 Impacted resources

Operational excellence
You are following all of our operational excellence recommendations
See list of operational excellence recommendations

Performance
2 Recommendations
0 High impact 2 Medium impact 0 Low impact
3 Impacted resources

Try Advisor Score
Preview the new Advisor score experience today. Easily prioritize recommendations, track progress, and measure impact.

See recommendations >



Home >

Advisor | Overview

Recommendations

Monitoring

Settings

Try the new Advisor score experience to better prioritize recommendations and measure impact. →

Subscriptions: 30 of 31 selected – Don't see a subscription? Open Directory + Subscription settings

30 subscriptions ⌄ | Active ⌄

Cost

✓

You are following all of our cost recommendations

See list of cost recommendations

Security

70 **Recommendations**

27 High impact 24 Medium impact 19 Low impact

658 **Impacted resources**

Reliability

2 **Recommendations**

0 High impact 2 Medium impact 0 Low impact

10 **Impacted resources**

Operational excellence

✓

You are following all of our operational excellence recommendations

See list of operational excellence recommendations

Performance

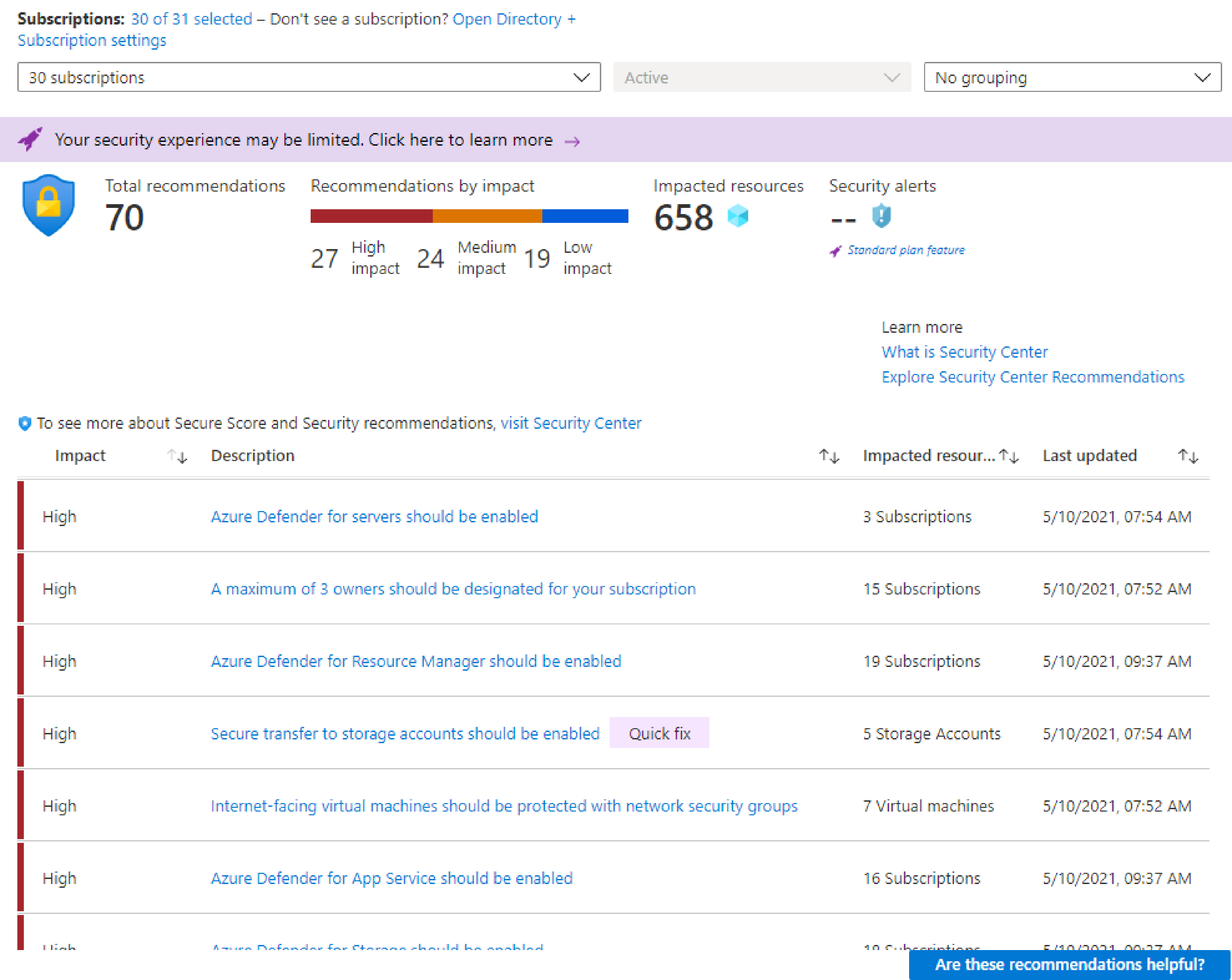
1 **Recommendation**

0 High impact 1 Medium impact 0 Low impact

1 **Impacted resource**

Try Advisor Score

Preview the new Advisor score experience today. Easily prioritize recommendations, track progress, and measure impact.



Subscriptions: 30 of 31 selected – Don't see a subscription? Open Directory + Subscription settings

30 subscriptions | Active | No grouping

Your security experience may be limited. Click here to learn more →

Total recommendations
70

Recommendations by impact
27 High impact 24 Medium impact 19 Low impact

Impacted resources
658

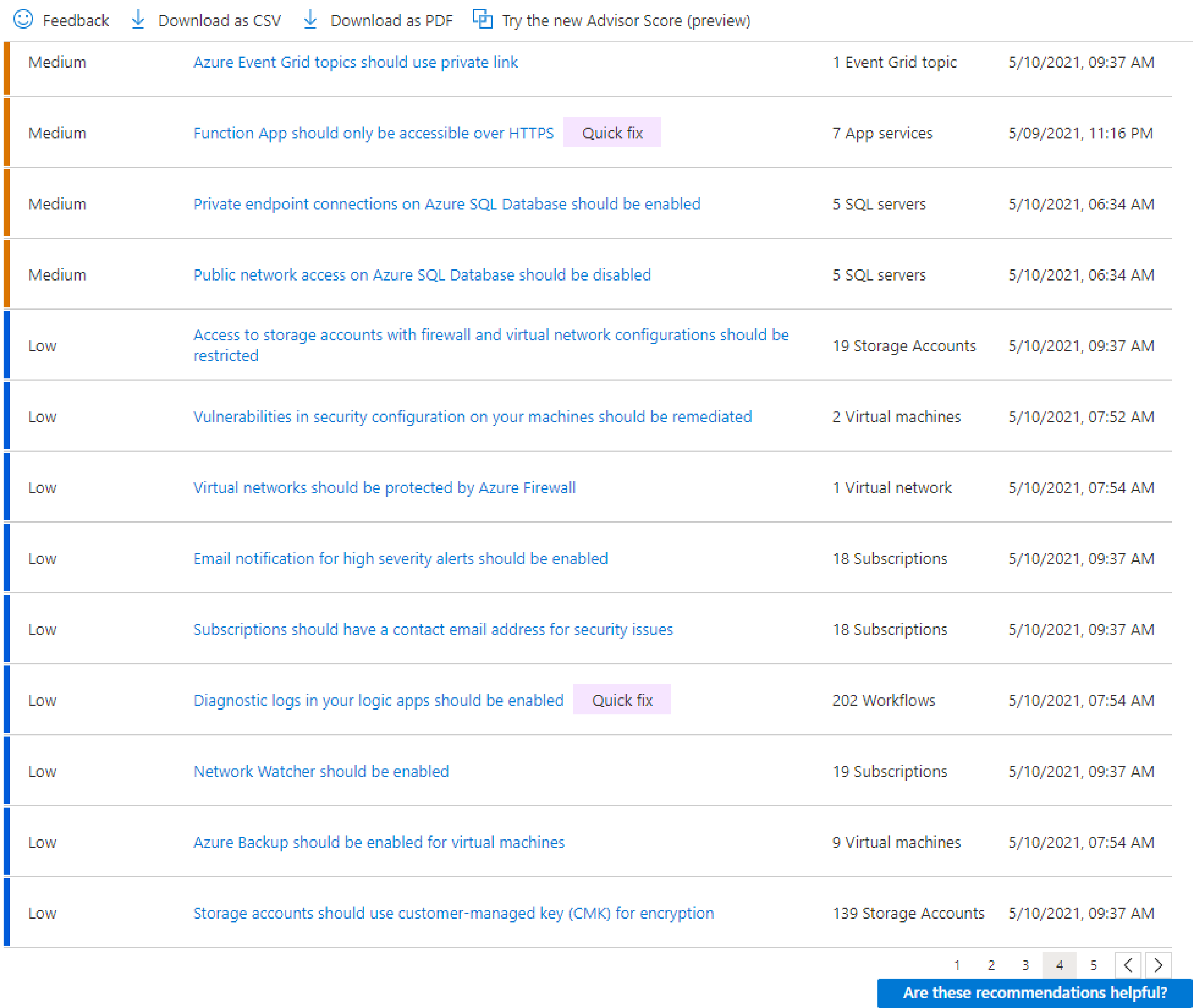
Security alerts
--
Standard plan feature

