Gold Microsoft Partner

Microsoft

Exelegent

Secure and Multi-Cloud Environment: 3-Week Workshop

by Exelegent & Microsoft

Exelegent

http://www.exelegent.com/ · · 36 W Main Street, Suite 300, Freehold, NJ, US 07728

CONTACT > Search for other providers

MPN 2875555

This provider has demonstrated competency in the following areas

Gold	Communications
Gold	DevOps
Gold	Data Analytics
Gold	Data Platform
Gold	Cloud Productivity
Gold	Security
Gold	Cloud Platform
Gold	Windows and Devices
Gold	Collaboration and Content
Gold	Messaging
Silver	Small and Midmarket Cloud Solutions
Silver	Enterprise Mobility Management
Silver	Application Development
Silver	Project and Portfolio Management
Silver	Datacenter

Explore our solutions at Microsoft Azure & AppSource Marketplace

About us

Exelegent is a cyber security and professional services company where efficiency is standard, and our customers are our partners. Headquartered in Freehold, NJ with supporting offices in Newark, NJ and L'viv Ukraine, Exelegent leverages years of experience to bring about a world-class experience for our clients.

Our specialties include:

More

Skills and Capabilities

- Advanced Analytics
- Agriculture, Forestry, & Fishing
- Application Integration
- Artificial Intelligence
- Azure
- Azure Security & Operation Management

36 W Main Street, Suite 300, Freehold, NJ, US 07728

495 N 13th street, Newark, NJ, US 07107

Exelegent

What our clients say:

- "Exelegent helped our company migrate from G-Suite to Microsoft Office 365 with zero downtime and zero data loss. During the process, over 3,500 users continued to collaborate and run critical business functions seamlessly."

  Robert Florescu, CISO, CityMD

- "Switching to Exelegent has been a major contributing factor to the growth of our group. As a company looking to expand, we really value our employees' time and productivity. Exelegent's IT Support has enabled our business to run as efficiently as possible."

  Bruce Lucarelli, CTO, DermOne

- "Exelegent has been with our hospital since we've opened our doors. Their experience in a wide range of projects and solutions, and management of vendors has made a tremendous impact on our efficiency"

  Alexey Gololobov, CFO, Columbus Hospital LTACH

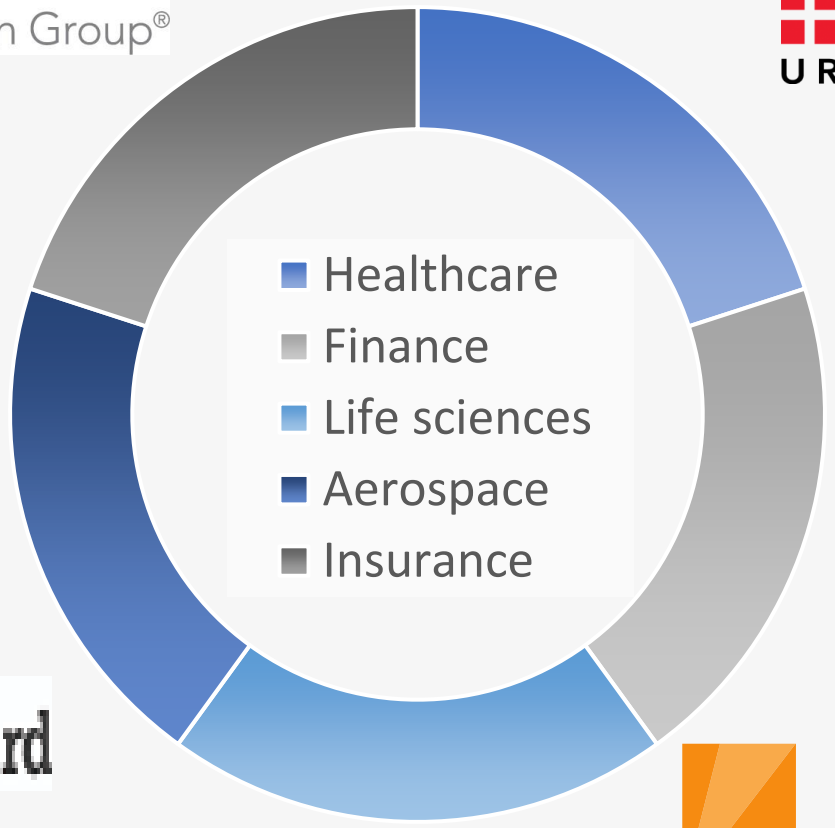
- "Exelegent has become our trusted business partner and completed migration on time, alleviated hosting responsibilities, and gave us capabilities to enable team productivity and data security.«

  Kevin Hannigan, President, ACC Inc.

