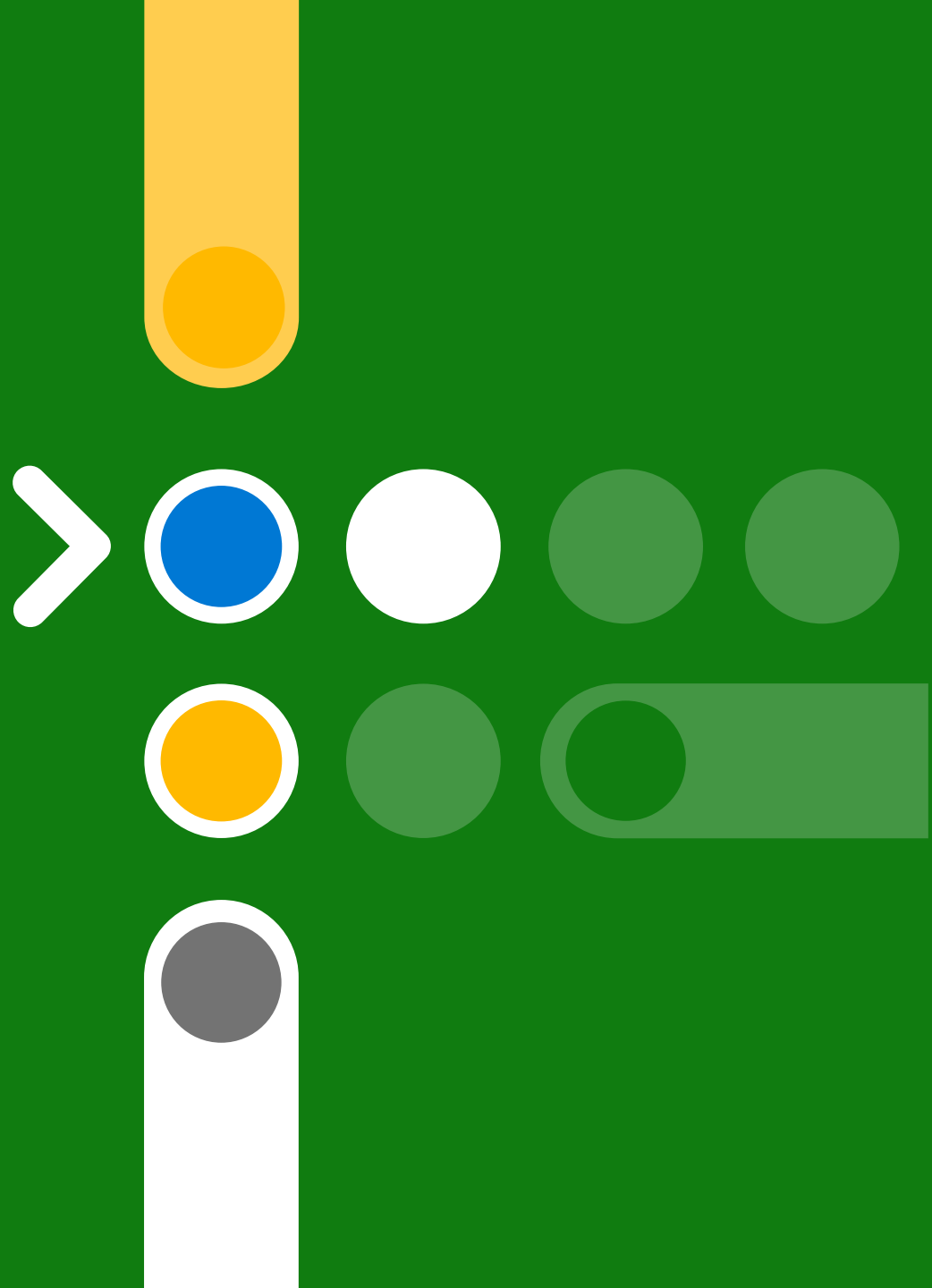
Microsoft Security

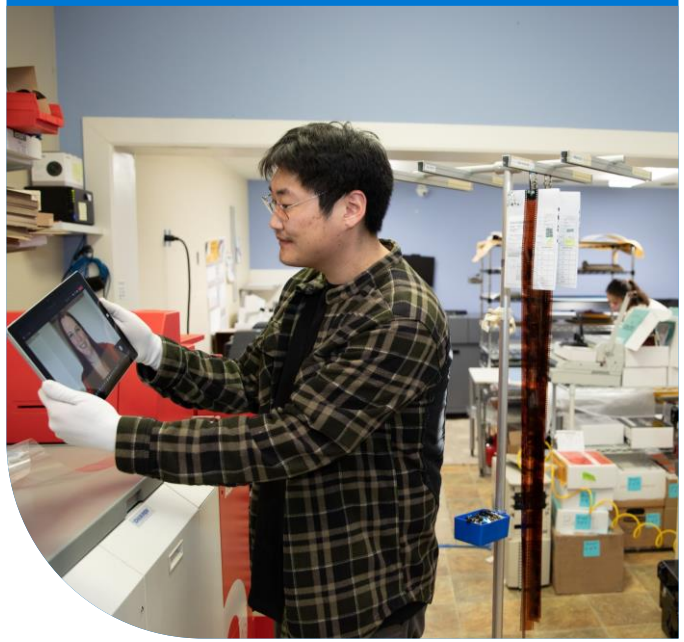
Secure your practice using the Microsoft Zero Trust framework.

Jasper Cottenie (DexMach)
Hans Hofkens (Microsoft)
André Ekas (Microsoft)



Security is top of mind for every business

Employees are working from more locations than ever. Are you confident that your data is safe?



+300%

Ransomware attacks in the past year, with more than 50% targeted at small businesses [1]

1 in 4

Nearly one in four small or medium businesses state that they had a security breach in the last year [2]

70%

Over 70% think cyber threats are becoming more of a business risk [2]

$108K average cost of a SMB data breach [3]

1. Homeland Security Secretary Alejandro Mayorkas, 06 May 2021 ABC report
2. Microsoft commissioned research, April 2022, US SMBs 1-300 employees
3. Kaspersky Global Corporate IT Security Risks Survey, 2019

Are there real-life examples of Partners impacted?