Learn more
What is Security Center
Explore Security Center Recommendations

To see more about Secure Score and Security recommendations, visit Security Center

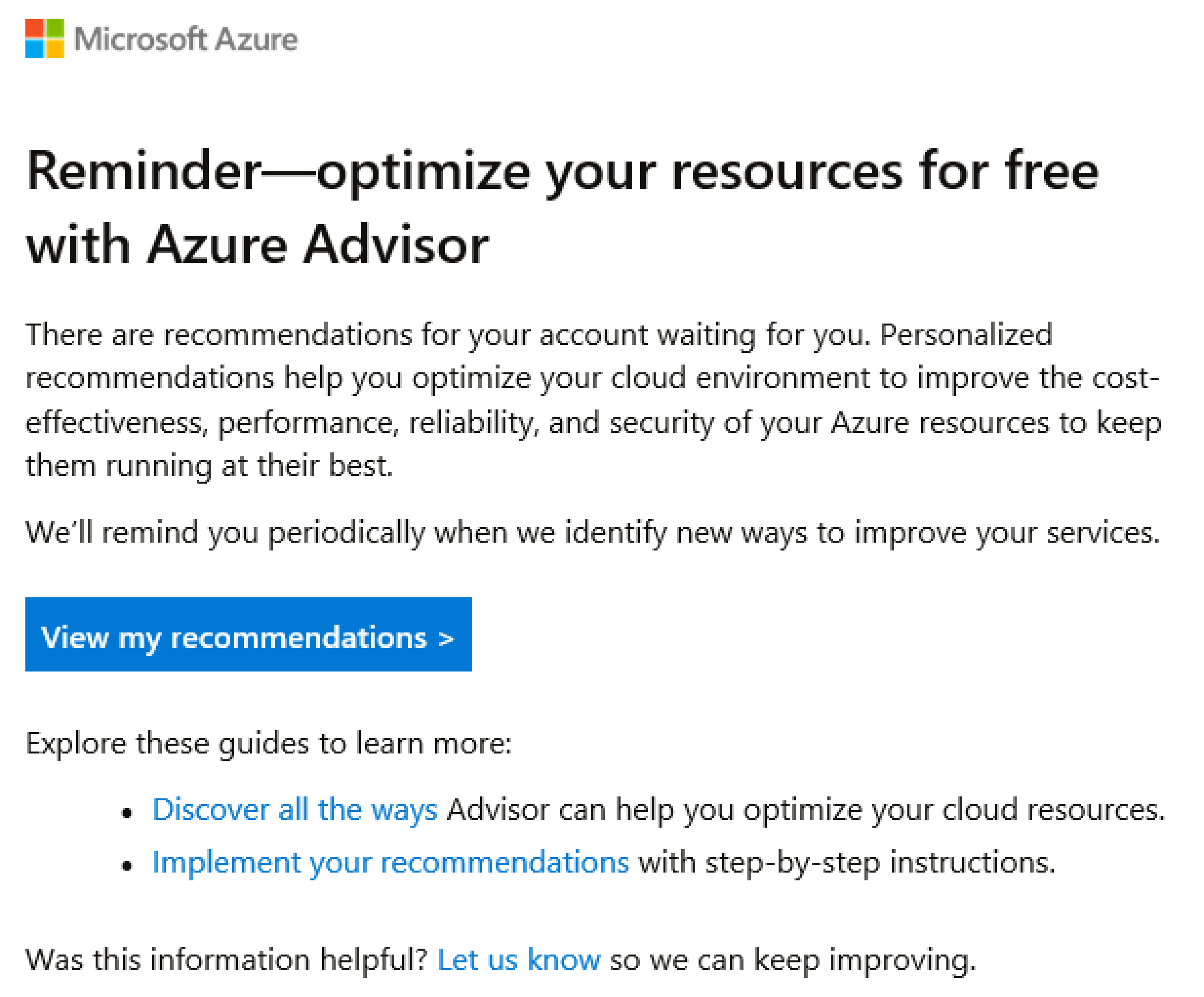
Impact	Description	Impacted resour...	Last updated
High	Azure Defender for servers should be enabled	3 Subscriptions	5/10/2021, 07:54 AM
High	A maximum of 3 owners should be designated for your subscription	15 Subscriptions	5/10/2021, 07:52 AM
High	Azure Defender for Resource Manager should be enabled	19 Subscriptions	5/10/2021, 09:37 AM
High	Secure transfer to storage accounts should be enabled Quick fix	5 Storage Accounts	5/10/2021, 07:54 AM
High	Internet-facing virtual machines should be protected with network security groups	7 Virtual machines	5/10/2021, 07:52 AM
High	Azure Defender for App Service should be enabled	16 Subscriptions	5/10/2021, 09:37 AM
High	Azure Defender for Storage should be enabled	19 Subscriptions	5/10/2021, 09:37 AM

