seceon
SECURITY FOR EONS

PRODUCT GUIDE

Seceon EDR & EPP

Endpoint Protection, Detection & Response with aiXDR-PMax

EDR •EPP • FIM• DLP •Device Control • Vulnerability Assessment • Live Forensics

This guide provides a complete reference to Seceon's endpoint security capabilities delivered through the aiXDR-PMax platform covering every prevention, detection, investigation, and response feature available to enterprises, MSPs, and MSSPs. It consolidates content from Seceon datasheets, solution briefs, RFP specifications, and seceon.com.

Contents

1. Executive Overview
1.1 Two Deployment Choices, One Platform
1.2 Key Outcomes
2. Product Architecture
2.1 Telemetry Collected by the Agent 2.2 Agent Footprint & Performance
2.3 Supported Operating Systems
3. EPP — Endpoint Protection Platform
3.1 Prevention Capabilities
3.2 Credential Theft & Advanced Attack Prevention
3.3 Binary & Application Control
3.4 Scanning Engine
3.5 End-User Experience
4. EDR — Endpoint Detection & Response
4.1 Detection Capabilities
4.2 Investigation & Threat Hunting
4.3 Response & Remediation
5. Data Security — DLP, Device Control & PII/PHI
5.1 Data Loss Prevention
5.2 Device Control & USB DLP
5.3 File Integrity Monitoring (FIM)
5.4 Vulnerability Assessment
5.5 Audit, Compliance & Retention
6. Native Platform Integration
6.1 Endpoint Dashboards & Analytics
7. Management & Operations
7.1 MSSP Operations
8. Complete Feature Matrix
9. Why Seceon for EDR & EPP
9.1 Differentiators
9.2 Cost Consolidation
9.3 Getting Started

1. Executive Overview

Endpoints remain the most targeted layer of the modern attack surface. Stealthy, persistent adversaries dwell silently inside networks for weeks or months, and desktops, laptops, and servers are often the weakest links in their preferred entry points. Traditional endpoint tools frequently fall short due to resource-heavy agents, siloed visibility, and a lack of intelligent automation.

Seceon aiXDR-PMax answers this challenge with a unified endpoint security offering that combines Endpoint Protection Platform (EPP), Endpoint Detection and Response (EDR), Data Loss Prevention (DLP), File Integrity Monitoring (FIM), Device Control, and automated remediation in a single lightweight agent — natively integrated with Seceon's AI/ML-powered aiSIEM and the broader Open Threat Management (OTM) Platform.

Unlike conventional tools that react after an attack, aiXDR-PMax continuously monitors and responds in real time, preventing threats before they escalate. Combining EDR, EPP, UEBA, and threat intelligence, it identifies phishing, malware, ransomware, insider threats, and multi-layered attacks across the entire environment from on-premises to cloud.

1.1 Two Deployment Choices, One Platform

Seceon offers partners and customers full flexibility in how endpoint security is delivered:

- **Bring Your Own EDR/EPP** — Ingest events and logs from an existing third-party EDR/EPP stack into Seceon aiXDR, centralizing detection and automated response across tools already deployed.
- **Seceon aiXDR-PMax** — Deploy Seceon's own EDR + EPP agents for complete, natively integrated endpoint protection, detection, and response with FIM, DLP, device control, vulnerability assessment, and PII/PHI monitoring included.

This flexibility lets partners customize deployments per organization. When aiXDR-PMax is deployed, teams gain increased protection, visibility, and context to uncover stealthy threats.

1.2 Key Outcomes

Outcome	How aiXDR-PMax Delivers
Faster Threat Detection	AI-driven correlation and behavioral analytics identify and contain threats before they spread, achieving MTTD in under 5 minutes.
Automated Incident Response	Automatically isolates endpoints, terminates malicious processes, and quarantines files in under 90 seconds.
Reduced Analyst Workload	Precision-driven detections and intelligent noise suppression reduce false positives by up to 95%, allowing analysts to focus on real threats.
Lower Total Cost of Ownership	Consolidates EDR, EPP, DLP, FIM, and Device Control into a single platform and license, reducing tool sprawl and operational costs.
Compliance & Audit Readiness	Supports PII/PHI discovery, File Integrity Monitoring, OS-level log collection, and endpoint data retention for up to 7 years to simplify compliance.