Exelegent

Clients

Industries we serve



PRISM Vision Group®

CITYMD URGENT CARE

SILVER LAKE HOSPITAL

OCEANFIRST BANK

fastpacehealth

ETS

CollegeBoard

CentraState Healthcare System®
ATLANTIC HEALTH SYSTEM PARTNER

Meadowlands Hospital

Summit Health

Microsoft Defender For Cloud

Cloud native application protection across clouds and on-prem environments

Harden and manage your Security Posture

Secure configuration of resources

Management of compliance requirements

Detect threats and protect your workloads

Full-stack threat protection

Vulnerability assessment & management

Respond & Automate

Assess and resolve security alerts and incidents

Automate response

Automate with the tools of your choice

Microsoft Azure

Amazon Web Services

Google Cloud Platform

On-prem

Exelegent

The security dashboard

Centralized posture view

Your security posture across Azure, AWS, and GCP in one place

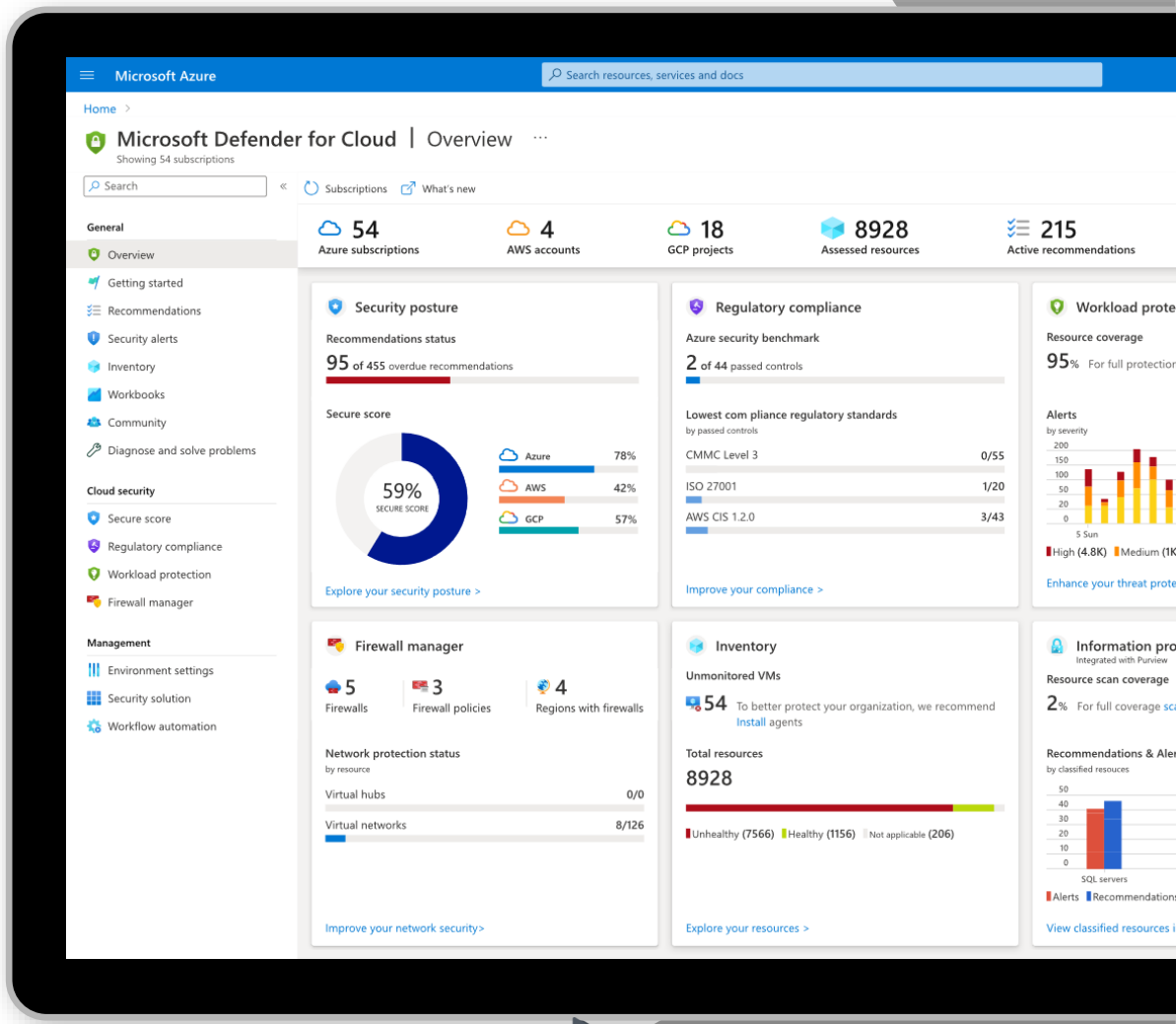
Focused views

Easily access deep dive views for security posture, resource inventory, workload protection, and more

Top insights front and center

Understand which recommendations to prioritize

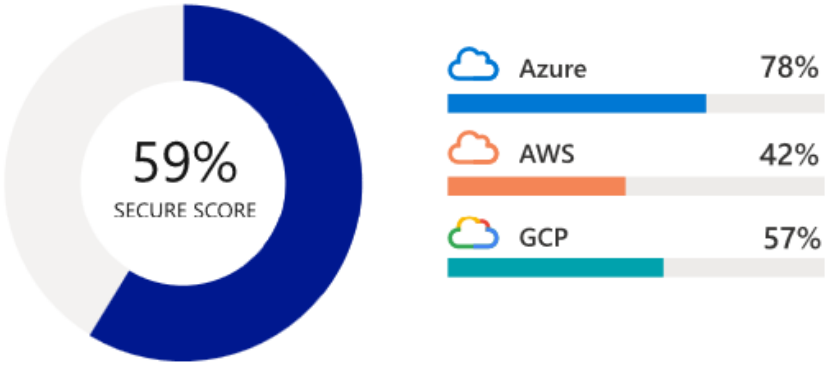
See your most attacked resources and take action