Are these recommendations helpful?



Medium	Azure Event Grid topics should use private link	1 Event Grid topic	5/10/2021, 09:37 AM
Medium	Function App should only be accessible over HTTPS Quick fix	7 App services	5/09/2021, 11:16 PM
Medium	Private endpoint connections on Azure SQL Database should be enabled	5 SQL servers	5/10/2021, 06:34 AM
Medium	Public network access on Azure SQL Database should be disabled	5 SQL servers	5/10/2021, 06:34 AM
Low	Access to storage accounts with firewall and virtual network configurations should be restricted	19 Storage Accounts	5/10/2021, 09:37 AM
Low	Vulnerabilities in security configuration on your machines should be remediated	2 Virtual machines	5/10/2021, 07:52 AM
Low	Virtual networks should be protected by Azure Firewall	1 Virtual network	5/10/2021, 07:54 AM
Low	Email notification for high severity alerts should be enabled	18 Subscriptions	5/10/2021, 09:37 AM
Low	Subscriptions should have a contact email address for security issues	18 Subscriptions	5/10/2021, 09:37 AM
Low	Diagnostic logs in your logic apps should be enabled Quick fix	202 Workflows	5/10/2021, 07:54 AM
Low	Network Watcher should be enabled	19 Subscriptions	5/10/2021, 09:37 AM
Low	Azure Backup should be enabled for virtual machines	9 Virtual machines	5/10/2021, 07:54 AM
Low	Storage accounts should use customer-managed key (CMK) for encryption	139 Storage Accounts	5/10/2021, 09:37 AM

Azure Advisor recommendations - reminders



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.