Post incident report

Timeline of an attack

Identity Protection

- MFA for all users
- Risk-based Conditional Access policies

Privileged Identity Management

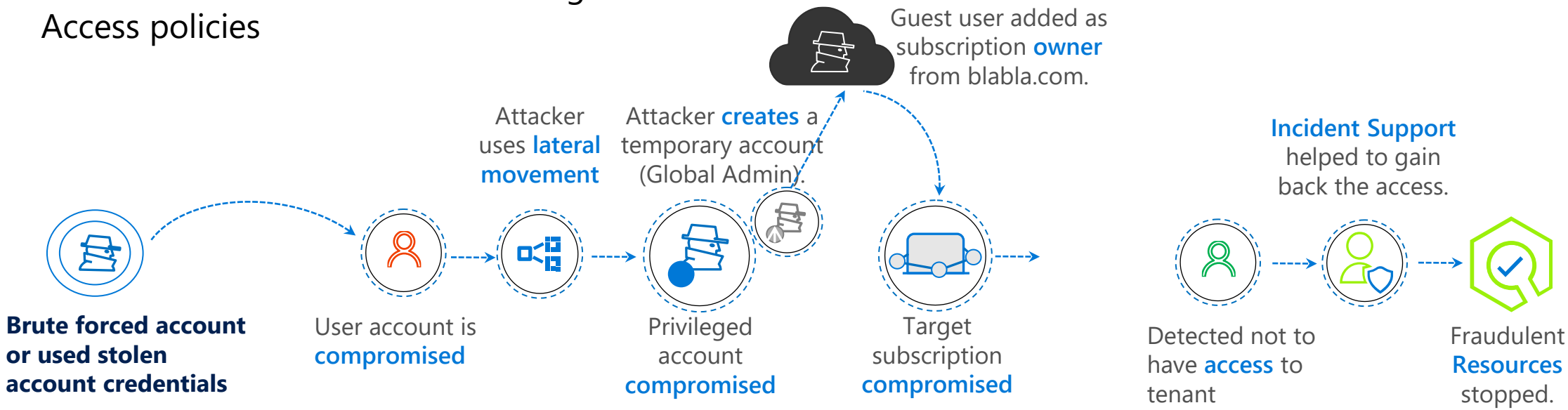
- JIT / JEA
- Auditing

Cost management

- Specific budgets

Monitoring

- Alerts across the attach chain



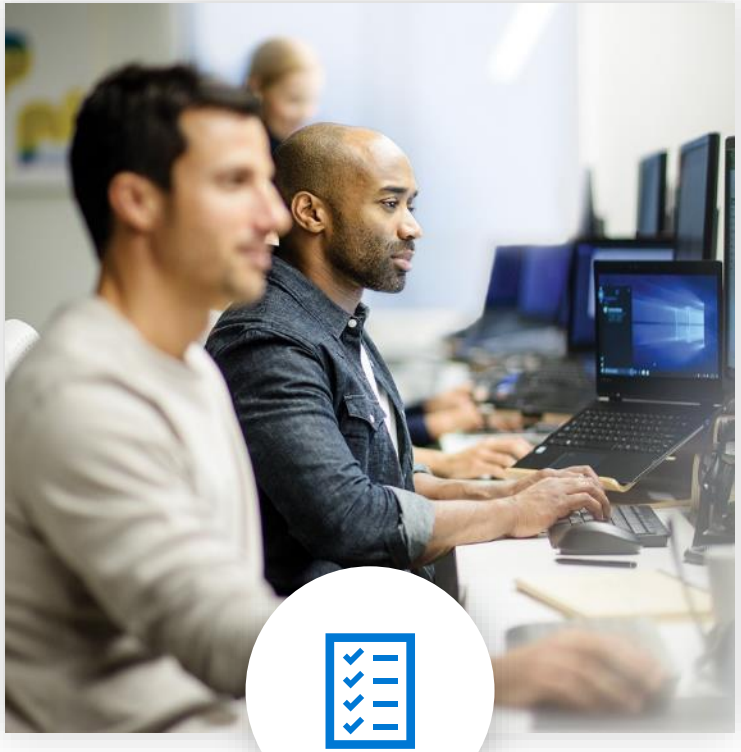
Timeline

3rd of August — 3rd of August — 4th of August — 22nd of August — 22nd of August

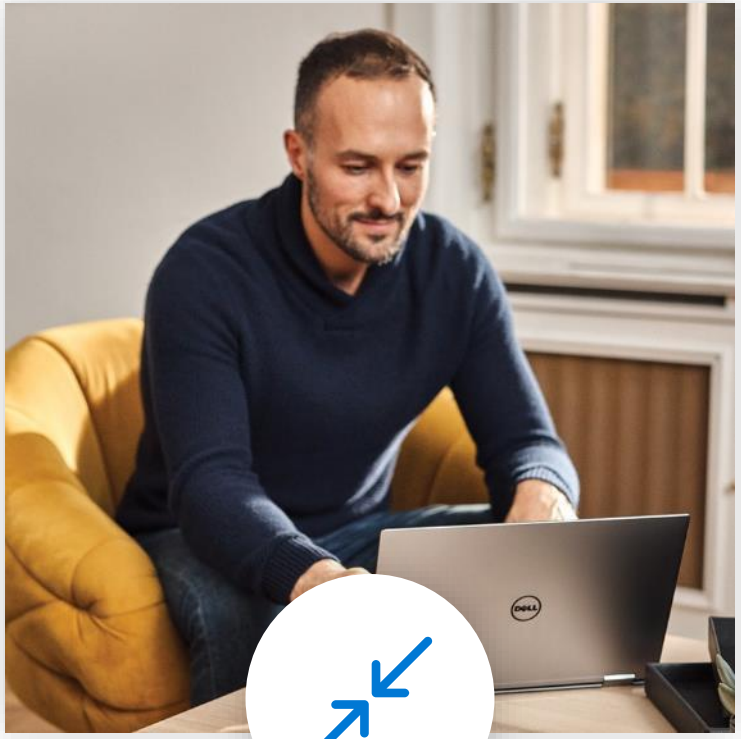
A new reality. How can we adapt?

Zero Trust

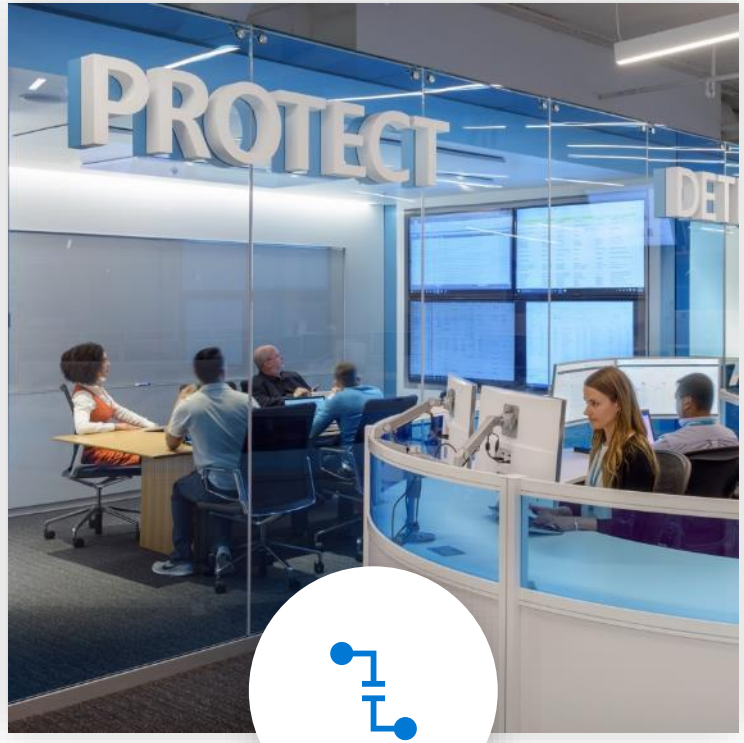
A new reality needs new guiding principles



Verify explicitly



Use least privilege access



Assume breach

What are best practices to secure my Microsoft Partner business?

Five steps

Commit to ongoing security with these best practices

Learn the landscape

Stay up-to-date on new security challenges and the tools available to meet them. Evolve with the security landscape to protect your organization and your customers.

Identify and add security contacts

Establish an individual or group who will be accountable for security-related issues, responding quickly when notified about potential threats.

Secure your identity

Take action to enforce multifactor authentication (MFA) and remove unnecessary delegated administrative privileges.

Secure your endpoints

Invest in platforms that prevent, detect, investigate, and respond to advanced threats.

Ongoing monitoring

Remain engaged with your Zero Trust framework, tapping into resources that help you detect fraud and protect identities.

Journey to Zero Trust (microsoft.com) | Neo – Partner Security

How do you easily assess the security posture of a Customer?

Secure Score

95%

of all breaches could have been avoided if proper cyber hygiene had been in place[1]

Do you have too many global admins?

