Difenda Managed Detection & Response

MDR

DIFENDA

Why Difenda?

It's all about the outcomes with Difenda. We take a value-driven approach to cybersecurity that keeps the focus on your success and helps you achieve mission-critical outcomes.

Decades of combined experience putting customer success first

It all started in 2008 with one mission: help our customers achieve success. Since then, we've leveraged our agile, innovative, and collaborative approach to create the powerful, modular cybersecurity suite Difenda Shield and launched several advisory and offensive security services to drive awareness and meaningful outcomes across the people, processes, and technologies that drive the modern enterprise forward.

Go-to Microsoft partner for complex Azure Sentinel deployments

Difenda is the company Microsoft recommends when their customers have difficult Azure Sentinel deployments. We are a proud Microsoft Gold Partner that has deep domain expertise when it comes to Azure Sentinel, Microsoft Defender, and the entire Microsoft security ecosystem.

Certified and compliant with industry-leading standards

Work with the best of the best when it comes to managed detection and response (MDR). We are compliant with PCI DSS, AICPA SOC 2, ISO 27001, and more. Difenda is also recognized by IDC and has a strategic partnership with CyberNB.

Manage advanced threats with Difenda MDR

Difenda MDR offers an enterprise-grade suite of managed detection and response services that unifies your people, processes, and technologies. We actively protect your cloud and on-prem applications, endpoints, network, and servers using agile cybersecurity technology, an integration-friendly approach, and a team with decades of combined DevSecOps experience.

Stay protected with full coverage from our C3

24/7 protection is the standard with Difenda MDR thanks to our best-in-class cyber command centres. With Difenda MDR, you get access to experienced teams of threat hunters, dedicated TAMs and CSMs, and project managers that keep your priorities in focus.

MDR

What's Included in Difenda MDR?

Difenda MDR offers the latest in Microsoft's extended detection and response (XDR) technology—allowing organizations of all sizes to benefit from a world-class cybersecurity program that's built for scale, and integration-ready from day one.

Difenda's MDR uses top security frameworks like the MITRE ATT&CK® and NIST Cybersecurity Framework to continuously identify, develop, and release enhanced detection and response capabilities.

Threat Profiling

Gain a thorough understanding of your organization's attack surface, critical infrastructure, sensitive data, and operational processes with full visibility into your threat landscape.

Threat Defense

Leverage Microsoft's AI-powered endpoint detection & response (EDR) technology to prevent, contain, and remediate attacks from all threat vectors before, during, and after execution.

Threat Hunting

Collect, analyze, and detect threats by combining Microsoft's security incident and event management (SIEM) technologies and Difenda's threat hunting teams.

Threat Response

Contain threats faster with 24/7/365 managed threat investigation and response. Difenda MDR customers get access to preferred rates for our remote incident response, giving you an immediate defense strategy to mitigate potential breaches.

Threat Intelligence

Access industry-leading threat intelligence (powered by Anomali) to improve your detection capabilities, receive proactive bulletins for potential threats, discover recent global attack campaigns in your industry, and leverage insights from our threat library through our C3 team.

Dashboards and Reporting

Stay protected with access to insights that go far beyond reporting offered by traditional Managed Security Service Providers (MSSPs). Drive informed decision making with full visibility into your security processes and technology.

How Does Our MDR Process Work?

Difenda MDR minimizes the gap between speed of compromise and speed of detection with proactive threat hunting and incident response services that reduce attacker dwell time and mitigate the potential impact of a breach.

Difenda Labs environment is a core part of our process that simulates common customer environment components. Within the Difenda Labs environment, our Cyber Research and Response team runs continuous attacks based on current cyber tactics and techniques used to breach customer environments. Successful attack patterns are translated into detection and response requirements, which are developed and released to Difenda Shield services using an agile delivery methodology.

Cyber Comman Center (C^3)