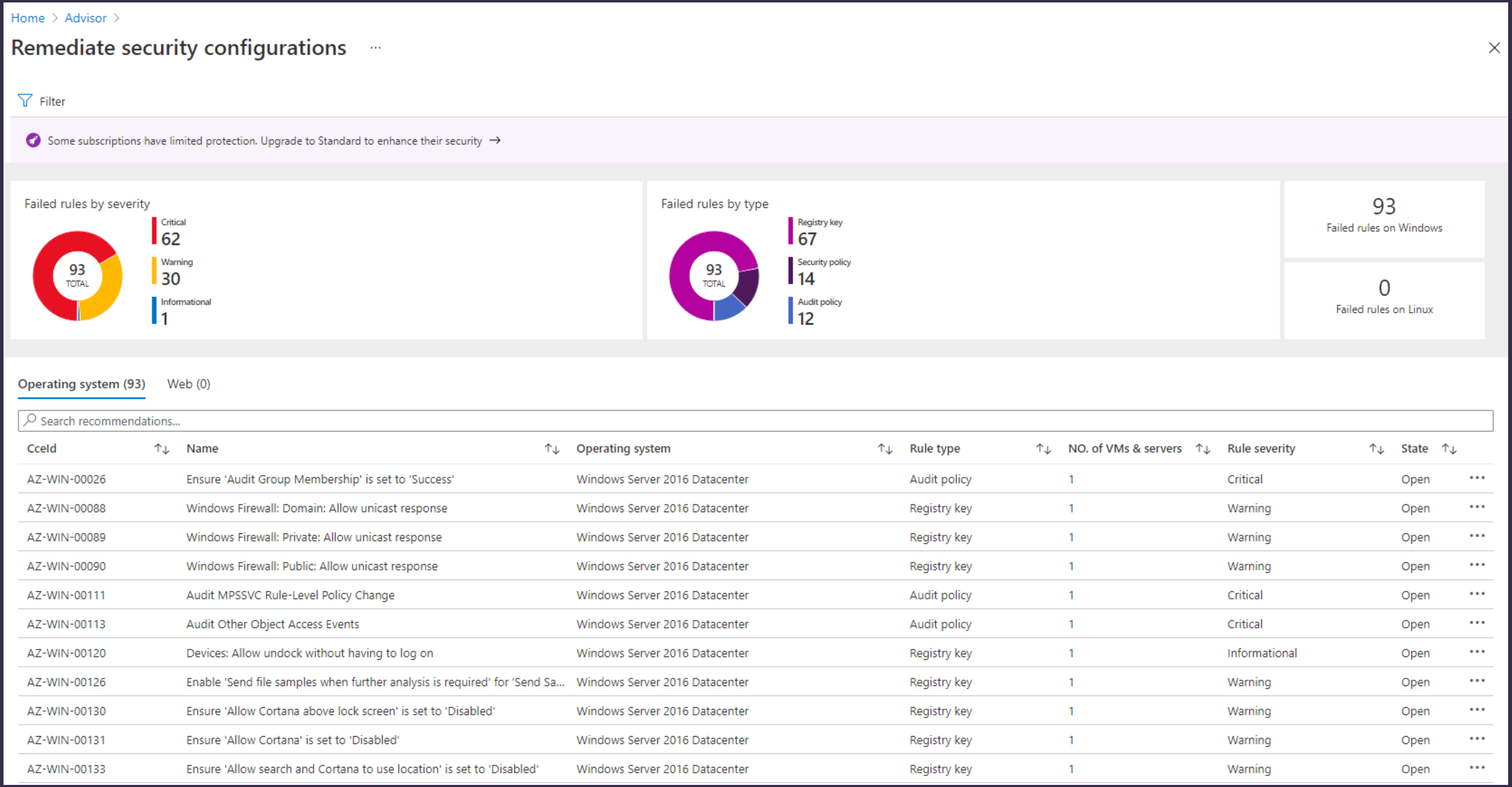
We'll remind you periodically when we identify new ways to improve your services.

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.

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 Sentinel

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

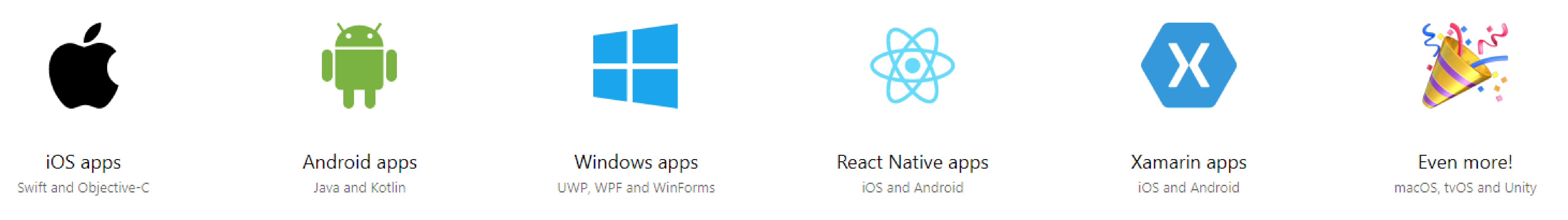
- Collect & Prevent
- Detect incidents – Analytics & Hunting
- Investigate
- Respond

App Center

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

- Integrate
- Test
- Distribute

App Center is great for ...