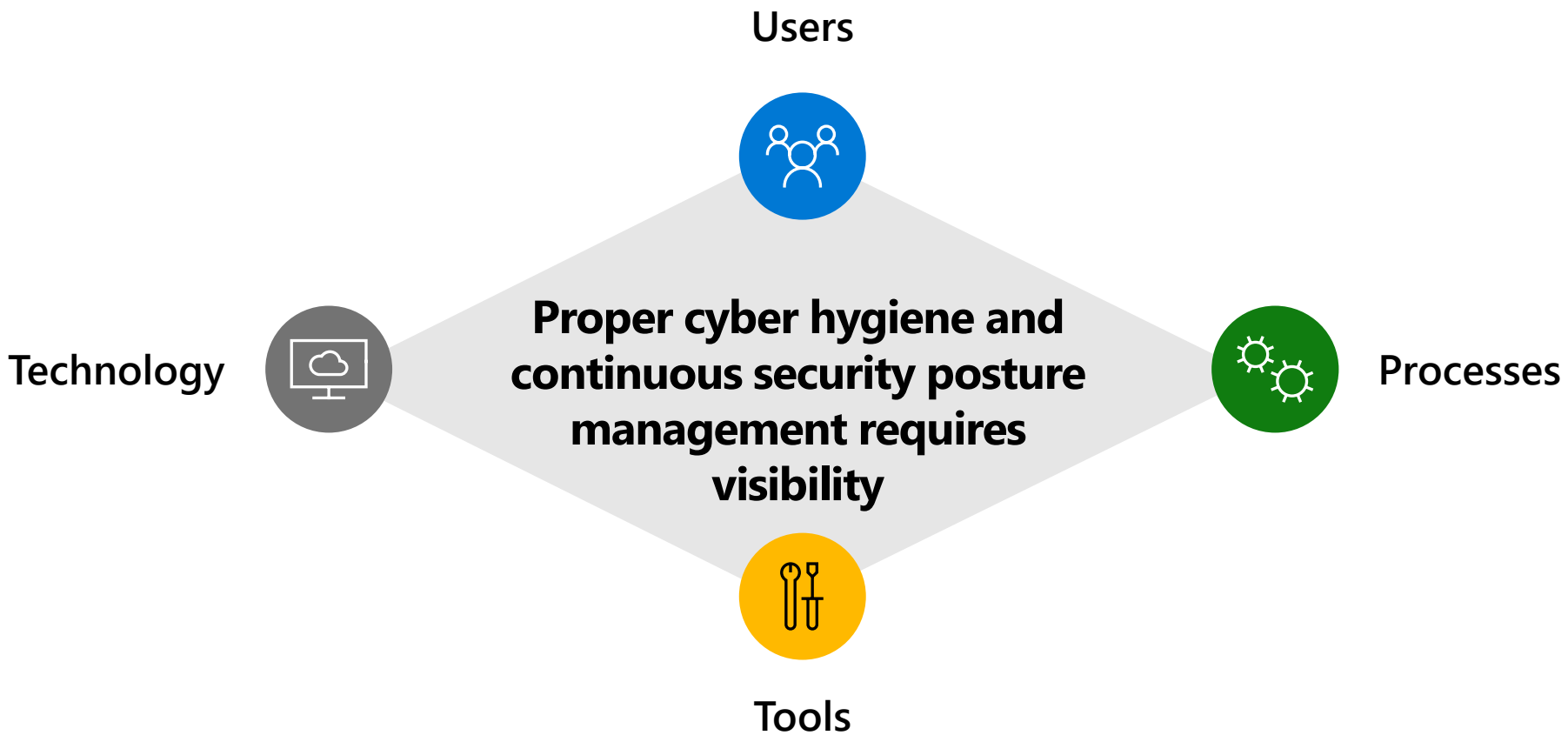
Are your users protecting data using DLP?

Are you managing shadow IT application usage?

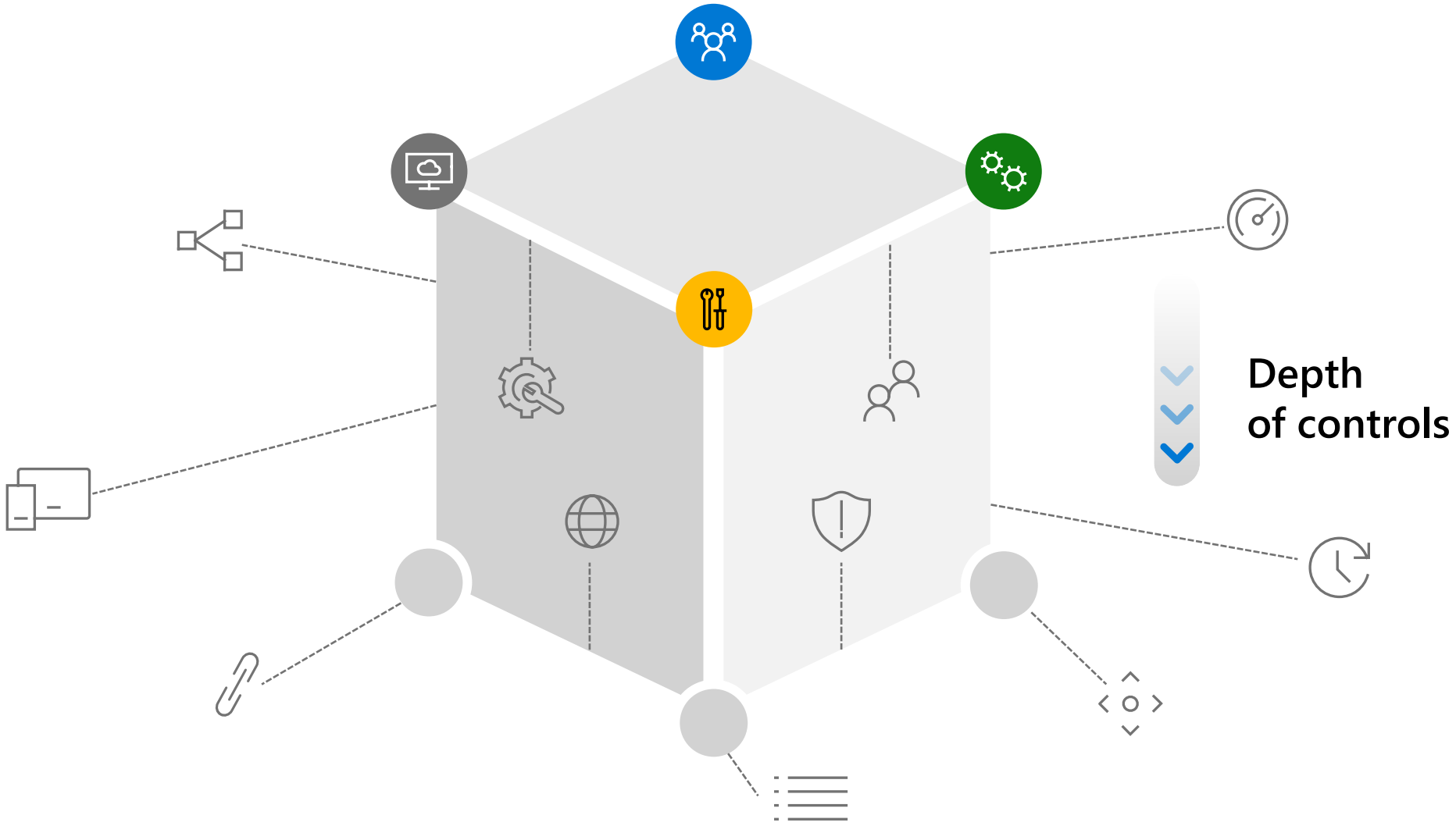
Are you using multifactor authentication?

Do you allow the use of deprecated protocols (e.g.: TLS 1.0)?

