MICROSOFT DEFENDER FOR SERVERS – PILOT

PROTECTIVE SHIELD FOR YOUR SERVERS

Microsoft Partner
Microsoft
Gold Application Integration
Gold Cloud Platform
Gold Application Development
Gold Cloud Productivity
Gold Collaboration and Content

Microsoft Partner
Microsoft
Gold Communications
Gold Data Platform
Gold Datacenter
Gold Enterprise Resource Planning
Gold Enterprise Mobility Management

Microsoft Partner
Microsoft
Gold Project and Portfolio Management
Gold Security
Gold Windows and Devices

Microsoft Partner
Microsoft
2020 Partner of the Year Finalist
Security and Compliance Award

FastTrack
Ready Partner

DELPHI
IT STRATEGY | CONSULTING | SUPPORT

MICROSOFT DEFENDER FOR SERVERS – PILOT AND HOW WE AIM TO HELP

DELPHI
IT STRATEGY | CONSULTING | SUPPORT

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.

Servers Onboarding

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Linux Server

Security Configuration Policies Creation

- Set automated response actions to threats based on the alert severity
- Setting up the scan settings
- Setting up exclusions
- Realtime protection & Advanced Settings

Integrations

- SIEM Solution
- SOAR Platform
- Microsoft 365 Security
- Threat Intelligence

MICROSOFT DEFENDER FOR SERVERS-PILOT OUR DELIVERABLES

DELPHI
IT STRATEGY | CONSULTING | SUPPORT

- 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
  - Configure Windows Defender AV and System Center Endpoint Protection client based on the server OS
  - 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 Microsoft 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

FEATURES AND CAPABILITIES

DELPHI
IT STRATEGY | CONSULTING | SUPPORT

Attack Surface Reduction

Protection against files and scripts used in Office apps, suspicious scripts, unexpected behavior of apps and more

Cloud Security Analytics

Leveraging big-data, device-learning, and unique Microsoft optics, behavioral signals are translated into insights, detections, and recommended responses to advanced threats

Features and Capabilities

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 organization

Threat Intelligence

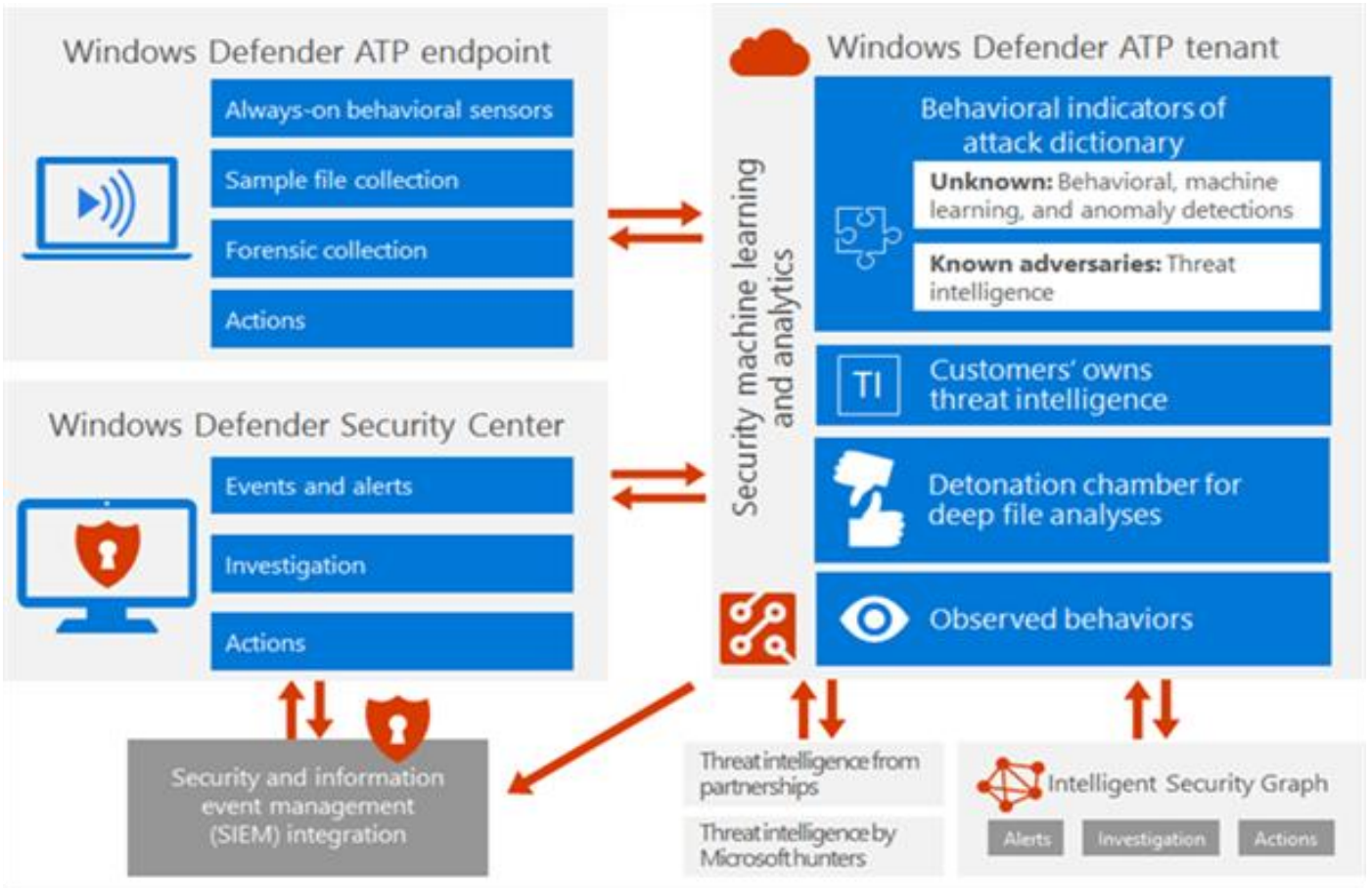
Generated by Microsoft hunters, security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Defender for Endpoint to identify attacker tools, techniques, and procedures

Automated Investigation & Remediation

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

DELPHI
IT STRATEGY | CONSULTING | SUPPORT

MICROSOFT DEFENDER ARCHITECTURE



DELPHI
IT STRATEGY | CONSULTING | SUPPORT

CUSTOMER SUCCESS STORY:

SERVERS THREAT PROTECTION FOR

REDINGTON GULF FZE

Redington Gulf FZE, one of the largest distributor of IT products in Middle East and Africa sought to gain a deeper visibility and control over the risks and threats identified on their on-premise servers.

Results:

- Comprehensive set of security controls configured on the servers.
- Enhanced Threat Detection and Protection.
- Unified SecOps experience to gain a complete visibility on all kinds of devices.

CONNECT WITH US TO KNOW MORE:

Get	Get a free trial: [delphime.com]
Call	Call for more information: [+971 56 253 1541]
Ask	Ask a Marketplace offer
Question	question via email: [security@delphime.com]
Learn	Learn more: [delphime.com]
Link	Link to your Microsoft Commercial (To be added)

DELPHI
IT STRATEGY | CONSULTING | SUPPORT