iOS apps
Swift and Objective-C

Android apps
Java and Kotlin

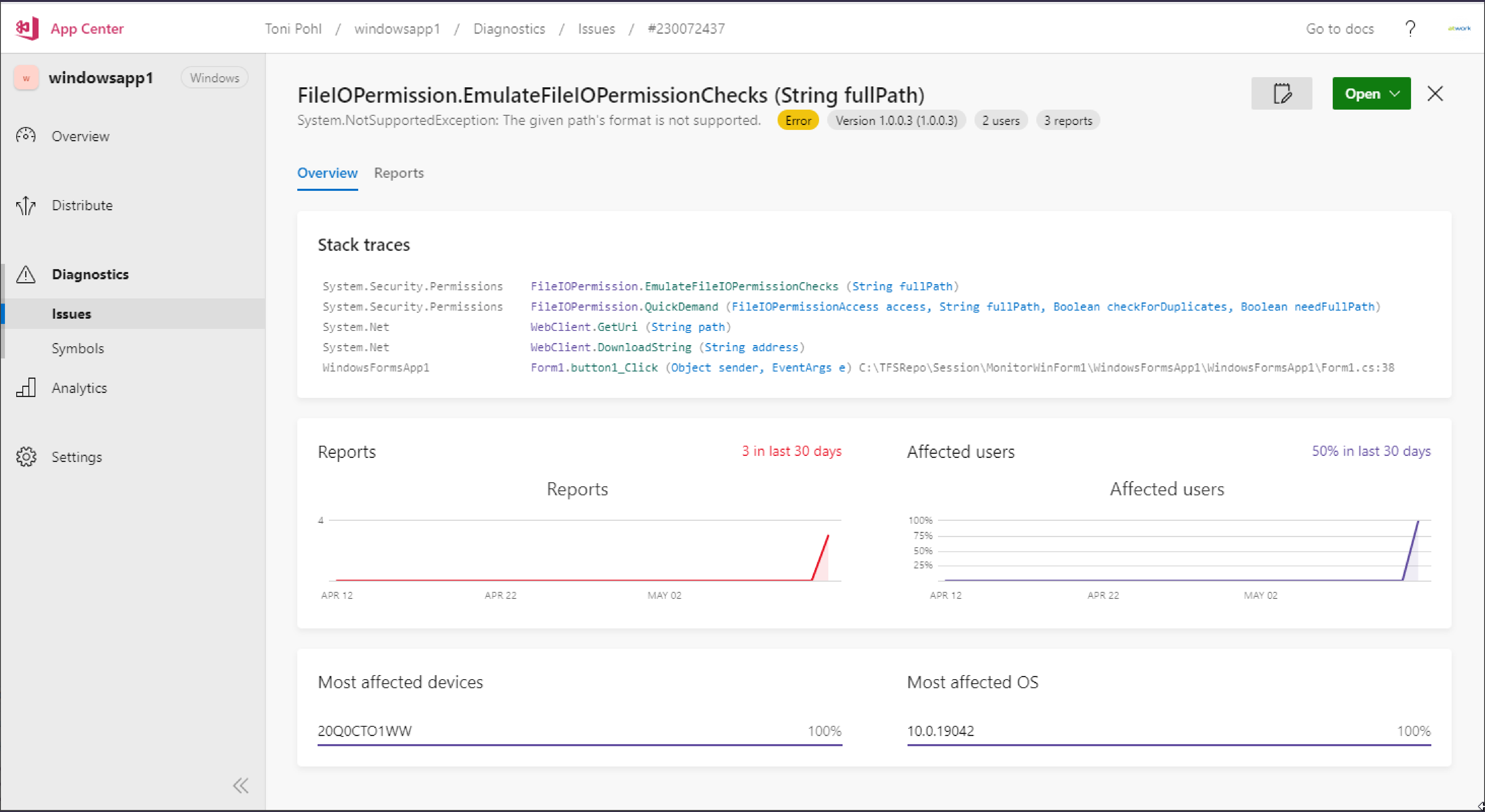
Windows apps
UWP, WPF and WinForms

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)



FileIOPermission.EmulateFileIOPermissionChecks (String fullPath)

System.NotSupportedException: The given path's format is not supported. Error Version 1.0.0.3 (1.0.0.3) 2 users 3 reports

Stack traces

```
System.Security.Permissions    FileIOPermission.EmulateFileIOPermissionChecks (String fullPath)
System.Security.Permissions    FileIOPermission.QuickDemand (FileIOPermissionAccess access, String fullPath, Boolean checkForDuplicates, Boolean needFullPath)
System.Net                     WebClient.GetUri (String path)
System.Net                     WebClient.DownloadString (String address)
WindowsFormsApp1               Form1.button1_Click (Object sender, EventArgs e) C:\TFSRepo\Session\MonitorWinForm1\WindowsFormsApp1\WindowsFormsApp1\Form1.cs:38
```