2. Product Architecture

aiXDR-PMax is delivered as an ultra-lightweight endpoint agent that streams rich telemetry into Seceon's Collection & Correlation Engine (CCE) and Analytics & Processing Engine (APE). All endpoint data is enriched in real time with user identity context, metadata, threat intelligence, and vulnerability assessments, then correlated by 4,000+ ML models alongside network, cloud, identity, and application telemetry.

2.1 Telemetry Collected by the Agent

The agent provides visibility into whether the endpoint is online or offline, with activity and summary data spanning:

- Files — Create, open, rename, delete, and execute operations, with full file interaction history.
- Processes — Process execution including the complete process tree, memory access, and process connections.
- Services & Drivers — Service and driver state, launched items, plists (macOS), and scheduled tasks.
- Registry — Registry changes on Windows endpoints.

- Network — Sockets, adapters, IP information, and per-process network activity.
- Scripts — PowerShell scripts, shell scripts, and command-line activity for living-off-the-land detection.
- User Activity — User logins, authentication attempts, and account activity for behavioral baselining.
- Software Inventory — Installed software / Application inventory and browser extensions.

2.2 Agent Footprint & Performance

Specification	Value
CPU Utilization	Under 2–3% during normal operation; up to 5% during full system scans
Memory Usage	Approximately 600 MB during initial setup, optimizing to under 100 MB during runtime
Disk Space	Approximately 750 MB
Threat Intelligence Database	12M+ known malware signatures, 1M+ exploit signatures, and 500K+ byte-code signatures
Malicious Hash Intelligence	Continuously updated threat intelligence with 8M+ known malicious file hashes
Update Management	Centralized, automatic updates with no user intervention or endpoint restart required

2.3 Supported Operating Systems

Platform	Coverage
Windows	Windows 7 and later; Windows Server 2008 R2 and later
Linux	Major distributions including Ubuntu, Debian, CentOS, Red Hat Enterprise Linux (RHEL), Fedora, and SUSE
macOS	macOS Mavericks and later; feature parity with Windows is under active development
Directory Integration	Native integration with Active Directory, supporting granular authentication and role-based access to the management console

The agent co-exists with commodity and proprietary software without bluescreens or process crashes, and protects fully offline endpoints. Threat protection does not rely on connectivity to a management server.

3. EPP — Endpoint Protection Platform

The EPP layer of aiXDR-PMax prevents threats from executing in the first place, using layered techniques: signature-based malware protection, machine-learning static analysis, behavioral analysis, dynamic (sandbox) analysis, and integrated threat intelligence.

3.1 Prevention Capabilities

- **Anti-Malware** — Identifies malicious files and blocks execution of viruses, trojans, ransomware, spyware, and cryptominers using signatures, ML static analysis, real-time sandboxing, and threat intelligence.
- **Ransomware Protection** — Protects against hostnames distributing malware that restricts system access and demands payment; detects unusual file behavior, lateral movement, and privilege abuse before encryption begins.
- **Malicious Web Download Protection** — Blocks harmful downloads before they reach endpoints.
- **Exploit Protection** — Identifies and prevents process-level, DLL-level (injection and sideloading), and network-level exploit attempts, including lateral movement and privilege escalation.
- **Blacklisted & Exploit IP Blocking** — Blocks known malicious or compromised IPs hosting C&C infrastructure, malware downloads, phishing sites, and drive-by download exploit kits targeting unpatched applications.
- **DGA Hostname Detection** — Detects domain generation algorithm hostnames used by malware families such as WannaCry, Conficker, and Ramnit to rendezvous with C&C servers.
- **Zero-Day Malware Protection** — Continuous anomaly and correlation insights identify and protect against the latest malware exploits, including zero-day and multi-layered attacks.
- **Offline Detection** — Detection continues in air-gapped environments or when internet connectivity is unavailable.