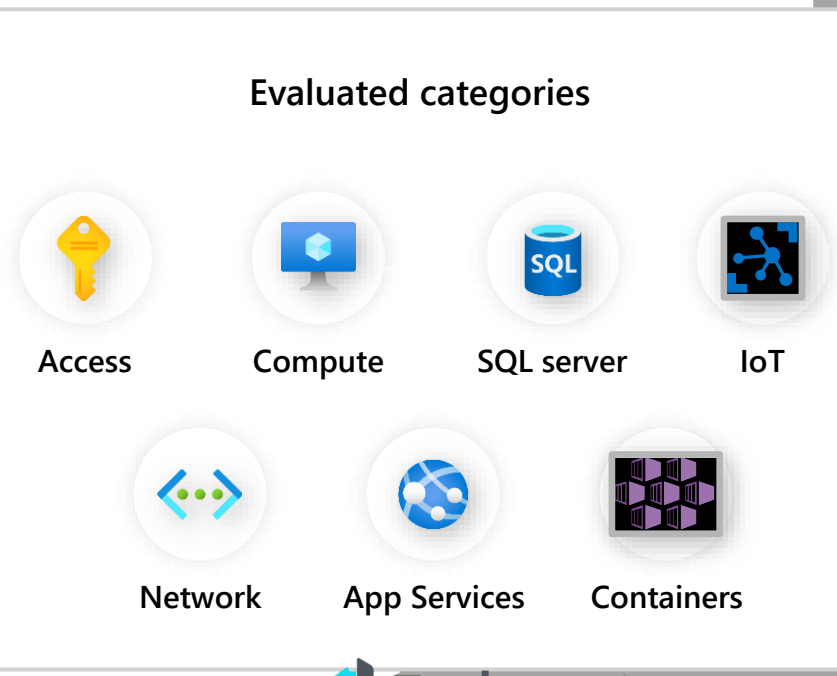


Exelegent

Secure Score

- Assess and implement best practices for security and compliance
- Cover all critical cloud resources across network, access, compute, databases, your service layer and more
- 450+out-of-the-box recommendations
- Create custom recommendations to meet organizational requirements
- Use “Quick fix” to remediate with a single click or scale enforcement mechanisms to enforce policies to avoid configuration drifts



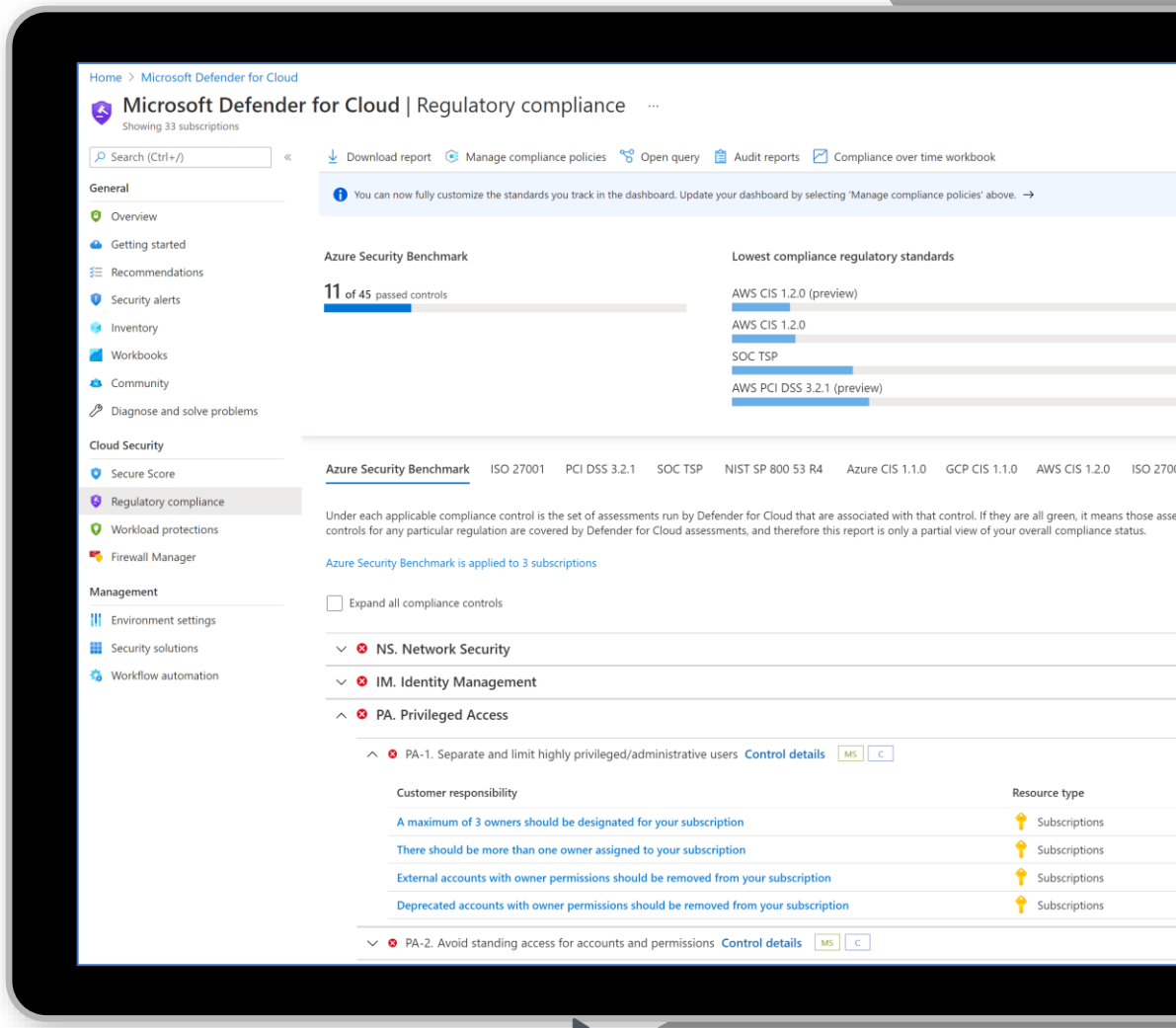


Compliance assessment and management

- Assess and manage your compliance status with a continuous assessment of your cloud resources
- Use industry standards, regulatory compliance frameworks, and vendor provided benchmarks to implement security and compliance best practices
- Create custom recommendations to meet unique organizational needs

Support for:

