DELPHI
IT STRATEGY | CONSULTING | SUPPORT

Microsoft Partner
Microsoft

Gold Communications
Gold Cloud Platform
Gold Cloud Productivity
Gold Enterprise Mobility Management
Gold Windows and Devices

FastTrack Ready Partner

Microsoft Defender for Servers – Pilot

Protective Shield for your Servers

ABOUT DELPHI CONSULTING:

When it comes to Security, you need an experienced partner. We have been Microsoft security and compliance finalist for 2020. We will work with you to understand your environment and identify opportunities to help you achieve continuous business value from your Teams investment.

As a trusted adviser, Delphi Consulting can help you protect your environments from an ever-evolving threat landscape with Microsoft Security and Compliance solutions.

See what customers are saying:

We met most of our security needs of detecting and blocking threats on servers with Defender ATP. The solution enables us to achieve comprehensive security and setting up with no downtime.

- Edwin K George , Redington Gulf FZE

WHAT WE OFFER

Securing servers is vital to protecting the reputation of your organization, as well as from the loss of money, productivity, and critical data. One server attack can bring an organization's critical operations to rapid halt. Cybercriminals understand that by targeting servers, they can inflict maximum damage, while still spreading laterally to other organizational servers and workstations. These data-rich targets provide criminals with the opportunity for data theft and ransom of sensitive information like financials, intellectual property, and more.

Delphi Consulting will help you onboard pilot set of servers to Microsoft Defender ATP demonstrating the advanced attack detection and investigation capabilities through Microsoft Defender Security Console.

Delphi's offering:

- Drive session with customer security team to understand all the security requirements around the Windows and Linux servers
- Onboard 2 servers each of below OS using GPO/SCCM
    - Windows Server 2008 R2
    - Windows Server 2012 R2
    - Windows Server 2016
    - Windows Server 2019
    - Linux Server
- Configure Advanced Security Configuration Policies
- Deliver High Level Design Document.

Why Microsoft Defender and Delphi?

Microsoft 365 Defender - Pilot

Delphi Consulting will guide you through the steps to start the Pilot onboarding of Servers to Microsoft Defender ATP based on the recommended deployment paths.

In addition to the onboarding, Delphi Consulting will help you set up the required security configuration policies for the servers.

Scope of Work

- Initial Discovery Assessment –Review the current AV policies, understand any specific security requirements, exceptions, need for auto-remediation, etc.
- Technical enablement
  - Install and configure Windows Defender AV and System Center Endpoint Protection client based on the server OS
  - Install and configure Microsoft Monitoring Agent
  - Configure the Linux Software Repository
  - Configure Security Configuration Profiles including scheduled scans, scan settings, real-time protection, exclusions
  - Integration with existing SIEM solution/3rd party solutions
- Provide Technical & Operational Guidance
- Documentation

Customer Key Take-aways

- Get a complete overview and understanding of Microsoft Defender ATP capabilities for Windows and Linux based servers
- Provide an overview on the Defender for Servers Licensing
- Get a high-level solution plan, roadmap and next steps
- Get a high-level Architecture Diagram
- Enable rapid detection, investigation, and response

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. Defender for Endpoint extends support to also include the Windows Server and Linux Server operating system. This support provides advanced attack detection and investigation capabilities seamlessly through the Microsoft Defender Security Center console..

Features & Capabilities

Attack Surface Reduction

ASR rules target specific types of behavior that is typically used by malware and malicious apps to infect devices. That includes protection against files and scripts used in Office apps, suspicious scripts, unexpected behavior of apps and more.

Next Generation Protection

Microsoft Defender Antivirus is the next-generation protection component of Microsoft Defender for Endpoint. This protection brings together machine learning, big-data analysis, in-depth threat resistance research, and the Microsoft cloud infrastructure to protect devices in your enterprise organization.

Cloud Security Analytics

Leveraging big-data, device-learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products and online assets, behavioral signals are translated into insights, detections, and recommended responses to advanced threats.

Threat Intelligence

Generated by Microsoft hunters, security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Defender for Endpoint to identify attacker tools, techniques, and procedures, and generate alerts when they are observed in collected sensor data.

Automated Investigation & Remediation

Microsoft Defender for Endpoint offers automatic investigation and remediation capabilities that help reduce the volume of alerts in minutes at scale.