3.2 Credential Theft & Advanced Attack Prevention

- **Credential Dumping Protection** — Detects and blocks execution of Mimikatz and similar credential-dumping tools; identifies and blocks in-memory credential theft (credential dump, brute force) and network-based theft (ARP spoofing, DNS Responder).
- **Memory-Access Allowlisting** — Allows specific trusted processes (e.g., Webex, Chrome) to perform memory dump operations while blocking unauthorized processes.
- **Behavioral Analysis** — Detects suspicious patterns such as vssadmin delete shadows commands and blocks such actions — a hallmark of ransomware staging.
- **Attack Tool Detection** — Identifies and blocks usage of common attack frameworks such as Metasploit, Empire, and Cobalt Strike through process monitoring.
- **LotL Detection** — Detects use of legitimate tools for malicious purposes — a common living-off-the-land (LotL) tactic — enabling teams to act before damage is done.
- **Reconnaissance & Discovery Blocking** — Identifies and blocks reconnaissance (scanning) and unauthorized host enumeration — early signs of attackers attempting lateral spread.

3.3 Binary & Application Control

- **Block Unsigned/Unknown Binaries** — Contains unsigned executables, PowerShell scripts, DLLs, and drivers; exceptions allowed for pre-approved publishers (e.g., Microsoft, Cisco, Google).
- **Aggressive Mode Controls** — In aggressive mode, blocks and contains files that are unsigned or have unknown publishers for maximum-security postures.
- **Whitelisting & File Management** — Whitelist processes, file paths, command lines, and devices; review and restore files from quarantine through an intuitive interface — no command line required.
- **Application & Device Control** — Administrators control which applications and external devices can interact with company systems.

3.4 Scanning Engine

Scan Mode	Description
Quick Scan	Scans critical system areas, including running processes, boot sectors, system files, and memory for rapid threat detection.
Full Scan	Performs a comprehensive analysis of the entire endpoint, including files, registry, memory, and network-related components.

Scan Mode	Description
Performance	Maintains CPU utilization at 5% or less during scans, minimizing impact on endpoint performance.
Signature Updates	Includes automatic signature updates at least daily with no separate signature licensing; supports offline signature distribution for isolated environments.
Windows Defender Replacement	Can replace Windows Defender with a high-performance scanning engine for enhanced malware detection and protection.

3.5 End-User Experience

- **Real-Time User Alerts** — When the agent detects or blocks suspicious activity, end users receive a clear, timely notification — informed without confusion.
- **Dedicated Desktop Interface** — Endpoint-level visibility into logs, threats, web filtering status, and database sync — valuable for IT admins managing remote or distributed users.
- **Tamper Protection** — End users are blocked from accessing program settings; the agent alerts and blocks on any tampering or disabling attempt.

4. EDR — Endpoint Detection & Response

The EDR layer provides deep, continuous visibility into endpoint activity, enabling security staff to monitor, analyze, investigate, and respond with granular data, easy search, forensic investigation, and automated response through incident-response playbooks.

4.1 Detection Capabilities

- **Agent-Based Deep Detection** — Lightweight agents deliver deep insights into processes, services, executables, and files, with malware footprint detection through advanced correlation of pre-built rules running on the agent.
- **Runtime Behavioral Detection** — Identifies malicious behavior of executed files, running processes, registry modifications, or memory access and terminates them at runtime covering exploits, fileless attacks, macros, PowerShell, and WMI abuse using memory monitoring, heuristic process behavioral analysis, fuzzy hashing, and threat intelligence.

- **Lateral Movement Detection** — Identifies and alerts on SMB relay, pass-the-hash, and other lateral movement techniques via network traffic monitoring; supports deception via fake nodes, fake user accounts, and fake network connections.
- **Covert Exfiltration Detection** — Detects data exfiltration over legitimate protocols, including DNS tunneling and ICMP tunneling.
- **Account Compromise Detection** — Profiles user account baselines to identify malicious behavior indicative of prior compromise, policy violations, and anomalies.
- **Unauthorized Software Detection** — Identifies unauthorized programs, drivers, or services; granular insight into all applications, services, drivers, and browser extensions on Windows, Linux, and Mac endpoints.
- **Browser Extension Monitoring** — Ensures only trusted browser extensions are active, minimizing the attack surface.
- **Online/Offline Endpoint Tracking** — Tracks which endpoints (Windows, Linux, macOS) are online versus offline, in real time.