- CIS
- PCI
- NIST
- SOC
- ISO
- HIPAA
- Local/National compliance standards
- Azure Security Benchmark
- AWS Foundational Security best practices



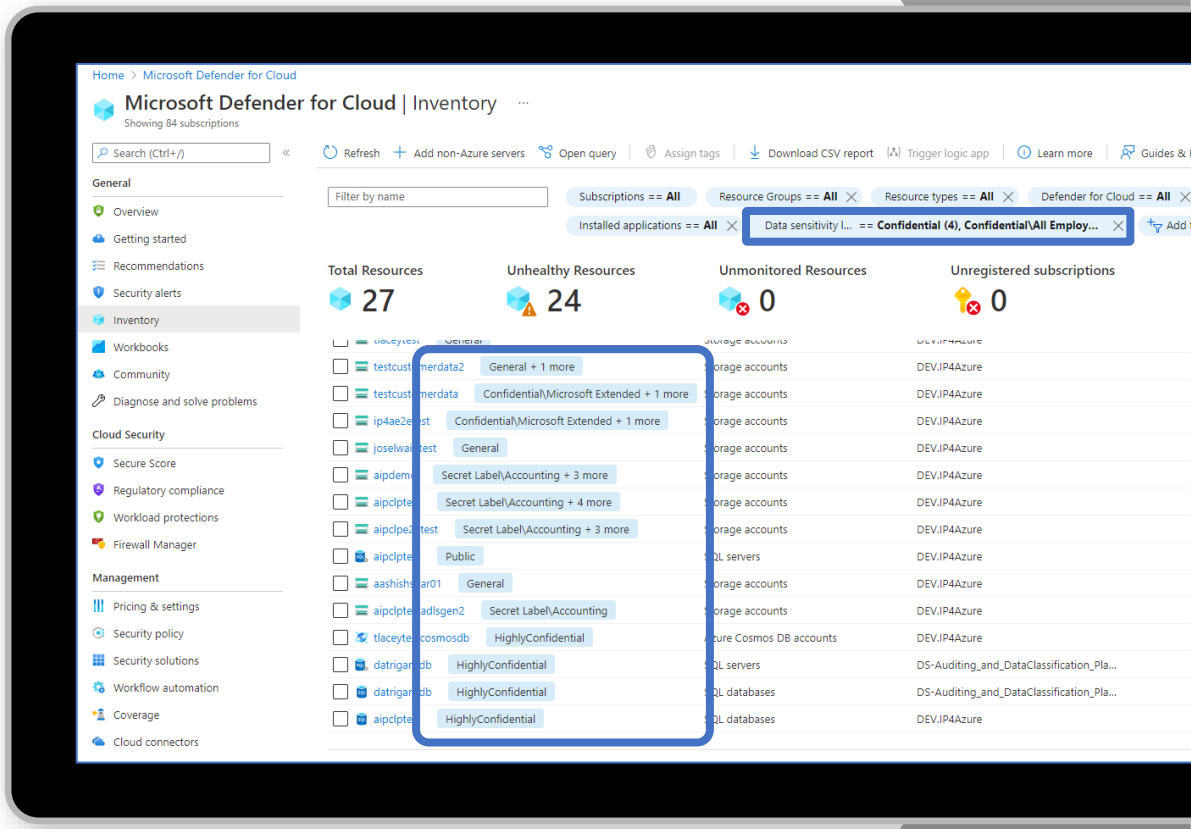
Exelegent

Identify sensitive data in cloud resources

Integrated with Microsoft Purview

Extend visibility from cloud infrastructure resources into the data layer

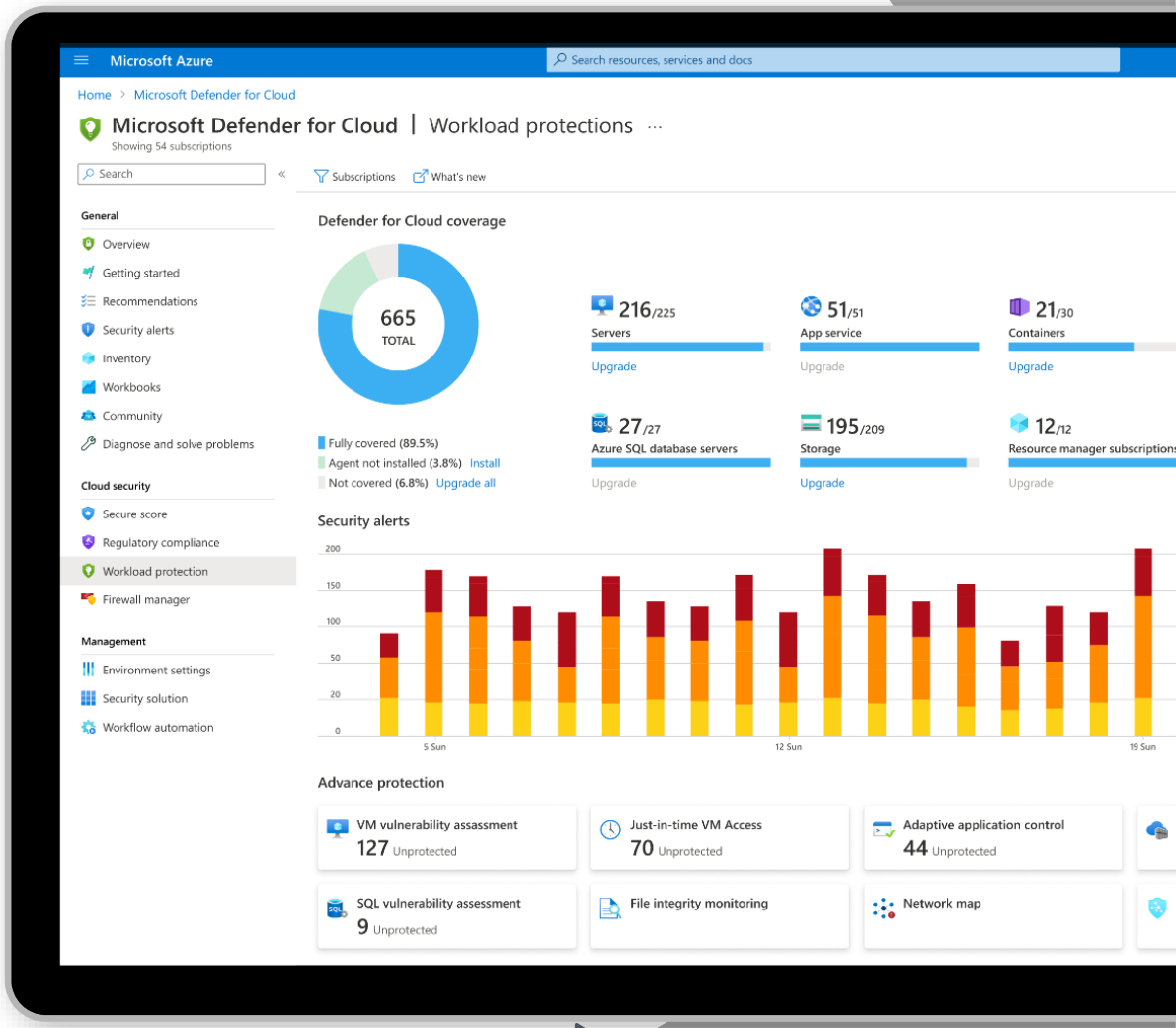
- Leverage an entirely new way to prioritize security policies and the investigation of alerts
- Filter recommendations and resources by data sensitivity
- Easily view the number of assets that contain sensitive information across your environment