Reports

3 in last 30 days

Affected users

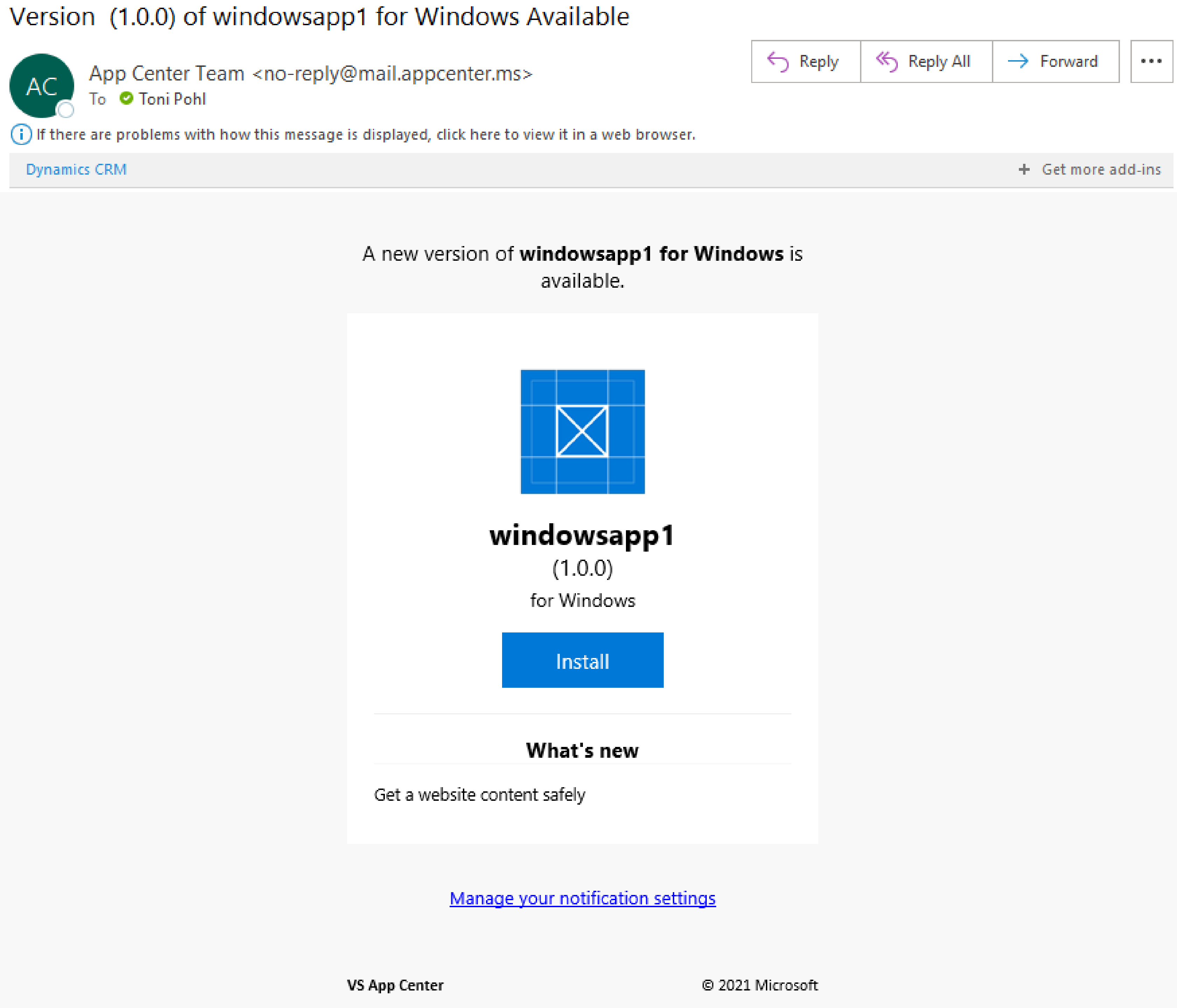
50% in last 30 days

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.