4.2 Investigation & Threat Hunting

- **Live Query** — Live forensic analysis directly on the endpoint: investigate running processes and files, machine-level state, and memory activity; obtain memory dumps on demand.
- **Cross-Organization Queries** — Search for the occurrence of any process, file, network, or user activity across all endpoints in the environment simultaneously.
- **Behavioral Pattern Search** — Search behavioral patterns across all coverage fields — users, files, machines, network traffic — and set rules, raise warnings, or assign risk levels based on results.
- **Transparent Alert Evidence** — Every alert exposes all indicators that raised it, so analysts understand how and when an attack happened across on-premises and cloud infrastructure.
- **MITRE ATT&CK Mapping** — Detections are mapped to MITRE ATT&CK TTPs, exposing adversary tactics including reconnaissance, evasion, and lateral movement.
- **Automated Risk Scoring** — Automatically assigns a risk score to all objects in the protected environment.

4.3 Response & Remediation

aiXDR-PMax executes automated and semi-automated remediation through Seceon's built-in SOAR approximately 70% of incident response is automated, with containment in under 90 seconds. Available response actions include:

Response Category	Actions
Endpoint Containment	Isolate endpoints from the network, connect or disconnect network interfaces, disable network adapters, modify IP configurations, and update the HOSTS file.
Process & File Remediation	Terminate malicious processes, delete files (including active runtime files), quarantine files with SHA-256 hash tracking, and remove malicious services or scheduled tasks.
Administrative Actions	Reboot or shut down endpoints and servers, and restore systems to normal operation after remediation.
Identity Protection	Disable Active Directory users, reset passwords, lock local or domain accounts, and block compromised credentials.
Network Enforcement	Block malicious IP addresses or domains at the firewall or proxy, perform DNS sinkholing, and block destination-based network communications.
Security Automation	Execute prebuilt incident response playbooks for common attack scenarios or create fully customized workflows to automate response actions.
Analyst Control	Allow administrator overrides for false positives and support alert-only mode for environments requiring manual approval before response actions.

5. Data Security — DLP, Device Control & PII/PHI

5.1 Data Loss Prevention

aiXDR-PMax includes data control and policy capabilities that discover and control sensitive data such as PII and PHI, capturing events at the system, user, and data level, whether the endpoint is connected to the corporate network or offline. Policies can be fine-tuned by user, risk level, or other context: from simply logging all actions to fully automated blocking, preventing data loss before it happens.

- **PII/PHI Discovery** — Automatically identifies all PII/PHI data movement within the organization, with visualization, analysis, querying, and reporting.
- **Custom Sensitive-Data Patterns** — Define custom patterns for regional identifiers, for example, Aadhaar numbers and ZATCA tax IDs, supporting compliance across multiple regulatory regions, including GDPR and HIPAA.
- **Data Movement Forensics** — Answers the key questions of who, where, what, and how about every sensitive data movement.

5.2 Device Control & USB DLP

- **Removable Media Control** — Secures and protects data on devices; blocks removable media (USB drive) access without admin permission.
- **Granular USB DLP** — Global or per-endpoint USB policy with exceptions for approved encrypted USB devices.
- **Peripheral Monitoring** — Monitors and restricts external storage devices to prevent data exfiltration; prevents unauthorized peripheral connections.

5.3 File Integrity Monitoring (FIM)

FIM continuously captures the what, who, and when of every file change in real time, so teams detect all changes, capture detail on each one, and use those details to determine security risk or non-compliance. FIM addresses the risks of data breach, system instability, degraded performance from unmanaged change, and compliance failure.

- Real-Time Change Detection — Detects any change to monitored files in real time; alerts can trigger even if a file was only accessed, not modified.
- Rich Change Context — Provides the time of change, the user responsible, the content, and the previous state of the file.
- Platform Coverage — Microsoft Windows, Active Directory (including Group Policy objects), Unix, and Linux.
- Baseline & Drift Analysis — Configuration data and system baselines let teams evaluate changes to less-critical files over time against overall system configuration.
- Privileged User & Compliance — Monitors privileged user activity for suspicious or unauthorized actions; supports PCI DSS and other regulatory requirements that mandate FIM.

