Seceon aiXDR-PMAX

Seceon aiXDR-PMAX takes a holistic approach to cybersecurity by gathering deep insights from endpoints, servers, clouds, network devices, applications, IoT, and OT and applying user identity, threat intelligence, and vulnerability assessment to establish threat profiles, generate threat indicators, raise essential alerts, and offer remediation path–automated or triaged. In essence, the solution ensures multi-layered threat detection and response, relying on EDR, Network Behavior, Advanced Correlation (SIEM), Network Traffic Analysis, UEBA (ML-based), and SOAR for an All-In-One platform that is organically and seamlessly fused together.

- Endpoint Security with agent-based and agentless technology for Windows, macOS, and Linux OS
- Behavior baselining with applied Machine Learning for users and entities based on host-centric insights (services, processes, file access, telemetry, etc) and network flows
- Data Exfiltration (breach), Insider Threat, and DDoS Attack detection with network traffic pattern analysis
- Exhaustive reporting across several key areas - security, compliance, operations, and investigation.
- Rules-based policy creation, enforcement, and notification for appropriate action and governance.

Advanced Security for Endpoints and Networks
Block brute-force attacks on endpoints leading to compromised credentials, VPN, early detection of malware and ransomware, network based attacks, and ultimately protect your users, data, applications, infrastructure and systems

Real-time AI/ML Based Detection and Response
Benefit from security automation through Machine Learning for anomaly detection and Artificial Intelligence for Dynamic Threat Modeling (DTM) as accurate risks are quantified based on threat indicators. Stop threats and limit blast zones before they turn into major incidents.

Instant 24/7 Response
Enable instant responses to governance policy violations through user-defined controls and initiate automated remediation to threats with high severity and confidence levels, targeted at business-critical assets.

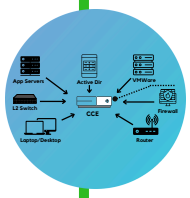
MITRE ATT&CK Modelling
Leverage MITRE ATT&CK Tactics, Techniques, and Procedures to model actual intrusions and attacks, focusing on kill chain activities such as reconnaissance, beaconing, evasion, privilege escalation, lateral movement, and exfiltration.

Single Pane of Glass
Rest assured with total protection against cyber security threats, exploits, and attacks across your servers, endpoints, and applications in the Cloud, On-Premise, Edge (IIoT & IT-OT), and Remote Workplaces.

Complete Attack Surface Visualization
Monitor your IT assets 24x7 with full details of behavioral attributes, prioritized statistics, performance indicators, drill-down data points and consolidated reports – visual and tabular – ensuring rapid attack/breach detection, regulatory compliance, threat hunting, operational oversight, and executive summary

Sample Threat Types & Use Cases Addressed by Seceon aiXDR-PMAX

Remote Workplace



On Prem/Data Centre

- Early Malware & Ransomware Detection and Protection
- Insider Threats
- Data Breach (Exfiltration)
- DDoS Attacks
- Web Exploits
- Brute-Force Attacks
- Vulnerability Exploits
- IoT-IIoT Security
- DNS Protection
- Endpoint Isolation
- Threat Containment
- Data Loss Prevention
- Deep Threat Hunting
- File Integrity Monitoring
- MITRE ATT&CK TTPs
- Policy Enforcement (Network, Database, Internet etc)

Extended Coverage with Seceon aiXDR-PMAX

Amazon/AWS

➤ CloudWatch, CloudTrail, S3, RDS

Microsoft Azure Environments

➤ M365, OneDrive, SharePoint, Network Watcher, Azure AD, NSG, Government Cloud, Cloud App Security

Google Cloud

➤ Google Workspace, StackDriver Flow Logs, Pub/Sub APIs

Other Cloud (IaaS / SaaS)

