DIFENDA

MICROSOFT ENDPOINT DETECTION AND RESPONSE (EDR)

DIFENDA MANAGED EDR AND DEPLOYMENT OVERVIEW

PRAGMATIC COST-EFFECTIVE BUSINESS VALUE

The Big Picture:

More and more organizations are taking a broader look at their security posture and embracing a Zero Trust approach to long term security plans. A Zero Trust approach extends throughout the enterprise, defining a comprehensive security philosophy and end-to-end strategy. EDR is a core component in any Zero Trust architecture, which ensures product fit short and long term.

An Effective Controllable Cost:

Microsoft Defender for Endpoint integrates seamlessly with the Microsoft Security technologies, such as Microsoft Sentinel, Defender for Cloud Apps, Microsoft Purview. This saves time and money, reducing the need for complicated integrations and expensive training costs often associated with a patchwork approach. Its value is in minimizing risk and eliminating hidden costs, allowing you to focus on your business and bottom line.

Enterprise-wide Coverage and Visibility:

Defender for Endpoint extends your security coverage across different layers of your IT environment including servers, workstations, and mobile devices. It supplies visibility into endpoint activities across your organization, monitoring in real-time, collecting and analyzing data across all of your processes, files, activities, and network connections.

Industry Leading Intelligence:

Augment your team by leveraging capabilities generated by Microsoft hunters, security teams, and 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.

Support for the Hybrid Enterprise:

Microsoft's cloud-native approach ensures organizations can easily deploy and manage EDR capabilities across a distributed workforce and hybrid IT environments, including endpoints on-premises as well as in private and public cloud infrastructures.

THE BUILDING BLOCKS FOR A COMPLETE SOLUTION

Microsoft supports Zero Trust aligned endpoint protection by using the following core components:

Defender for Endpoint (MDE):

The center of endpoint protection, Microsoft Defender for Endpoint is designed to provide vulnerability management, attack surface reduction, threat detection and response capabilities, and automatic investigation and remediation features to help organizations protect their mobile devices, desktop computers, virtual machines, embedded devices, and servers.

Defender for Cloud:

Defender for Cloud includes the integrated license for Microsoft Defender for Endpoint, security baselines, OS level assessments, vulnerability assessment scanning, adaptive application controls (AAC), file integrity monitoring (FIM), and more.

Intune:

Central to any deployment or management requirement, Intune focuses on mobile device management (MDM) and mobile application management (MAM), allowing your organization to manage smartphones, tablets, laptops and other devices used by employees to access corporate data and applications. Intune integrates closely with other Microsoft services such as Azure Active Directory and Microsoft 365.

Azure ARC:

Like Intune, ARC extends Azure's management capabilities, enabling organizations to control resources running outside of an Azure environment. These resources can include physical or virtual servers, Kubernetes clusters, and data services across on-premises, multi-cloud environments, and edge locations.

CORE DIFENDA SERVICES – DEPLOYMENT SERVICES AND MANAGED EDR

Deployment Services

Every implementation is custom designed with your organizational needs fully defined. Design documents and deployment plans are developed with your team, then supplied and approved before work begins. At a high level, the deliverables for a standard deployment include:

- **MDE configuration design and deployment plan**
  - Design and support configuration of Intune (Defender for Endpoint) + Azure ARC (Defender for Servers)
  - Consider / document plans for unsupported Operating Systems

- **Develop an MDE design and deployment document**
  - Assumes Intune used for workstation MDE deployment and Azure ARC for server MDE deployment
  - Deployment plan to include initial test phases
- **Provide knowledge transfer + migration support**
- **Deliverables:**
  - Intune / ARC Design document
  - Defender for Endpoint Design and Deployment document

Managed Services

Difenda Managed Services are designed to support ongoing cyber program maturity and reduce loads on internal teams. As part of the service, customers benefit from Difenda AIRO, our automated triage and response engine backed by our 24x7x365 ISO27001, SOC II Type 2 and PCI Certified Cyber Command Center (C3) team for around-the-clock protection.

We use iterative processes to help customers tune configurations to enhance proactive controls and reduce alert volume. Real-time insights are generated through our Difenda Shield Analytics platform, providing cyber security leaders with the data points and dashboards required to drive cyber strategy.

Difenda's 4 step methodology to provide actionable outcomes:

THREAT PROFILING
Iterative contextualization of environmental threats.

THREAT DETECTION
Rapid, 24x7 identification of threats.

THREAT HUNTING
Continuous search for new and emerging threats.

THREAT RESPONSE
A combination of automated processes and human intervention for effective threat containment.

What's included?

- **Managed EDR Implementation**
  - Microsoft Defender for Endpoint (MDE) Implementation Support
  - Microsoft Sentinel Implementation and MDE Integration
  - Microsoft Sentinel Custom Development (Analytic Rules, Playbooks, etc.)
  - Difenda Shield EDR Services Overview
  - 24x7x365 Managed EDR triage and response
- **Difenda AIRO Automated Triage and Response engine (SOAR)**
  - Difenda Shield Analytics Platform portal and real-time reporting
  - Integrated Threat Intelligence, including advisories and bulletins
  - Proactive Threat Hunting
  - Remote Incident Response (RIR) retainer
  - Dedicated Technical Account Manager (TAM) & Customer Success Manager (CSM)

WHY DIFENDA

Difenda is a cybersecurity managed service provider that takes a cybersecurity-first, Microsoft-only approach to solving today's toughest cybersecurity challenges. As a Full Stack Microsoft Security Services Provider, we leverage the full suite of Microsoft Security technologies to deliver comprehensive managed extended detection and response (MXDR) services. Our team ensures 24/7/365 coverage, providing end-to-end security operations tailored to your organization's unique needs. Difenda focuses on professional and managed services that support and evolve with you at every stage of your cybersecurity journey, accelerating your security operations maturity.