FIM is configured centrally from the OTM console (Provisioning → FIM Configuration) per host and path, for Windows, Linux, and macOS. An EDR license and agent are required.

5.4 Vulnerability Assessment

Integrated vulnerability assessment proactively scans endpoint applications and systems to identify security gaps and misconfigurations that attackers could exploit, including missing security updates in systems and applications with prioritized findings so teams can remediate before exposure is exploited.

5.5 Audit, Compliance & Retention

- **OS-Level Log Collection** — Collects OS-level logs from all endpoints for compliance evidence.
- **Compliance Reporting** — Report templates supporting compliance and audit requirements, delivered from the central console.

- **Long-Term Retention** — Endpoint data stored in compressed form for compliance purposes for up to 7 years.

6. Native Platform Integration

Because aiXDR-PMax is built on the Seceon OTM Platform, endpoint telemetry is never siloed. It is correlated with network, cloud, identity, and application signals for full-kill-chain detection capabilities that standalone EDR products require separate SIEM, SOAR, UEBA, and TIP purchases to match.

Platform Capability	How It Enhances EDR & EPP
aiSIEM Correlation	Correlates endpoint telemetry with logs from firewalls, cloud platforms, identity providers, and applications to deliver high-fidelity, context-rich threat detection.
Built-in SOAR	Automates containment and remediation workflows across endpoints, networks, and identity systems in under 90 seconds.
UEBA	Uses 4,000+ machine learning behavioral models to baseline users and entities, uncover insider threats, and detect compromised credentials.
Threat Intelligence	Enriches detections with 8M+ malicious file hashes, IP and domain reputation, DGA intelligence, and behavioral indicators of compromise (IOCs).
NDR / NBAD	Combines network traffic analysis and behavioral anomaly detection with endpoint telemetry for comprehensive threat visibility.
SERA AI	Provides a GenAI-powered security assistant that answers natural language queries, explains alerts, and recommends remediation actions.
Multi-Tenancy	Delivers secure multi-tenant operations with logical separation of data, analytics, policies, and AI/ML models, making it ideal for MSSPs.
SIEM Export	Supports Syslog-based forwarding of alerts and events to third-party SIEM platforms when required.

6.1 Endpoint Dashboards & Analytics

The console provides real-time endpoint operational views, including:

- **Endpoint Health** — Endpoints Monitored, OS Distribution, and Infected Endpoints in real time — identify risky devices directly from the dashboard.
- **Activity Analytics** — Top Endpoints by Activity and Public Network Access, Countries Visited, and Risky Endpoints to spot unusual patterns.
- **Process & Network Analytics** — Top Processes Running, Query Result Distributions, and Network Stats using AI/ML baselining.
- **Trend Visualization** — Interactive charts for Endpoint Activities Trend, Process Analytics, and Network Events supporting proactive threat hunting.

7. Management & Operations

aiXDR-PMax is designed for convenient daily operation by security staff, at enterprise and MSSP scale:

- **Centralized Management** — Multi-site deployments report into a single management console; alerts are centrally collected and processed in real time.
- **Alert Tuning** — Alert exclusion rules for selected objects; rules to exclude specific addresses and IP ranges; severity rating of security alerts.
- **Configuration Portability** — Export the current configuration and import it to the same or another computer.
- **Update Management** — Central distribution of updates with no user intervention and no endpoint restart; scheduled update downloads with the option to disable automatic updates; offline signature distribution.
- **Notification Control** — Enable or disable notification types; email integration to notify security personnel on alerts.
- **Audit Logging** — Logging of all events, alerts, and updates; complete user-activity audit trail across tenant activities.
- **Zero-Touch Collection** — Endpoint, file, process, user-activity, and network telemetry collected in a fully self-sustained manner no manual rule/policy configuration or reliance on additional devices.

7.1 MSSP Operations

- **Multi-Tenancy** — True Multi-Tier Multi-Tenancy (MT-MT) with full tenant isolation; manage 50+ client tenants from a single console.
- **Commercial Flexibility** — Per-tenant policy, reporting, and billing; white-label and co-branding options.