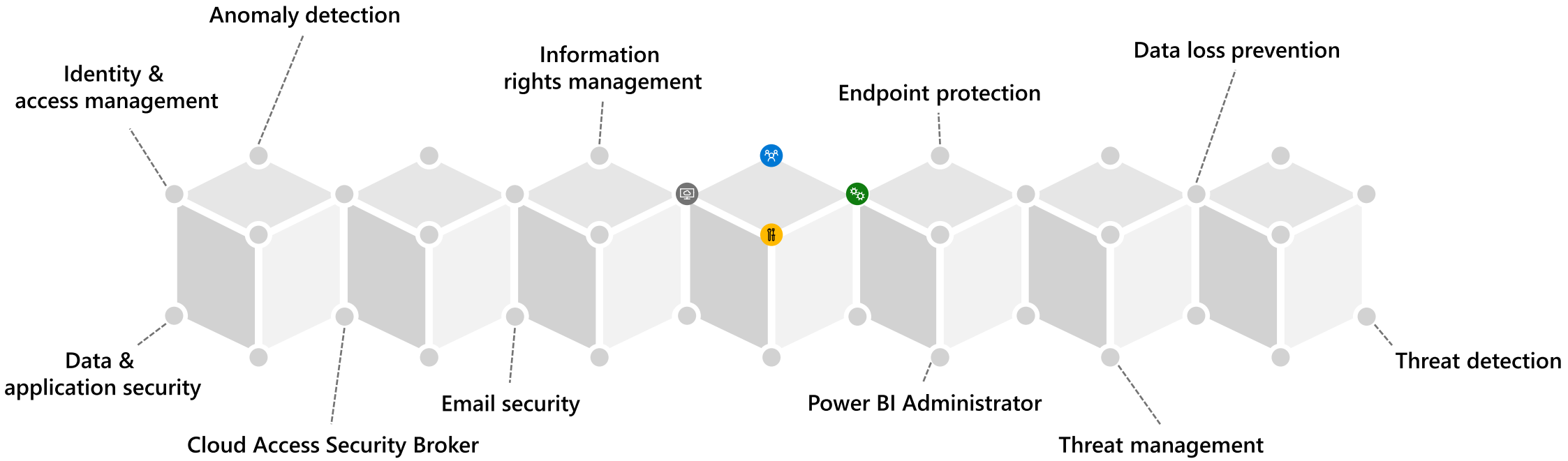
[1] https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf


Users
Technology
Proper cyber hygiene and continuous security posture management requires visibility
Processes
Tools

Accurate security posture visibility, assessment, and transformation across domains is hard



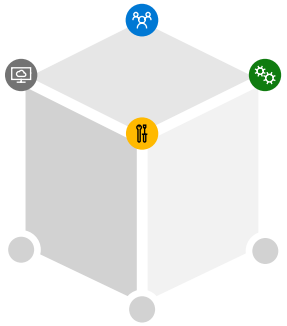
Accurate security posture visibility, assessment, and transformation across domains is hard



Breadth of tools

Accurate security posture visibility, assessment, and transformation across domains is hard

1000s of security controls



~100 security apps and tools

Microsoft Secure Score: Overview

Visibility, assessment, and guidance
to strengthen your security posture

Company-wide visibility

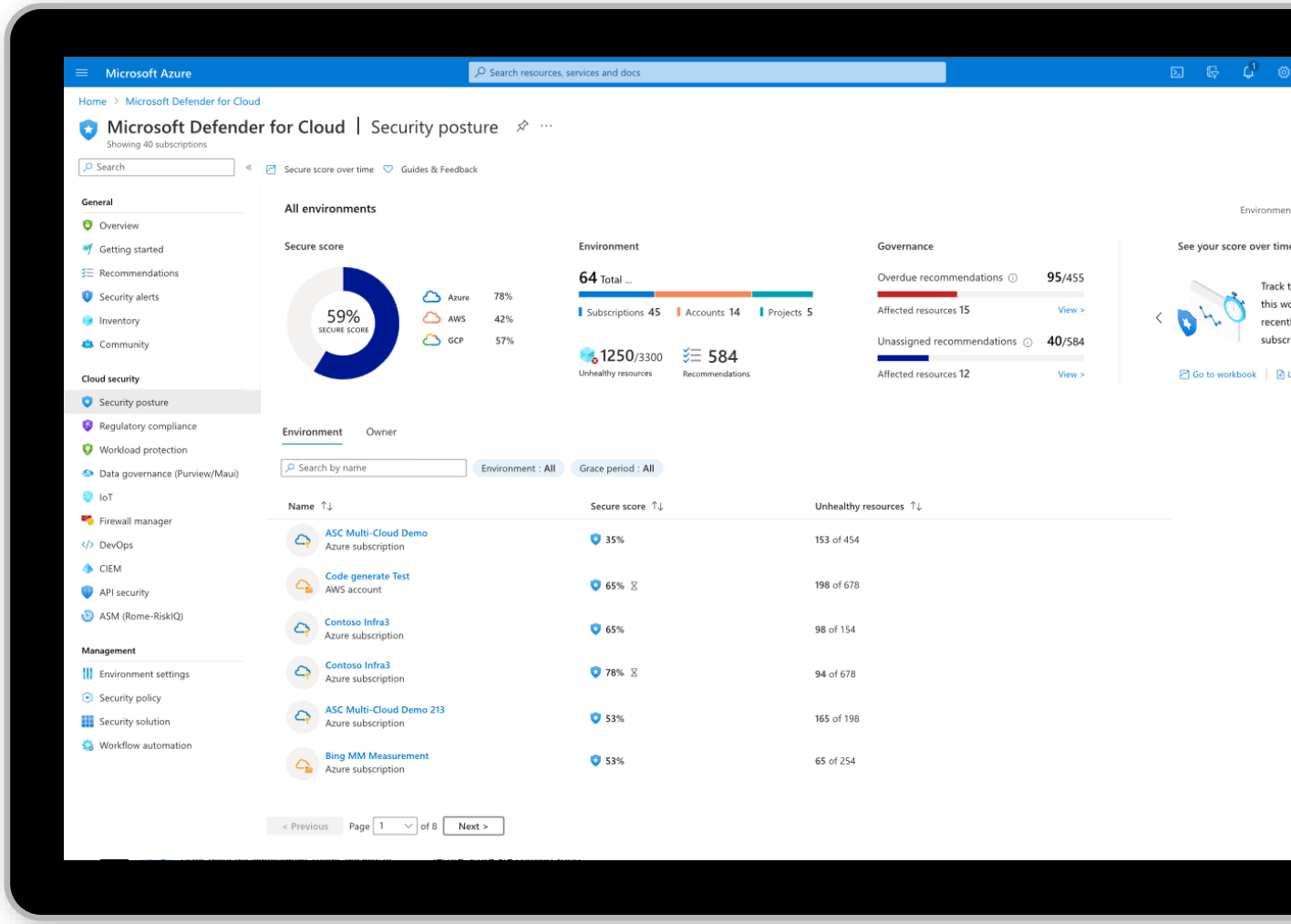
Assess your organization's security posture across identity, devices, information, apps, and infrastructure

Intelligent guidance

Identify where to improve your security posture using threat-prioritized insights and guidance

Comprehensive controls

Integrated workflow capabilities to determine impact and procedures to implement



What is the business opportunity and how to start the Customer conversation?

Cybersecurity Self-assessment

SMBs and Security

80% of SMBs

have antivirus in place, but 93% still have Security concerns

70% of SMBs

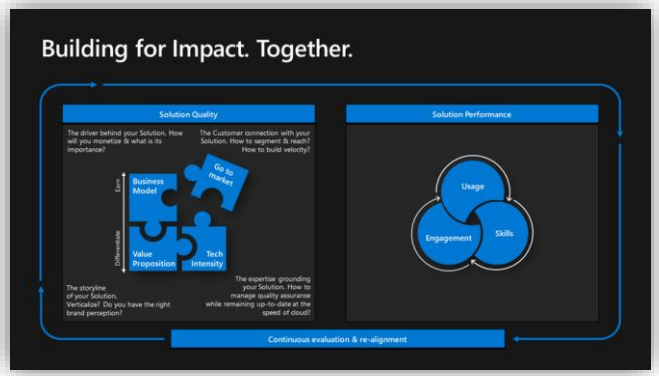
believes security is becoming more of a risk

Nearly 1 in 4

have experienced a cyber attack

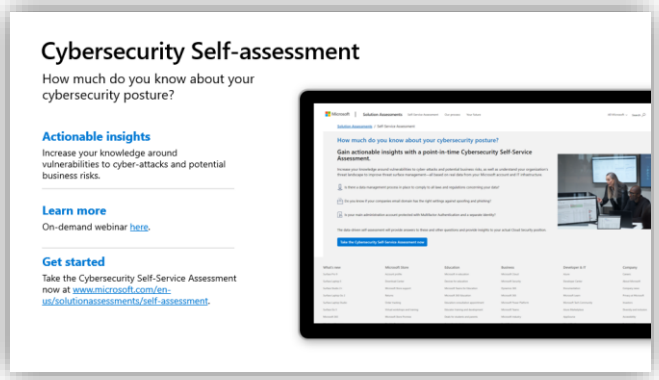
Are you the Security Partner for your Customers?

