2025

seceon

Why Seceon's Platform is the Best for Tackling Sophisticated Cyber Threats vs. Best-of-Breed Security Products?

Table Of Content

Introduction:

The evolving cyber threat landscape, with sophisticated attacks such as APTs, zero-day exploits, ransomware, and insider threats, demands a proactive, AI-driven, and automated security approach. Traditional best-of-breed security products work in silos, making them ineffective against modern threats.

Seceon's AI-powered cybersecurity platform delivers a unified, automated, and intelligent defense with:

✅ AI-Driven Real-Time Threat Detection

✅ MITRE ATT&CK Framework-Based Analysis

✅ Automated SOAR-Based Remediation

✅ Full-Stack SIEM + XDR + Compliance in One Platform

✅ 850+ API, Log & Flow Integrations to Create a Cybersecurity Mesh

Did You Know?

Siloed security tools increase complexity, delay response times, and create higher costs for enterprises.

The Challenges with Best-of-Breed Security Products

Limitations of Traditional Security Products:

- Rely heavily on signatures and rule-based detection, making them ineffective against zero-day attacks.
- Lack of integration across SIEM, XDR, EDR, SOAR, and Compliance tools, leading to gaps in detection and response.
- Require manual correlation of alerts, causing alert fatigue and delayed incident response.
- Expensive due to multiple licenses, high ingestion costs, and complex management.

Why Seceon Outperforms Best-of-Breed Security Products

Problem with Best-of-Breed Security Stacks:

- Enterprises use multiple disconnected security tools:

1. SIEM (Splunk, QRadar, Sentinel)
2. EDR (CrowdStrike, SentinelOne, Defender)
3. SOAR (Cortex XSOAR, ServiceNow SecOps)
4. Cloud Security (Palo Alto Prisma, AWS Security Hub)

- These tools don't communicate efficiently, creating gaps in threat detection and response.
- Security teams waste time correlating alerts manually, leading to alert fatigue and delayed incident response.

Did You Know?

Automating threat response can reduce security team workload by up to 80%.

AI-Powered Real-Time Threat Detection vs. Traditional Signature-Based Security

Problem with Best-of-Breed Tools:

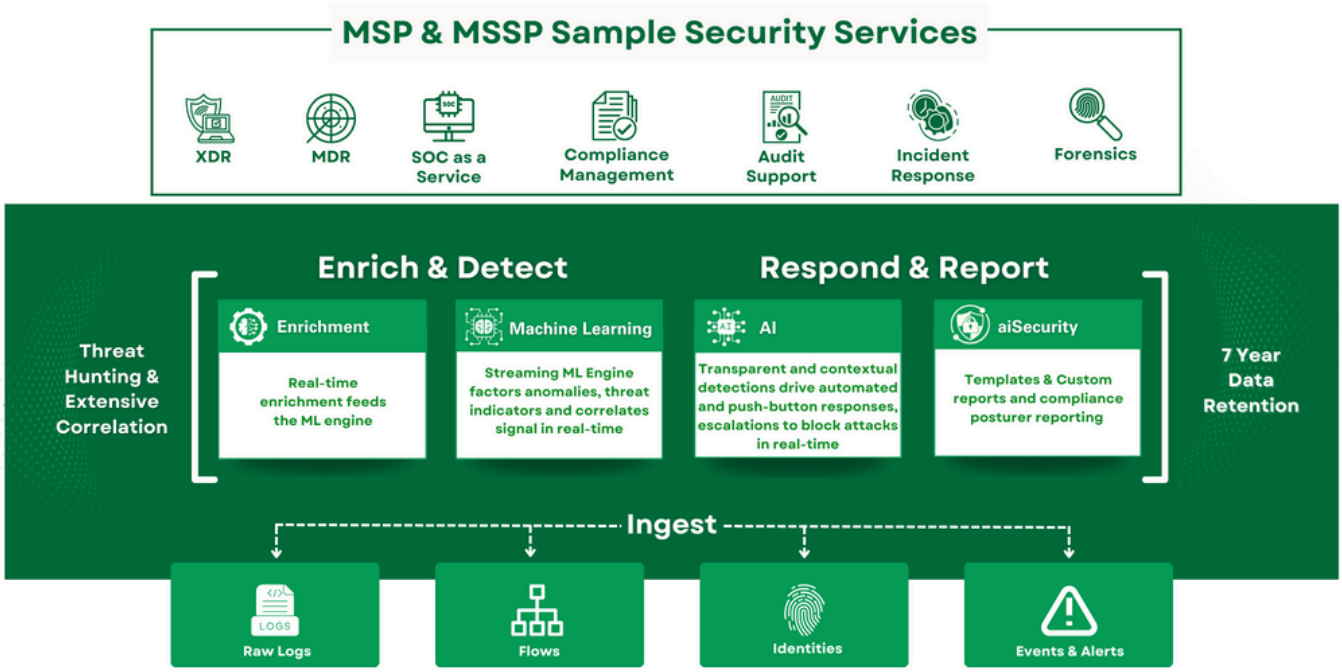
- SIEMs (Splunk, QRadar) and EDRs (SentinelOne, CrowdStrike) rely on signatures and rule-based detection, missing zero-day threats.
- They detect threats only after indicators of compromise (IoCs) are known.