- **Scale Deployment** — Rapid rollout at scale across thousands of endpoints with central agent deployment.

8. Complete Feature Matrix

The matrix below consolidates the full endpoint feature set of Seceon aiXDR-PMax.

S. No.	Feature	EPP	EDR
1	Signature + ML static + sandbox anti-malware (viruses, trojans, ransomware, spyware, cryptominers)	✓	
2	Ransomware hostname & behavior protection	✓	✓
3	Malicious web download blocking	✓	
4	Exploit protection (process, DLL injection/sideloading, network)	✓	
5	Blacklisted & exploit IP blocking; DGA hostname detection	✓	
6	Zero-day malware protection via anomaly & correlation	✓	✓
7	Mimikatz / credential-dump detection & blocking	✓	✓
8	Block unsigned/unknown binaries; aggressive mode	✓	
9	Quick & full scans (≤5% CPU); Defender replacement	✓	
10	Offline / air-gapped protection	✓	✓

S. No.	Feature	EPP	EDR
11	Tamper protection (alert & block on disable attempts)	✓	
12	Real-time user alerts & dedicated desktop interface	✓	
13	Process, file, registry, script, network & service telemetry		✓
14	Runtime detection: fileless, macros, PowerShell, WMI		✓
15	Lateral movement detection (SMB relay, pass-the-hash) + deception		✓
16	DNS/ICMP tunneling exfiltration detection		✓
17	Live Query — live forensic analysis on endpoint		✓
18	Cross-organization queries across all endpoints		✓
19	Online/offline endpoint tracking (Windows, Linux, macOS)		✓
20	Browser extension monitoring		✓
21	Unauthorized program, driver, or service detection		✓
22	Isolate endpoint, kill process, quarantine file (SHA-256 logged)		✓
23	Targeted actions: reboot, shutdown, connect/disconnect network		✓

S. No.	Feature	EPP	EDR
24	Playbook-driven automated response (<90 seconds)		✓
25	File Integrity Monitoring (Windows, AD/GPO, Unix, Linux)	✓	✓
26	Vulnerability assessment on endpoints		✓
27	Device control & USB DLP (encrypted USB exceptions)	✓	
28	PII/PHI discovery, monitoring & custom patterns	✓	✓
29	OS-level log collection & compliance reporting		✓
30	Endpoint data retention up to 7 years (compressed)		✓
31	MITRE ATT&CK TTP mapping & threat hunting		✓
32	Automated risk scoring of all protected objects	✓	✓
33	Multi-tenant with logical data & analytics separation	✓	✓

9. Why Seceon for EDR & EPP

9.1 Differentiators

- **One Agent, Six Products** — EDR, EPP, DLP, FIM, device control, and vulnerability assessment in one agent and one license, no point-product stack to integrate.
- **Featherlight Footprint** — Under 2–3% CPU and under 100 MB RAM at runtime, robust protection without compromising user experience or device speed.
- **Native SIEM/XDR Correlation** — Endpoint telemetry natively correlated with network, cloud, and identity by aiSIEM — full attack-chain visibility that standalone EDRs cannot provide.
- **AI/ML + Signatures** — No signature purchase required; 12M+ signatures plus AI/ML behavioral detection for zero-day and LotL attacks.
- **Machine-Speed Response** — Sub-90-second automated containment through built-in SOAR — no separate SOAR license.
- **Built for MSSPs** — Multi-tenant by design with white-labeling; asset-based licensing with no per-event or ingestion tax.
- **Air-Gap Ready** — Full protection for offline and air-gapped endpoints — detection does not depend on cloud connectivity.

9.2 Cost Consolidation

In Seceon's annualized stack comparison, a best-of-breed approach prices a standalone endpoint protection suite at roughly $120K/year and a separate DLP solution at $40K/year, both of which are included in the Seceon platform. Combined with SIEM, SOAR, TI, and UEBA consolidation, the unified platform roughly halves the total cost of ownership versus a multi-vendor stack.

9.3 Getting Started

aiXDR-PMax deploys in days, not months. Agents roll out centrally across thousands of endpoints, connectors onboard existing tools, and detection begins immediately with pre-built rules and ML baselines.