Think about your Partner business model



- Reach out to your Microsoft or Disti team.

Start the conversation with your Customers



Can you give a real-life example how to operationalize all these tips?

Best practice by DexMach

DEXMACH
A CEGEKA COMPANY

Dexmach csp azure secure score

Microsoft - DexMach

Visualize your landscape

Making your landscape visual is an essential first step towards a more robust security posture. For CSPs, this means gaining a clear view of the security posture of all your linked customers.

5

5 steps to insights

DexMach CSP Secure Score Insights

ACCOUNT PERMISSIONS

APP REGISTRATION

SCAN YOUR CSP CUSTOMERS

STAGE YOUR DATA OUTPUT

CENTRAL INSIGHTS IN POWERBI DASHBOARD

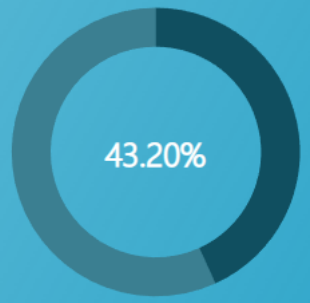
DEXMACH
A CEGEKA COMPANY

UNLOCK THE FULL POTENTIAL OF YOUR CLOUD ENVIRONMENT WITH OUR PREMIUM INSIGHTS!

TENANT: All

SUBSCRIPTION: All

AZURE SECURE SCORE



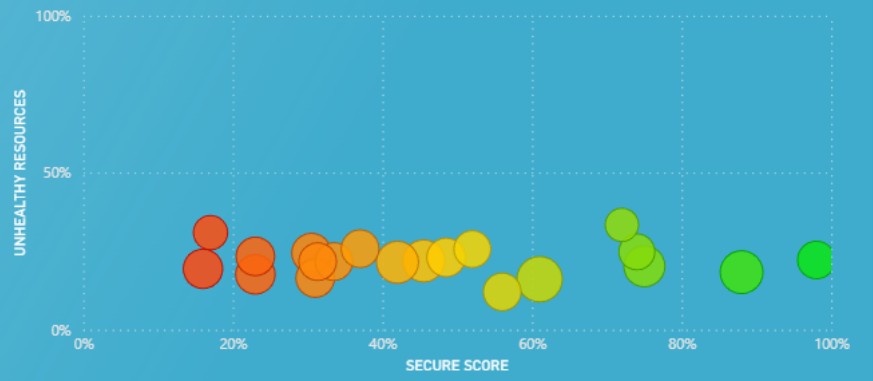
OVERVIEW

TOTAL CUSTOMERS WITH SECURE SCORE : 9

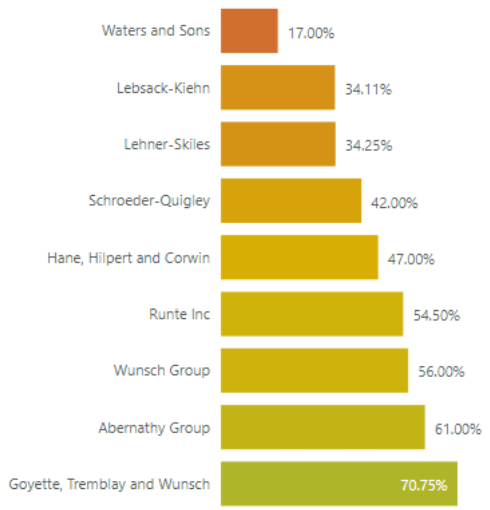
SUBSCRIPTIONS WITH SECURE SCORE : 20

UNHEALTHY vs TOTAL RESOURCES : 3177/12762

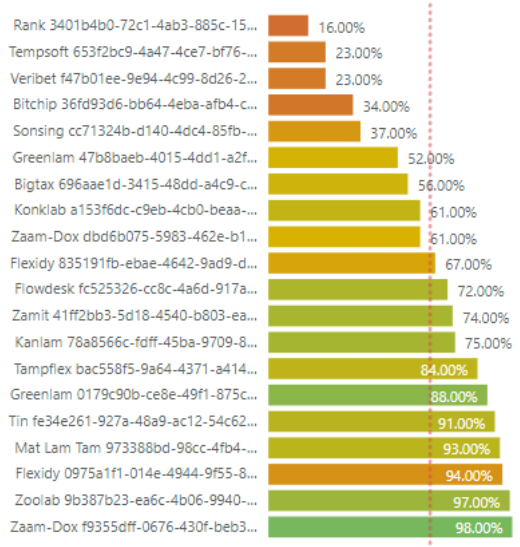
SUBSCRIPTIONS <50%	SUBSCRIPTIONS 50%-65%	SUBSCRIPTIONS >65%
12	5	7



