OLIVE + GOOSE

Your Endpoint Security with Our Managed Microsoft Defender + EDR Service

Executive Summary & Service Overview

Managed Microsoft Defender + EDR

Proactive Endpoint Protection Backed by Microsoft + Human Expertise

Cyberattacks continue to evolve—and endpoints are often the first target. Our Managed Microsoft Defender + EDR service is built to deliver next-gen protection using the security tools you already own. We combine Microsoft Defender Antivirus with expert monitoring, response, and remediation to deliver a full-scale Endpoint Detection and Response (EDR) solution.

As a Microsoft Gold Partner, we help you strengthen your security posture while maximizing the value of your existing Microsoft 365 investment.

Why Organizations Choose Us

- **Built on Microsoft Defender:** No need to add another agent—just unlock the full power of what's already in your stack.
- **Full-Service Management:** We take care of configuration, monitoring, response, and continuous improvement.
- **Expert-Driven EDR:** Our analysts review alerts, hunt for threats, and act fast when automated protection isn't enough.
- **Simple, Scalable Security:** Whether you manage 50 or 5,000 endpoints, our platform adapts to your needs.
- **Improved ROI & Reduced Risk:** Offload day-to-day endpoint security and free your team to focus on higher priorities.

Key Capabilities

- Real-Time Threat Detection & Containment
- Behavioral Analysis & Persistent Threat Hunting
- Ransomware Canary Traps
- Policy & Exclusion Management
- Customizable Alerts & Reports
- Direct Integration with Microsoft Security Stack
- Continuous Visibility into Device Health & Risk

OLIVE + GOOSE

Technical Detail & Customer Value

How It Works

Our team connects directly to your Microsoft Defender environment using secure integration, extending it with advanced threat detection, expert analysis, and live remediation support.

We analyze endpoint telemetry in real time to identify threats like:

- Fileless malware and malicious process chains
- Lateral movement attempts
- Unauthorized persistence mechanisms
- Ransomware deployment activity
- Suspicious PowerShell or script abuse

Use Case Example: Ransomware Prevention

A user receives a phishing email that drops a loader attempting to launch ransomware. Microsoft Defender flags the executable, but it's our system that detects lateral movement and persistence attempts. Within minutes, we:

- Isolate the affected endpoint
- Kill the malicious processes
- Provide a post-incident report with next-step guidance

What You'll See as a Customer

- A clean, multi-tenant dashboard to view detections and device status
- Daily threat intel and executive summaries
- Transparent remediation logs with recommendations
- Zero overhead on your internal team—everything is managed

Ready to Modernize Your Endpoint Protection?

Let us help you secure your environment with the EDR capabilities you need—without the complexity.

Start your free trial or reach out today for a personalized walkthrough.

Contact Us: Olive + Goose
info@oliveandgoose.com
https://www.oliveandgoose.com