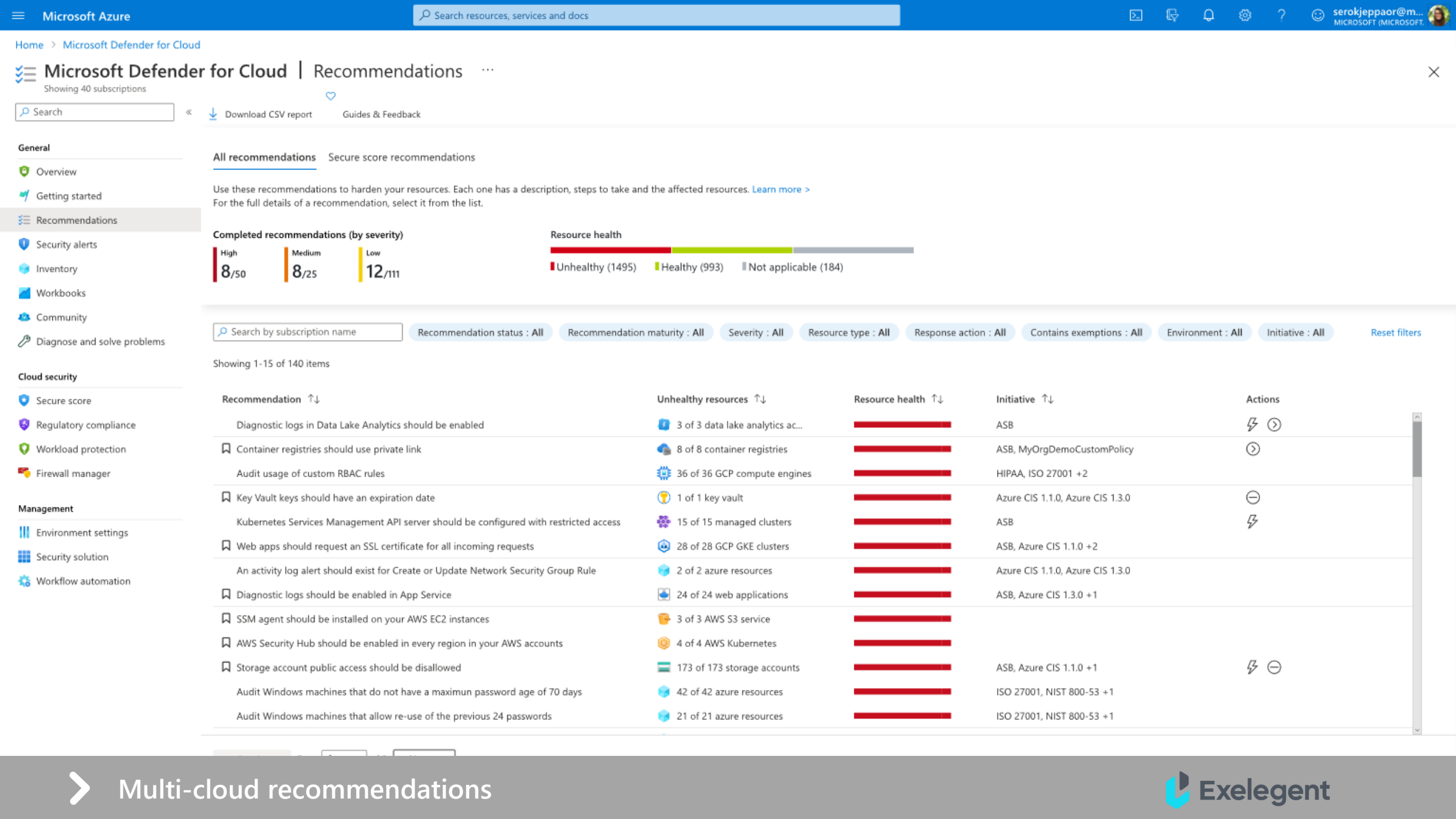
Exelegent

Protect your workloads in the cloud and on-premises

- Use detections that are built for the unique attack vectors of each resource type, built on the powerful insights of Microsoft Threat Intelligence
- Reduce your attack surface by continuously scanning workloads to identify and manage vulnerabilities
- Automatically protect new workloads as soon as they are deployed
- Integrate with your SIEM for easy management of incidents