Cyber Detection & Response

- Alert Investigation
- Threat Hunting
- Threat Response

24x7x365 Threat Hunters

Technical Leads

Technical Management

DevSecOps

- ATT&CKDetection Development
- Difenda Shield Development

Developers

Development Management

Cyber R&R

- Cyber Research
- Incident Response

R&R Team

R&R Management

Platform & CloudSec

- SIEM/Platform Management
- Cloud Security
- System Integrations

Platform Team

Technical Lead

CloudSec Team

Technical Leas

Platform & CloudSec Management

C^3 Customer Support Teams

Customer Success

TAMS

TAM Management

CSMs

Sales Management

Project Management

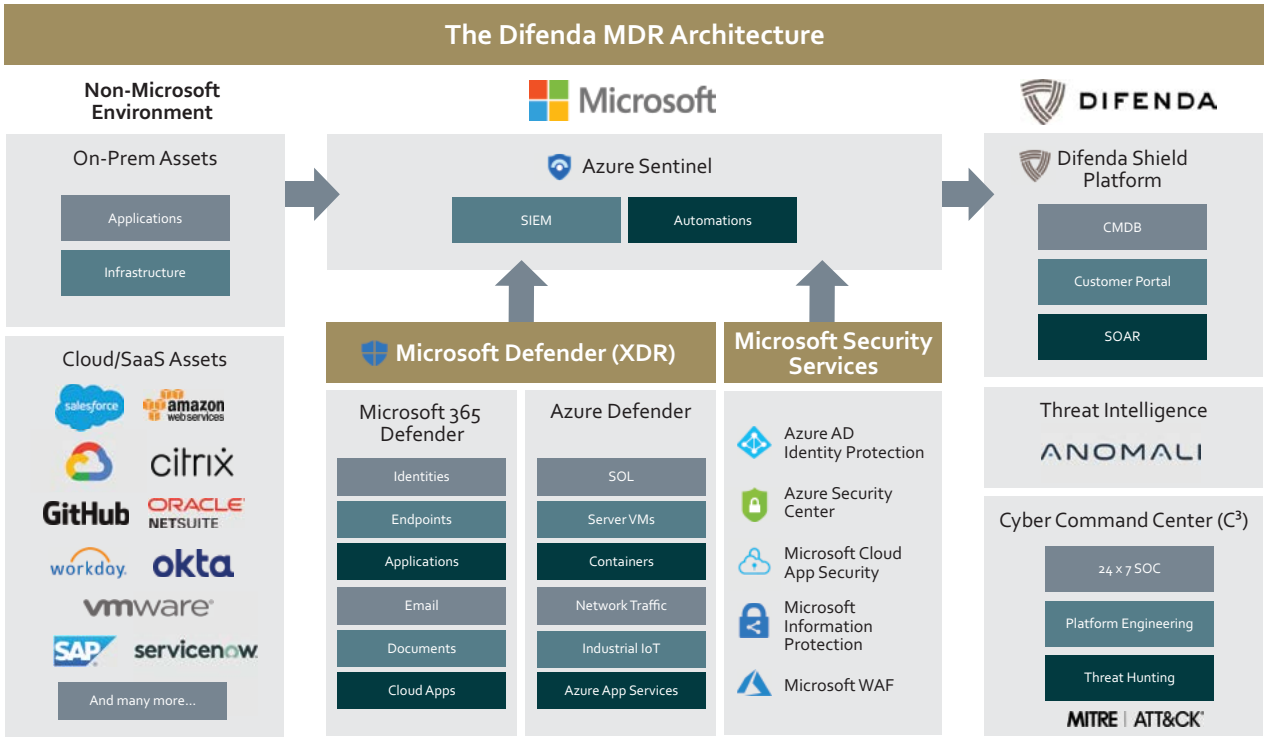
Project Managers

PM Management

Simplify Your Security Processes

With an integrated cybersecurity suite that leverages Azure Sentinel, Microsoft Defender, and active services to provide proactive and ongoing protection. Our MDR solution is also compatible with Azure Active Directory (Azure AD), Microsoft Cloud App Security (MCAS), and Microsoft Information Protection (MIP).

1. Deploy quickly with out-of-the-box integrations for popular products and services.
2. Supports syslog or CEF log forwarding or custom log forwarding
3. Security event data flows from your SaaS and cloud service providers into Azure Sentinel and Difenda Shield.
4. Security event data flows from your endpoints, servers, and on-prem infrastructure into Azure Sentinel and Difenda Shield.
5. Difenda Shield and Azure Sentinel automatically analyze event data, identify threats, and respond accordingly.



See the Entire Picture With the Difenda Shield Portal

Every Difenda Shield customer can use our Difenda Shield Portal, a powerful web-based platform where you can interact with various aspects of threats, make changes to requests, and more.

Our Difenda Shield dashboards allow you to:

- Collect daily trend data
- Provide a summary of key information to improve decision making
- Enable end-user dashboard parameter selection
- Support for interactive drill down into underpinning data
- Export dashboards and reports to supported formats
- Automatically pull, store, and report on monitored assets, daily threat events, and service requests

Supported Technologies (Out-of-the-Box)

- Azure Sentinel
- Azure Active Directory (Azure AD)
- Azure Security Center
- Microsoft Cloud App Security (MCAS)
- Microsoft Defender (Azure, Endpoint, & Servers)
- Microsoft Information Protection (MIP)

Supported Technologies (Custom Integration)

Integration of custom data sources is possible via API or log ingestion.

Please contact us for more details.

DIFENDA

Difenda MDR has a process for onboarding that has been perfected over the years with our team of experts to ensure the success of your plan.

How Does Onboarding Work?

Our Rapid Cover™ deployment methodology allows us to get MDR production-ready very quickly and consistently—even when you're starting from scratch.

Prepare
Our team of experts will go through a comprehensive checklist and onboarding process to ensure we can streamline your project successfully.