➤ Oracle Cloud, Service Now, Slack, others

Endpoints

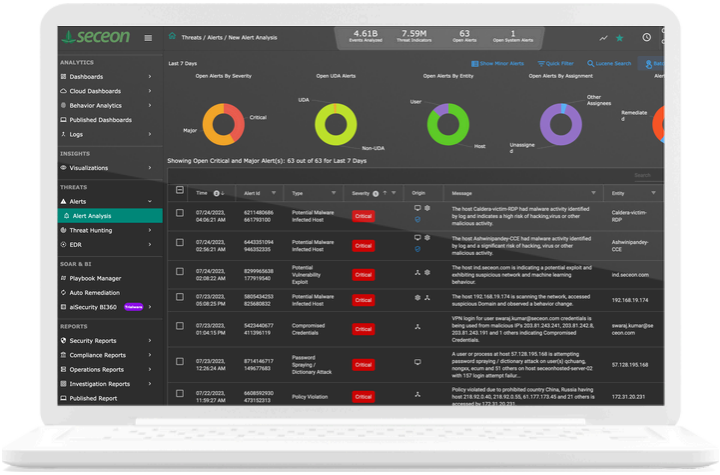
➤ Windows, macOS, Linux Desktop

On-Premise Infrastructure

➤ Servers: Windows, Linux, DNS, DHCP, FTP, SMTP

➤ Database: Oracle, MS-SQL, MySQL, Postgres

➤ Other: Network based Anomalies, 3rd Party Security Tools, Vulnerability Scanners, IoT-IIoT Devices, IT-OT Systems



Seceon Dashboard

PRODUCT FEATURES	aiSIEM	aiXDR	aiXDR-PMAX
Automated Threat Detection with Real-time Processing	✓	✓	✓
Automated and Semi-Automated Remediation	✓	✓	✓
Advanced Correlation with Contextual Enrichment	✓	✓	✓
Network Behavior Anomaly Detection and Network Traffic Analysis	✓	✓	✓
User Entity Behavior Analytics	✓	✓	✓
Visualization, Alerts, Notification and Incident Management	✓	✓	✓
Threat Hunting and MITRE ATT&CK Framework	✓	✓	✓
Log Collection, Retention and Forensics	✓	✓	✓
Administration and Provisioning	✓	✓	✓
Continuous Compliance, Audit and Reporting	✓	✓	✓
Multi-tenant, designed for isolation between clients or organizations	✓	✓	✓
aiXDR adds EDR + EPP			
• Gain deeper insights into processes, services, executables, and files with lightweight Pmax agents		✓	✓
• Protection from malicious web downloads and emails			✓
• Protection from exploits - process, dll, and network			✓
• Offline detection and Protection – Detection and protection without an internet connection			✓
• Application and device control			✓
• Removable media scanning and protection			✓
• Scanning Capability to protect from known malware (Quick and Full)			✓
• PII and PHI Discovery			✓
• Web / Content Filtering			✓
• Static Analysis of files			
• Track endpoints (Windows, Linux, and macOS) that are online versus offline		✓	✓
• Detect malware footprint with an advanced correlation of data gathered through pre-built rules running on an endpoint agent		✓	✓
• Contain threats by isolating affected endpoints, enforcing policy changes, stopping malicious processes and quarantining malicious files		✓	✓
• Enriched set of TI feeds with 8+ million malicious hash files		✓	✓
• FIM - File Integrity Module		✓	✓
• Vulnerability assessment on endpoints		✓	✓
• Browser extension monitoring		✓	✓
• Targeted Action and Response (Reboot, Shutdown, Connect/Disconnect from/to Network)		✓	✓
• Live Query - Live forensic analysis on endpoint		✓	✓

• Compliance - Collect OS-level logs	✓	✓
• Detect & protect unauthorized - programs, drivers, or services	✓	✓
• Real time threat detection and protection notification		✓
• Multi-tenant by design with logical separation of data, analytics, ML, and AI rule-set	✓	✓

About Seceon

Seceon enables MSPs, MSSPs, and IT teams to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon augments and automates MSP, MSSP, and IT security services with an AI and ML-powered aiSIEM and aiXDR platform. It delivers gapless coverage by collecting telemetry from logs, identity management, networks, endpoints, clouds, and applications. It's all enriched and analyzed in real-time with threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 640 partners are reselling and/or running high-margin, efficient security services with automated cyber threat remediation and continuous compliance for over 8,800 clients.

Learn more about Seceon aiXDR-PMax and

Schedule a Demo www.seceon.com/contact-us/