Exelegent



Multi-cloud recommendations

Exelegent

Approach

Analyze

Business and IT requirements

Existing security management solutions for hybrid cloud workloads

Existing security solutions for Azure resources

Security Operations automation requirements

Define scope & deploy

Define the scope of the Microsoft Defender for Cloud deployment

Deploy and configure Microsoft Defender for Cloud

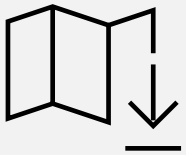
Onboard servers to Microsoft Defender for Cloud, including Microsoft Defender for Endpoint

Onboard Azure SQL and Azure storage account services to Microsoft Defender for Cloud

Discover threats

Discover threats to your hybrid workloads

Learn how to use Microsoft Defender for Cloud to investigate and respond to incidents



Explore Azure Network Security

Learn about Azure Network Security capabilities **[Optional]**

Experience Azure Network Security in a demonstration environment **[Optional]**

Explore vulnerabilities

Use Microsoft Defender for Cloud to explore hybrid and multi-cloud vulnerabilities

Learn how to reduce the attack surface for hybrid and multi-cloud workloads

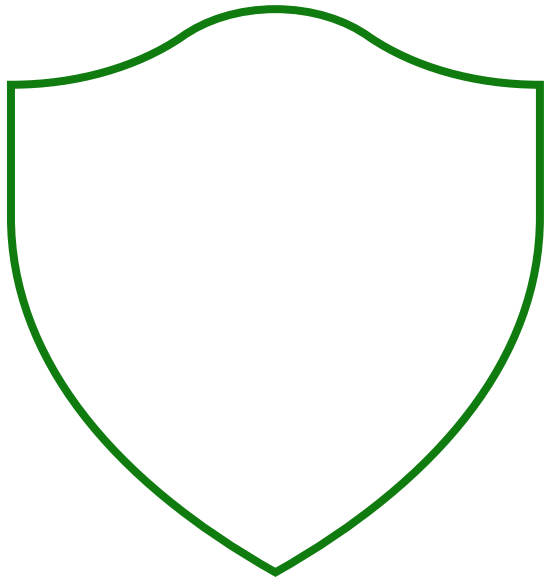
Recommend

Map threats and vulnerabilities found to recommended mitigation strategies

Provide next steps for the deployment of Microsoft Defender for Cloud

Provide next steps for the deployment of Azure Network Security services

Microsoft Defender



What is Microsoft Defender for Cloud?

Microsoft Defender for Cloud provides cloud security posture management (CSPM and cloud workload protection (CWP).

Microsoft Defender for Cloud is an enterprise security platform designed to help organizations prevent, detect, investigate, and respond to advanced threats to hybrid and multi-cloud workloads and discover vulnerabilities in them.

Insights into threats

Discover and analyze threats to hybrid and multi-cloud workloads.

In scope for this engagement.

Discover vulnerabilities

Discover vulnerabilities and learn how to reduce the attack surface for hybrid and multi-cloud workloads.

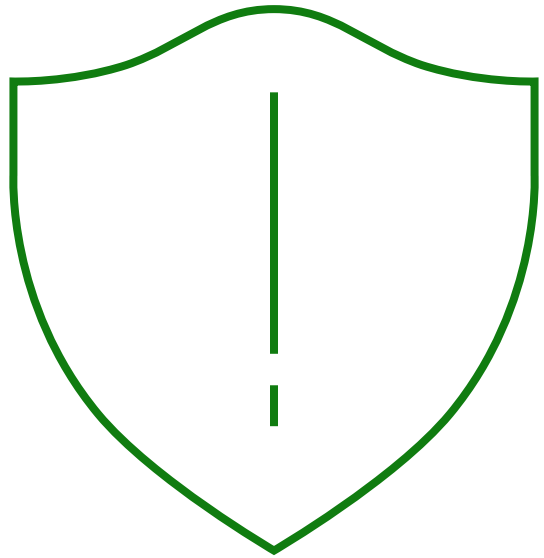
In scope for this engagement.

Requirements

Microsoft Defender for Cloud has a free tier which does not include the enhanced security features available as part of the Microsoft Defender for Cloud plans.

The Microsoft Defender for Cloud plans enables enhanced security features and is available to any customer with an Azure subscription and can be individually set to on or off.

Azure Network Security



What are Azure Network Security services?

Azure Network Security services provide capabilities to build secure virtual networking infrastructure and protect Azure resources at various networking levels (L3-L7).

This engagement is focused on four services:

Azure Firewall is a managed cloud-based network firewall service that protects your Azure resources.

Azure Firewall Manager is a security management service that provides central security policy and route management for cloud-based security perimeters.

Azure Web Application Firewall is a service that protects web applications from bot attacks and common web vulnerabilities such as SQL injection and cross-site scripting.

Azure DDoS Protection is a service that protects Azure resources from denial of service (DoS) attacks with always-on monitoring and automatic network attack mitigation.