Build
Any Difenda Shield services which are using one or more Microsoft security technologies are designed, implemented, and enabled by our team.

Connect
Once the systems are built and ready, the first telemetry data can be sent. Once an asset begins transmitting event log data—you're protected. For services that require customer-managed technologies, our team will reach out to you with instructions and guidance to help you configure your connections as needed.

Verify
We then validate that each service is operating as designed with a formal quality assurance process. This includes configuring and monitoring to ensure that Difenda Shield is always protecting you.

Fortify
This series of collaborative working sessions ensures that every customer we work with hits the ground running and can maximize Difenda Shield while transitioning from onboarding to ongoing operations. These sessions include documentation delivery, knowledge transfer sessions, and ongoing operational meetings.

What Can You Achieve With MDR?

Proactive Approach to Security Risks
Develop a quantitative and qualitative understanding of the risks created by your people, assets, data, and technologies before an incident occurs.

Cloud-Native MDR Offering Infinite Speed and Scale
Quickly expand your cybersecurity capabilities with access to next-gen, cloud-native cybersecurity solutions built for speed and scale.

24/7/365 for the Entire Business
Keep your business protected at all times with 24/7/365 that leverages automation, tactical response teams, and multiple C3 locations to ensure service availability.

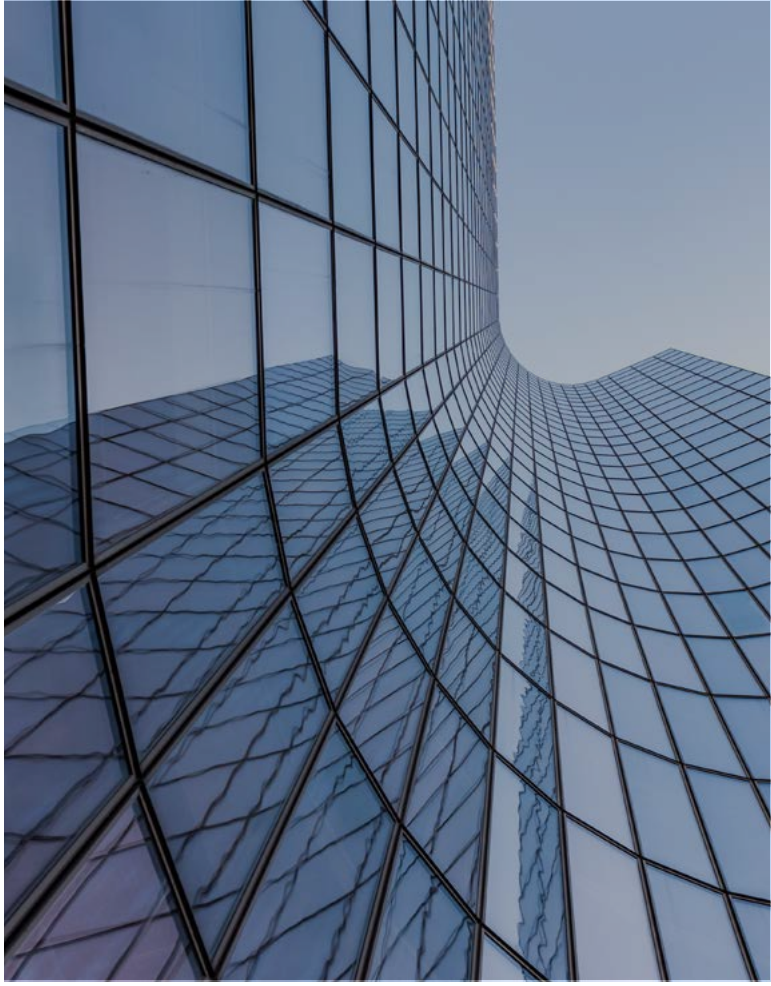
Integration-Friendly Cybersecurity Solution
Our integration-friendly approach means you always get access to cutting edge cybersecurity technology through the Difenda Shield and Microsoft's award-winning security solutions.

Create a Collaborative Cybersecurity Process
Turn cybersecurity into a company-wide objective with real-time data dashboards, notifications, alerts, and enhanced visibility using the Difenda Shield Portal.

Enhanced Protection With Automation
Identify and respond to threats quicker with automated processes that proactively alert key members of your security teams, ingest data, coordinate responses, and remediation.

MDR for On-Prem, Cloud, or Hybrid
Whether you're looking for on-prem, cloud, or hybrid—Difenda MDR is the easiest way for you to integrate a best-in-class MDR solution into your cybersecurity stack.

Work With the Azure Sentinel Experts
Difenda is Microsoft's go-to partner for complex Azure Sentinel configurations. Implement best practices and drive valuable insights with ongoing support and solution optimization.



Stay protected with a cybersecurity solution that's both proactive and reactive

Get in touch with a Difenda MDR specialist today sales@difenda.com

Learn more at www.difenda.com/mdr