Benefits

Generate new revenue streams
From advanced threat hunting, detection and prevention, to incident response, compliance, and risk assessment, extend your catalog to service all customer needs

Meet rigorous client SLAs
Triage and investigate all alerts in seconds, increasing incidents handled by 10-100x and improving productivity from even inexperienced staff

Lower operational costs
Augment your existing security technology and scale your staffing resources by automating several Tier 1, 2, and 3 tasks

Reduce response times
Automate the investigation and analysis of security alerts to cut response times to mere seconds

Eliminate remediation downtime
Deploy any of the remote cleanup techniques to get systems back to a healthy state without disruption, then extend prevention across all clients

Increase endpoint productivity
Eliminate the need for multiple endpoint agents and streamline your EDR needs with a the low-impact Secdo agent on endpoints

SUPERCHARGE
MSSP & MDR SERVICES

Secdo's Managed Services Partner Program combines the only multi-tenant Endpoint Detection and Response (EDR) platform that has been purpose-built precisely for service providers, with a flexible arrangement that offers extensive support and zero upfront terms—ensuring your success, every step of the way.

Whether you are an established MSSP or are looking to build an MDR practice, the challenges of a managed service provider are often the same: generating more revenue, meeting rigorous customer SLAs, staffing 24/7 teams, decreasing operational costs, and looking for ways to differentiate your operation.

Secdo offers the most complete platform to centralize every function of detection and response, including advanced threat hunting, threat detection and prevention, alert triage and investigation, incident response, compliance and risk assessment. It allows you to establish—or grow—your managed security services with the tools you need to dramatically increase the efficiency of your current services, extend your catalog, generate new revenue streams, and meet client demand for key services.

Program Highlights

Flexible Deployment

Roll out Secdo instantly—on-prem or in the cloud—and begin servicing clients immediately

Extend Your Service Catalog

- Alert Triage & Investigation
- Incident Response
- Proactive Threat hunting
- Insider Threat Detection
- Customized Threat Prevention
- Anti Ransomware
- Application Control
- 24/7 Monitoring
- Compliance Support

Zero-upfront Terms

No startup costs from initial scoping to setup and training

How Secdo Works

For MSSP Workflows

Secdo's multi-tenant, SaaS platform can be integrated with SIEM and threat-detection technologies to streamline alerts and automate their analysis. Combining a low-impact agent for thread-level endpoint visibility—the most granular view available today—with its Causality Analysis Engine™ to automatically investigate each incoming alert in seconds, Secdo:

- Correlates alerts related to the same threat, reducing their total number
- Re-prioritizes alerts based on the level of risk assessed in the threat activity
- Reveals a complete picture of the threat, including a forensic timeline of all activity
- Determines the root cause of the attack
- Verifies artifacts against reputation services
- Initiates a customizable playbook of response actions for identified attack behaviors

By automating the investigation process—including root-cause analysis and reputation verification—security analysts of any skill level can validate an alert with the speed and accuracy of a seasoned expert. This level of performance allows security operations to work with complete efficiency, lowering training time for new analysts, reducing the burden on experienced team members, and drastically increasing the number of alerts handled per hour.

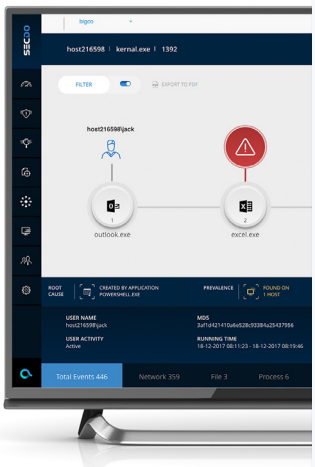
For MDR Workflows

Secdo's integration with SIEM and other threat detection technologies ensures incident response teams have complete visibility from the initial security alert to the automated investigation within a single platform. By taking advantage of the forensic detail—in addition to the complete picture of the threat, attack timeline and root-cause analysis—incident response teams can immediately identify threat artifacts and surgically respond to incidents, allowing fast containment and removal from one or many infected systems.

To prevent the recurrence of similar activity across single or multiple client deployments, Secdo can then be programmed with behavioral indicators of compromise (BIOCs) to automatically prevent or terminate attack behaviors that resemble any previous incident. Along with traditional IOCs, Secdo's BIOCs are also used as powerful search queries to conduct advanced threat hunting and proactively identify vulnerabilities that may lead to possible risk. The results of these queries are also automatically investigated and any identified attack activity can be programmed for future prevention—eliminating repetitive handling of the same event, creating customizable threat prevention and significantly lowering the attack surface for each unique network.

About Secdo

Secdo offers the only endpoint security platform to automatically investigate and resolve every security alert for you, cutting the time it takes to detect and respond to security alerts down to seconds. With enhanced productivity, security teams leverage Secdo's unrivaled thread-level visibility to hunt for unseen threats, creating a scalable proactive defense. Secdo is headquartered in New York, NY, with office and security teams around the globe.



Platform Highlights

Multi-Tenant EDR Solution
Move seamlessly and securely between tenants, purpose-built to improve existing services, and multiply revenue streams

Automated Investigations
Reduce alert triage and incident analysis to seconds while eliminating repetitive tasks through automation

Surgical Response
Surgically remediate any threat without affecting business continuity with dozens of remote response tools

Adaptive Defense
Optimize Secdo to prevent the recurrence of any threat using attack behaviors across one or all tenants

Limitless Threat Hunting
Hunt for external threats, file-less attacks, policy violations and malicious insiders

Unmatched Visibility
Gain instant access to live and historical thread-level activity of every endpoint in seconds

Tech Specs

Delivery Model
On-Prem / Private Cloud / Hybrid

Scale
From 1 to over 300,000 Endpoints

Retention
100 days minimum storage of endpoint data

Deployment
Silent, with optional fast mode

Communication
SSL encrypted

Agent & Network Resources
< 1% CPU, 50 MB RAM
< 7 MB of network traffic / day

Windows | Mac | Linux

SECDO

Voted #1 Incident Response platform on G2Crowd

E info@secdo.com T 917.338.2277 www.secdo.com