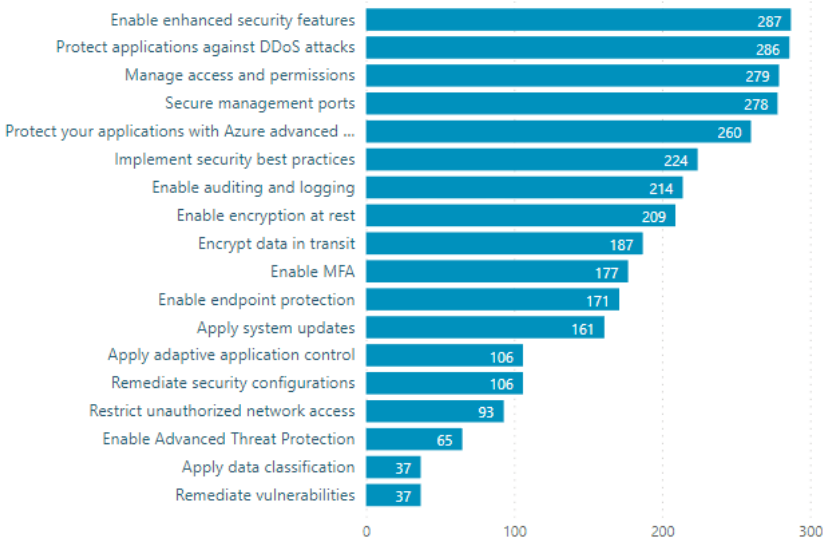
TENANT OVERVIEW



SUBSCRIPTION OVERVIEW



SECURE SCORE CONTROLS - UNHEALTHY RESOURCES



1

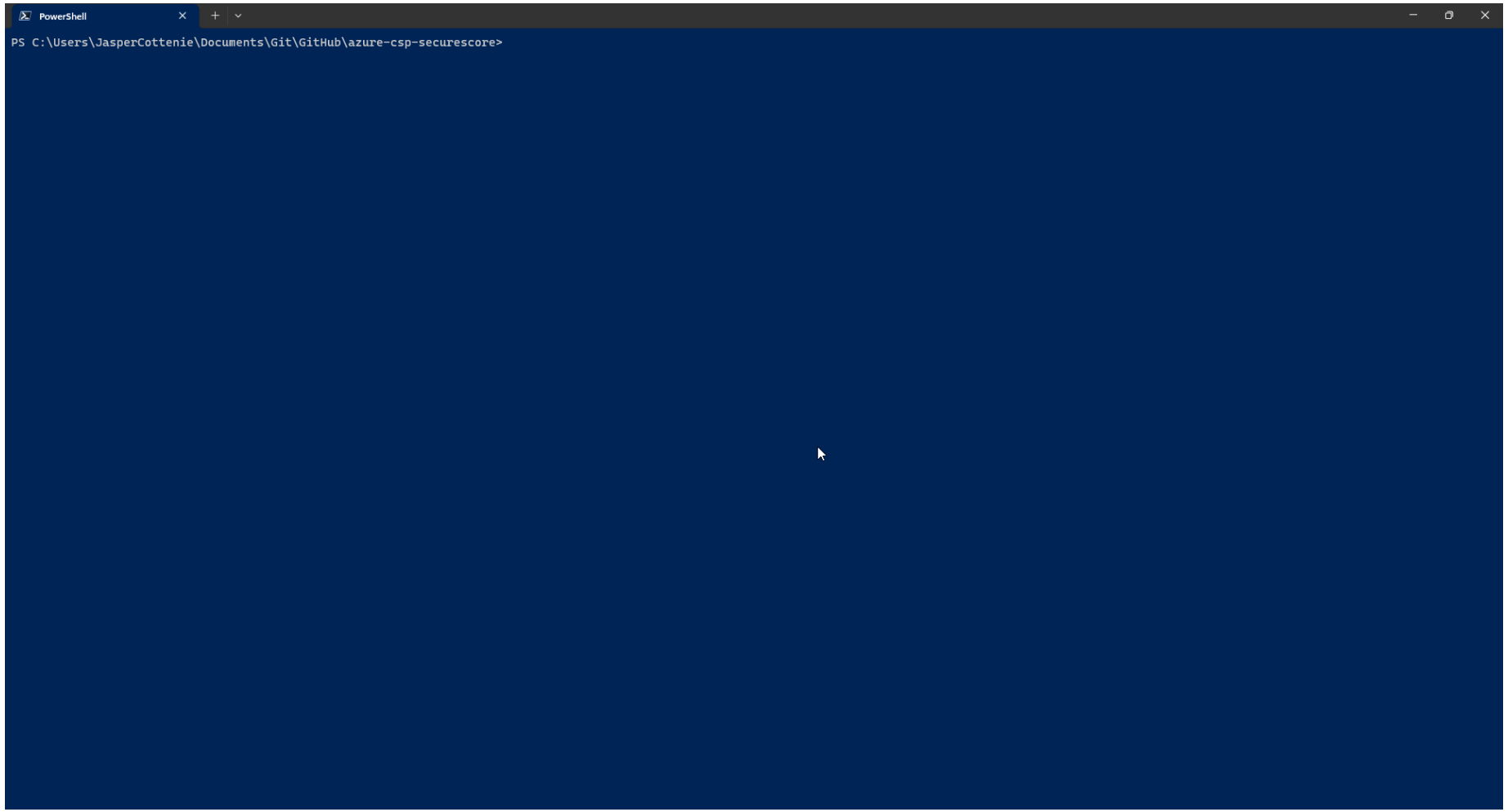
ACCOUNT PERMISSIONS

- Partner center
  - User with Admin Agent role
- Azure AD Service principal*
  - Consent API permissions
- Power BI
  - Pro or Premium license