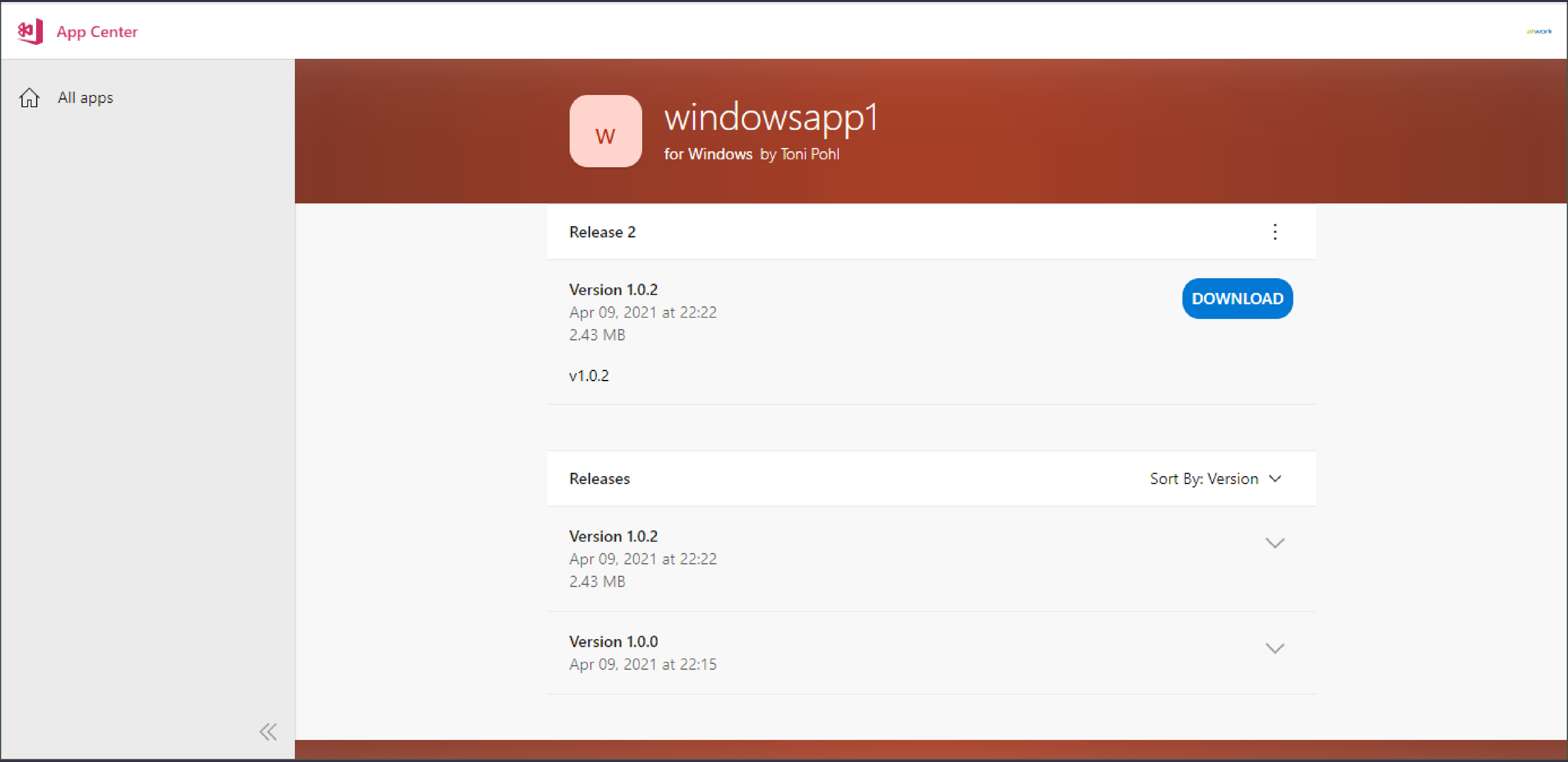
windowsapp1
(1.0.0)
for Windows

What's new

Get a website content safely

Manage your notification settings

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 cost 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

	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									🟢

Let‘s connect

Toni Pohl
MVP Azure & Office Development, CTO atwork
@atwork | toni.pohl@atwork.at | github.com/tonipohl

atwork

Rate my session & Calls to Action

✓

Rate this session

Attend more sessions and join our keynotes at 19.00 CET

Show your love for Teams Nation on Twitter and LinkedIn using #TeamsNation and @TeamsNation

https://teamsnation.rocks/feedback