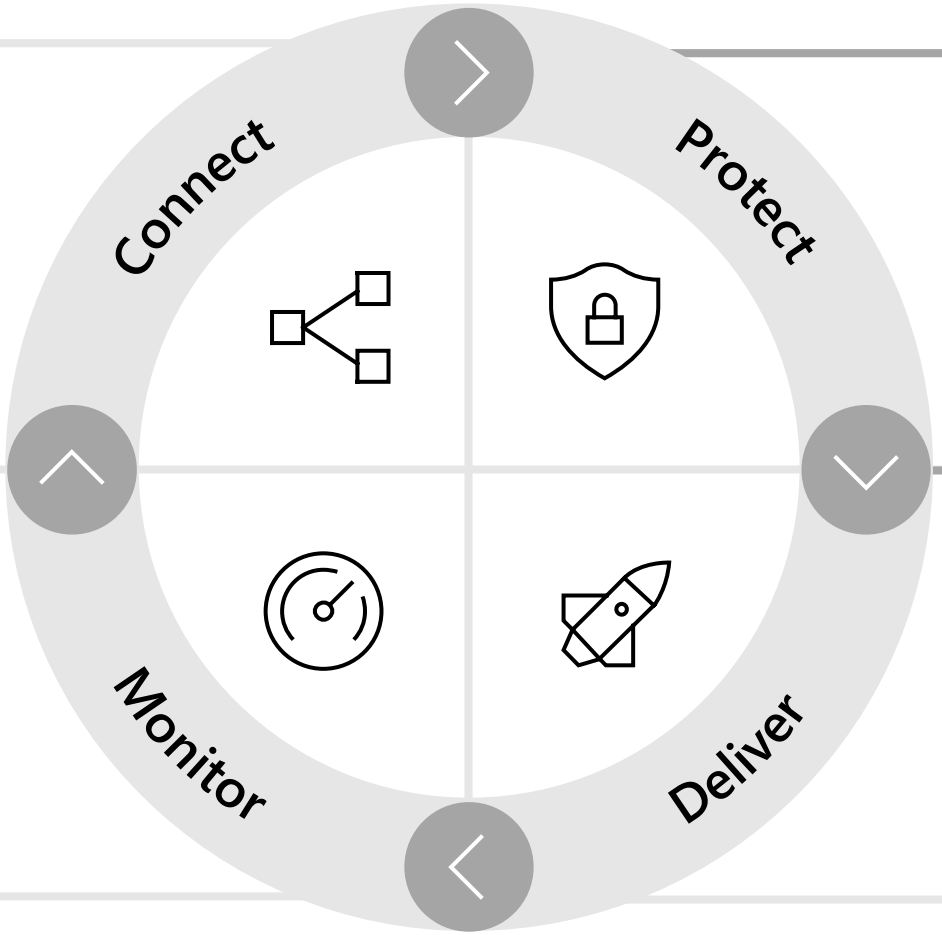
More information about these and other Azure Network Security services: Azure Networking → Secure Network Infrastructure

Requirements

Azure Network Security services are priced and available to any customer with an Azure subscription.

Exelegent

Azure Network Security



Virtual Network
Virtual WAN
ExpressRoute
VPN
DNS

DDoS Protection
Azure WAF
Azure Firewall
Azure Firewall Manager
Network Security Groups
Service Endpoints/Private Link

Network Watcher
ExpressRoute Monitor
Azure Monitor
Virtual Network TAP

CDN
Front Door
Traffic Manager
Application Gateway
Load Balancer

Exelegent

Azure Application Delivery portfolio

Together, application delivery services let you build mission-critical dynamic, high-performance global applications


Azure Front Door


Web Application Firewall


Application Gateway


Azure Load Balancer


Azure CDN


DDoS Protection


API Manager


Azure Traffic Manager

Secure Multi-Cloud Environments Workshop phases and activities

Pre-engagement Call
– 1-2 hours *

- Introductions
- Engagement walk-through
- Expectations
- What's next

Secure Multi-Cloud Environments Workshop questionnaire

- Fill in and return the questionnaire
- Other pre-engagement preparations

Microsoft Defender for Cloud Overview – 1 hour [optional]

- Microsoft Defender for Cloud overview presentation

Kick-Off Meeting – 1 hour

- Engagement walk-through
- Engagement tools
- Expectations
- What's next

Define Scope – 1 hour

- Define and document deployment scope

Configuration and Verification
– 4 hours

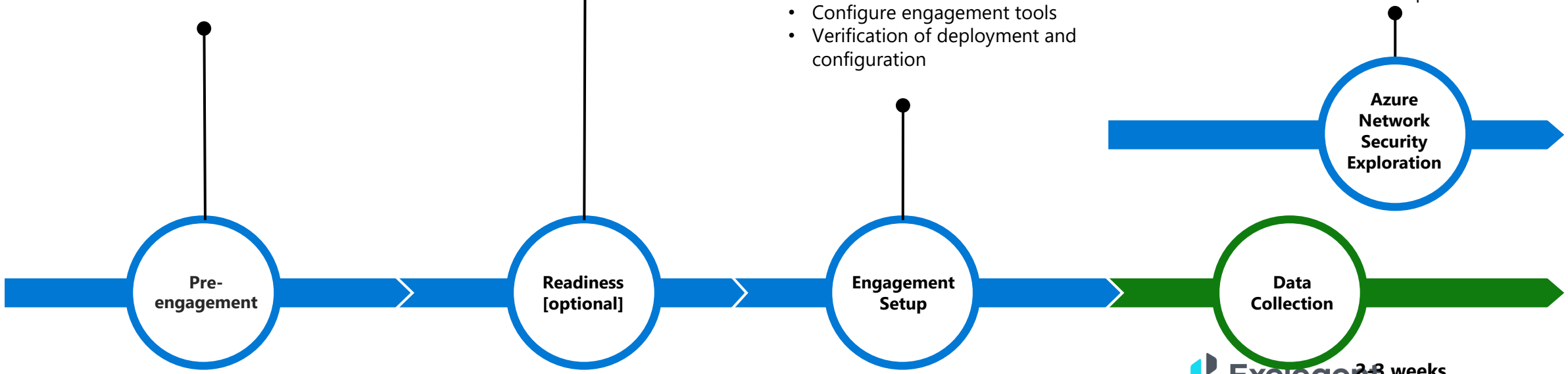
- Configure engagement tools
- Verification of deployment and configuration