* Recommended to use automation script, flow 1

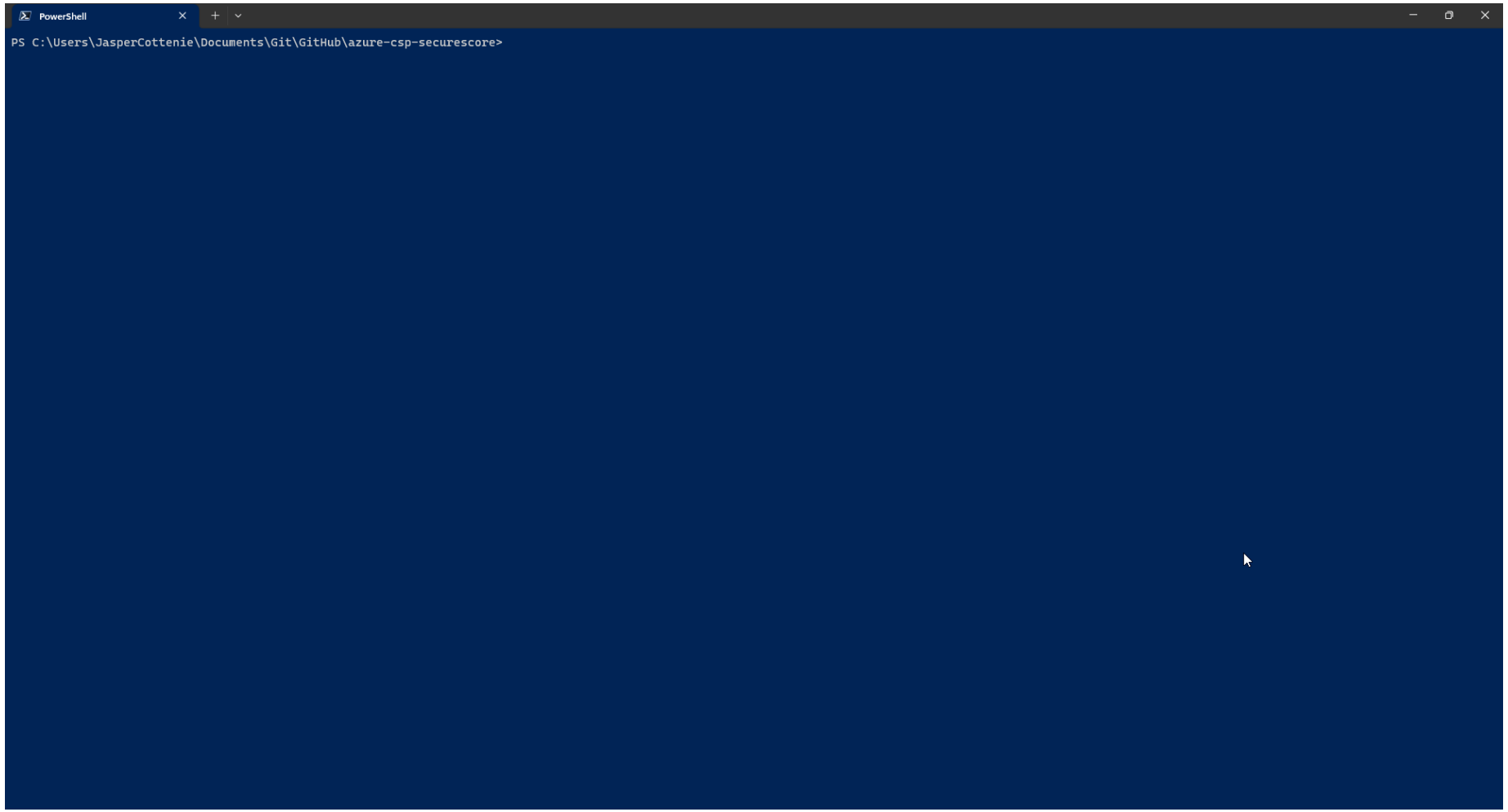
2

APP REGISTRATION



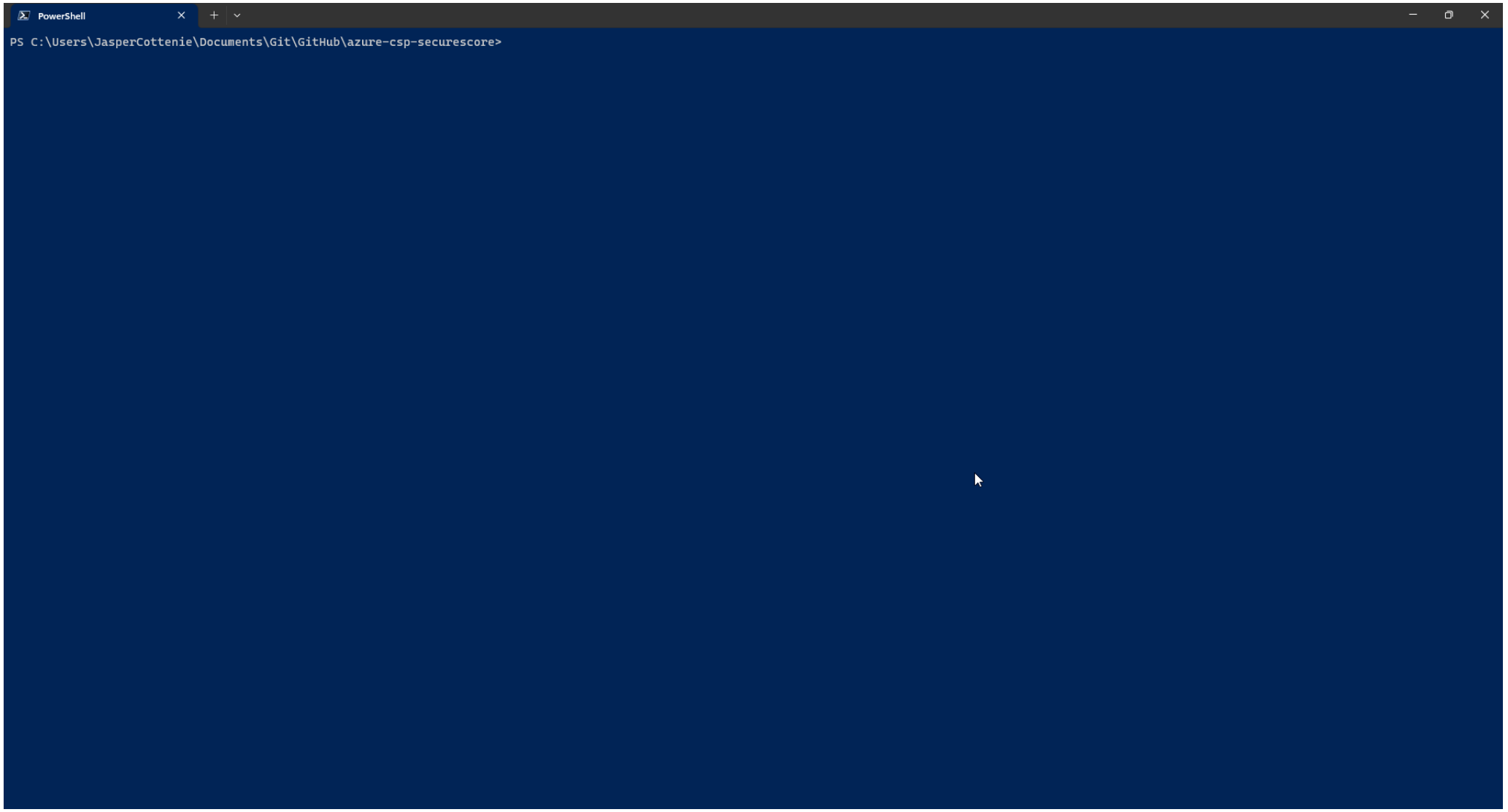
3

SCAN YOUR CSP CUSTOMERS



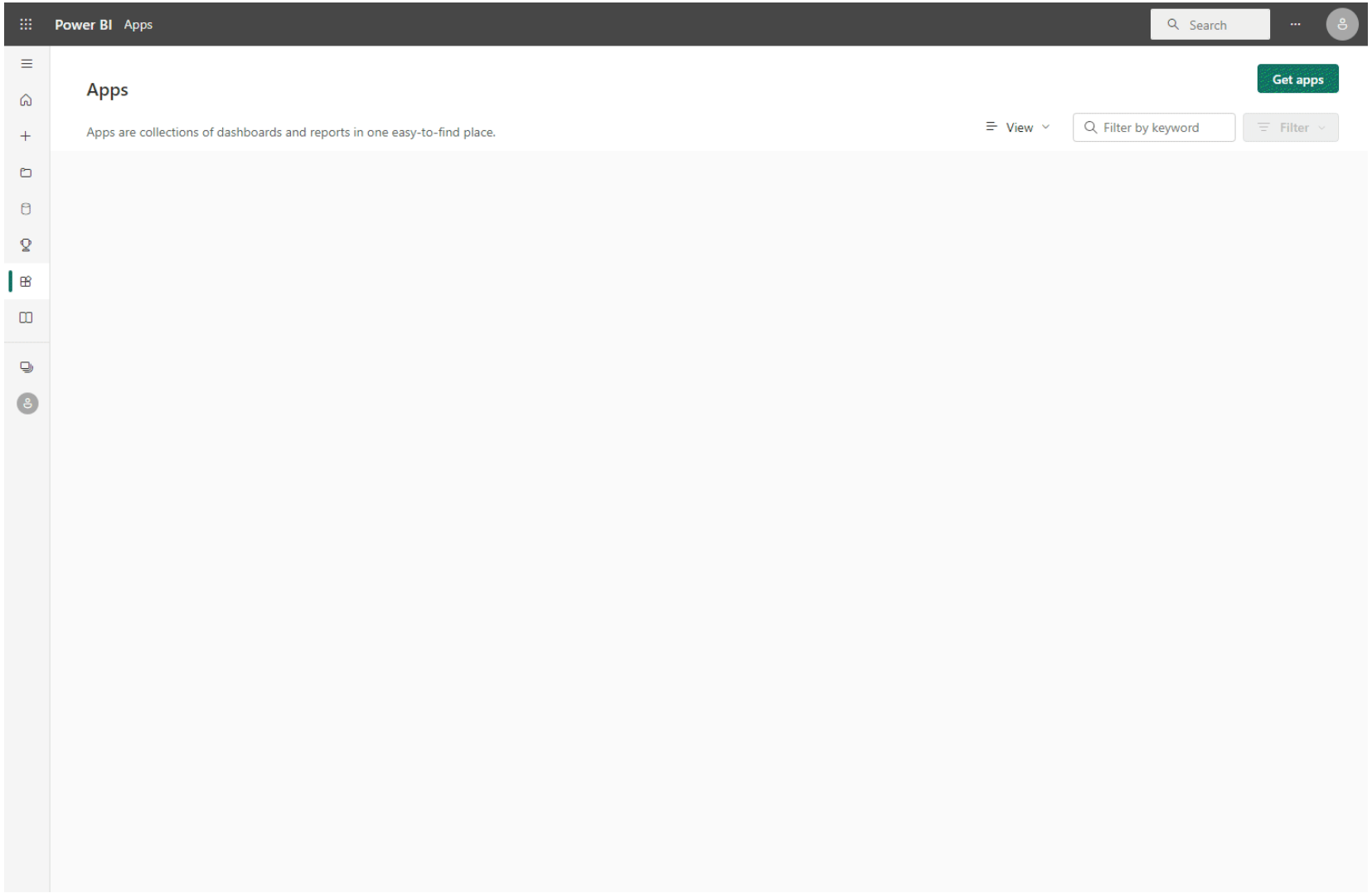
4

STAGE YOUR DATA OUTPUT



5

CENTRAL INSIGHTS IN POWERBI DASHBOARD



Community release

GitHub Link – Data retrieval
Repository

AppSource Link – Visualization
Direct install

DEXMACH
A CEGEKA COMPANY

Insight is not the end goal

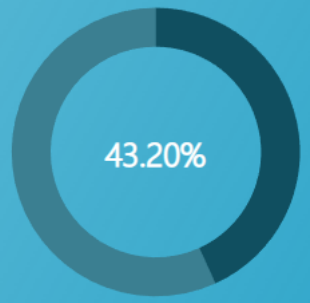
DEXMACH
A CEGEKA COMPANY

UNLOCK THE FULL POTENTIAL OF YOUR CLOUD ENVIRONMENT WITH OUR PREMIUM INSIGHTS!

TENANT: All

SUBSCRIPTION: All

AZURE SECURE SCORE



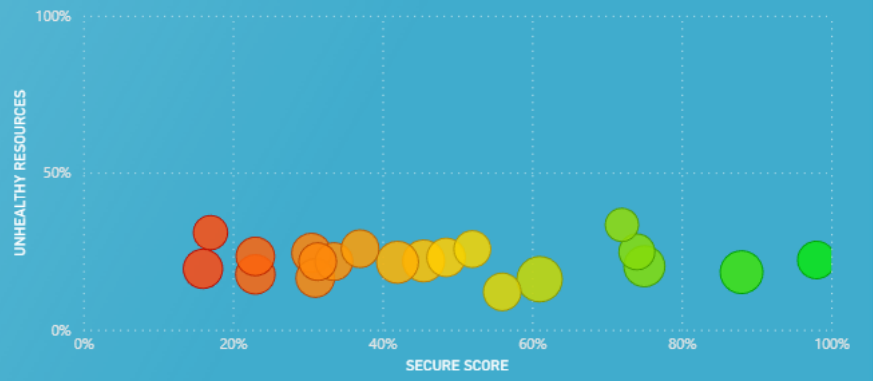
OVERVIEW

TOTAL CUSTOMERS WITH SECURE SCORE : 9

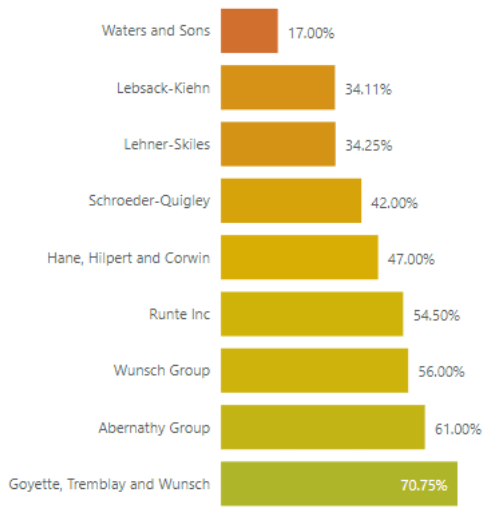
SUBSCRIPTIONS WITH SECURE SCORE : 20

UNHEALTHY vs TOTAL RESOURCES : 3177/12762

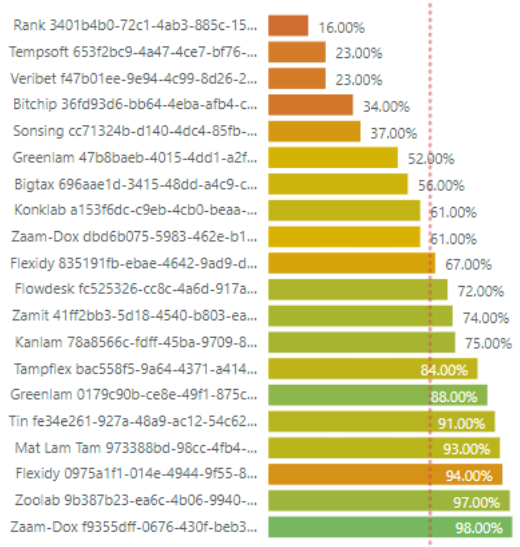
SUBSCRIPTIONS <50%	SUBSCRIPTIONS 50%-65%	SUBSCRIPTIONS >65%
12	5	7



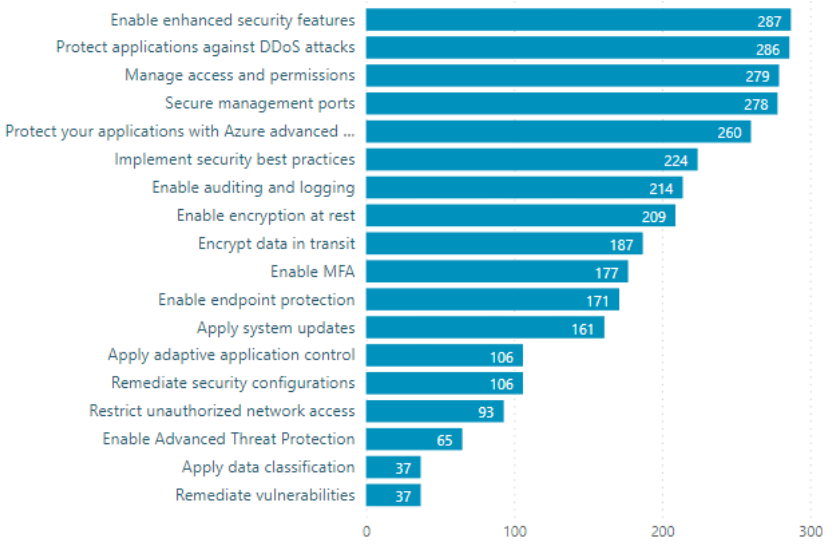
TENANT OVERVIEW



SUBSCRIPTION OVERVIEW



SECURE SCORE CONTROLS - UNHEALTHY RESOURCES

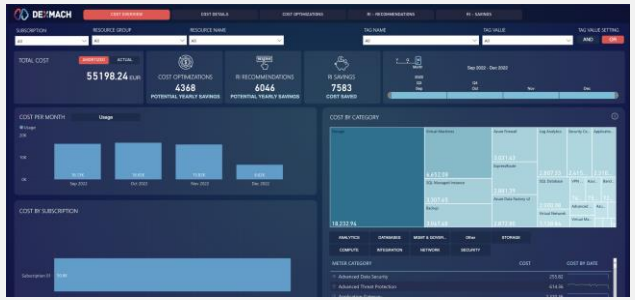


Act on your insights

- Dive deeper with premium insights:
  - How to **mitigate security risks** by fixing controls
  - Steps to implement **security best practices** in your environment
  - **Advanced security insights** including MITRE, CVE, and patching strategies
  - All data remains in your own environment

Premium Insights

Identity Insights



Cloud Cost Insights

Cloud Security & Compliance Insights

Cloud Vulnerability Insights

Kubernetes Smart Insights

- new version in development -

Data Operations Smart Insights

Interested to make this available to your customers through your own marketplace or through Microsoft marketplace?

Book a session now to benefit from our early launch offer.

dexmach.com/security-webinar

#oneteam at your service

+32 (0)2 896 27 60

sales@dexmach.com

www.dexmach.com

https://www.linkedin.com/company/dexmach

Question and Answers

Best practice by DexMach

What’s next? Act today.

Secure your Partner business.

Protect your Customers.

Neo.

Your guide for successful cyber-practices with Microsoft.

aka.ms/Neo-Journey

All resources for Partners to build impactful, repeatable & profitable Security, Compliance, Identity & Endpoint Management solutions.

- **In two slides**
  aka.ms/Neo-Journey/2S
- **Envisioning**
  aka.ms/Neo-Journey/M1
- **Certification & Specialization Plan**
  aka.ms/Neo-Journey/M2
- **Sales & Technical Enablement**
  aka.ms/Neo-Journey/M3
- **Design & Build**
  aka.ms/Neo-Journey/M4
- **Grow your Business**
  aka.ms/Neo-Journey/M5

aka.ms/Neo-Partner

All resources for Partners to broaden & deepen their Partnership with Microsoft across Solution Areas.

- **MS Cloud Partner Program (MCPP)**
  aka.ms/Neo-Partner/MCPP
- **Partner Skilling**
  aka.ms/Neo-Partner/Skilling
- **Partner Solutions**
  aka.ms/Neo-Partner/Solutions
- **Partner Co-sell**
  https://aka.ms/Neo-Partner/Co-sell
- **Partner Attribution**
  aka.ms/Neo-Partner/Attribution
- **Partner Security**
  aka.ms/Neo-Partner/Security
- **Partner Support**
  aka.ms/Neo-Partner/Support

Thank you