Azure Network Security Overview – 1 hour [Optional]

- Azure Network Security overview presentation

Azure Network Security Demonstration and Discussion – 2 hours [Optional]

- Azure Firewall demonstration
- Azure Web Application Firewall demonstration
- Azure DDOS Protection Standard demonstration
- Discussion of next steps



Exelegent

Secure Multi-Cloud Environments Workshop phases and activities

Threat Exploration and Report Generation – 4 hours

- Threat Exploration
- Report Generation

Threat Results Presentation – 1 hour

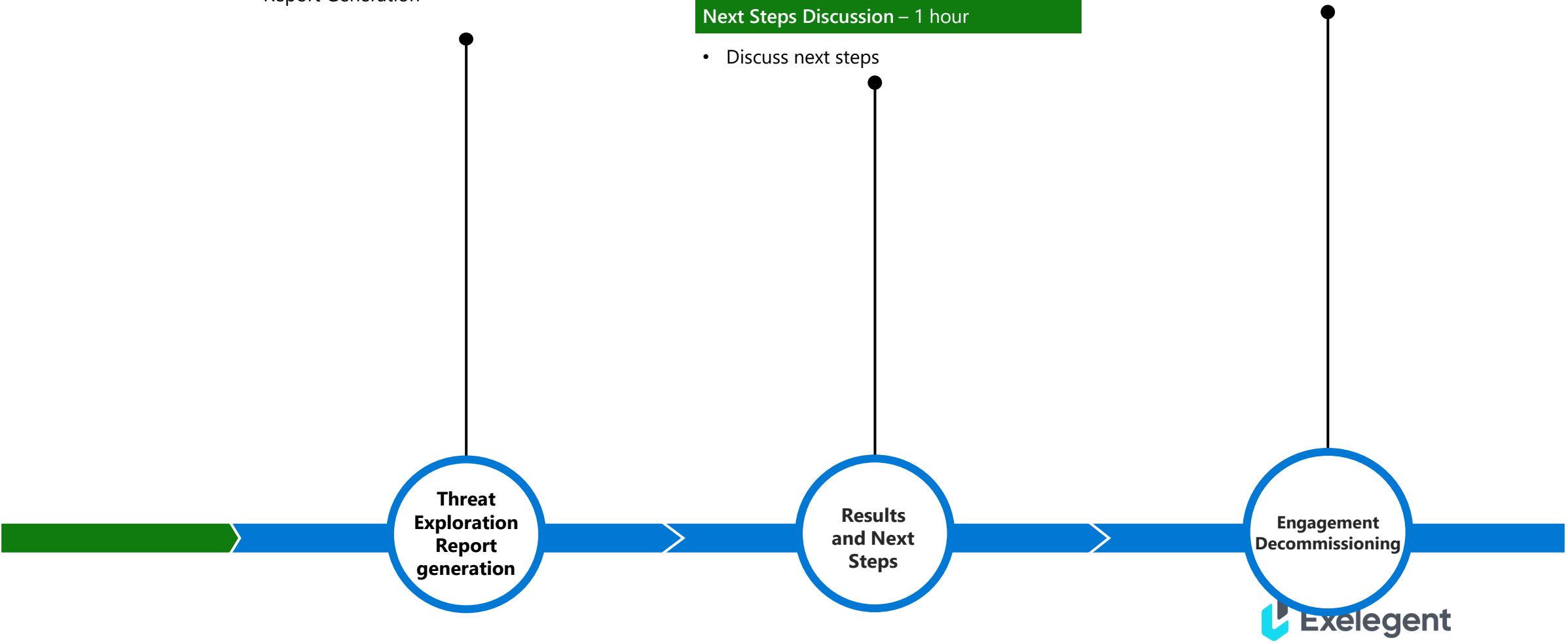
- Present and discuss results
- Record next steps

Next Steps Discussion – 1 hour

- Discuss next steps

Engagement Decommissioning – 1 hour

- Remove configuration changes
- Deactivate trial licenses



Exelegent

Use of Microsoft Defender for Endpoint

Licensing – Microsoft Defender for Cloud includes license for Microsoft Defender for Endpoint for Windows and Linux servers.

Compatibility - to be able to showcase the best possible experience with Microsoft Defender for Endpoint we need to consider the potential impact of running Microsoft Defender for Endpoint on servers side-by-side with existing non-Microsoft antivirus (AV) and/or Endpoint Detection and Response (EDR) solutions.

Existing AV/EDR solutions	Impact	Recommendation
AV solution: Microsoft Defender Antivirus **EDR Solution:** None	No impact.	Onboard servers to Microsoft Defender for Endpoint without additional changes required. RECOMMENDED
AV solution: Non-Microsoft product **EDR Solution:** None	It is not recommended to run Microsoft Defender Antivirus in parallel with a non-Microsoft antivirus solution due to potential performance issues.	To experience the full functionality of Microsoft Defender Antivirus and Microsoft Defender for Endpoint we recommend disabling or uninstalling existing non-Microsoft AV solutions on the servers included as part of the engagement.
AV solution: Microsoft Defender Antivirus **EDR Solution:** Non-Microsoft product	It is not recommended to run Microsoft Defender for Endpoint in parallel with a non-Microsoft EDR solution due to potential endpoint performance issues.	We recommend that you uninstall or disable the existing non-Microsoft EDR on the servers included as part of the engagement before onboarding the devices to Microsoft Defender for Endpoint.