Seceon's Advantage:

✅ **AI/ML-Based Threat Detection** – Uses behavioral analysis and anomaly detection for proactive defense.

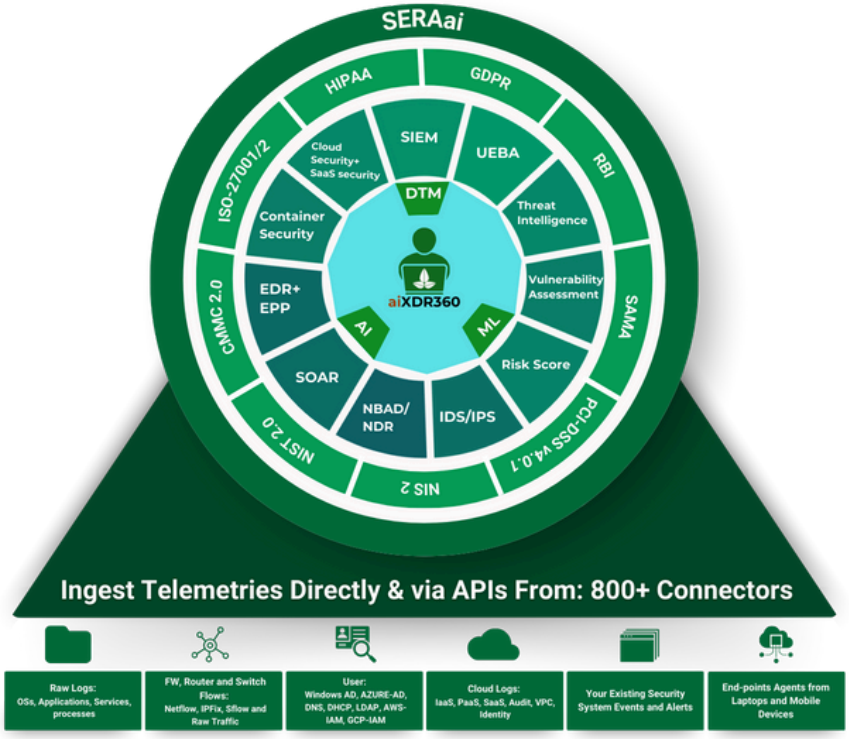
✅ **Prevents Attacks Before Damage Occurs** – Detects threats early in the MITRE ATT&CK framework, stopping lateral movement.

✅ **Stops Zero-Day & APT Attacks** – Learns from evolving attack patterns dynamically.



Quick Fact:

AI-driven security reduces dwell time for threats from 200+ days to minutes.



Unified Security Approach (SIEM + XDR + SOAR) vs. Siloed Security Tools

Problem with Best-of-Breed Security Stacks:

- Organizations use multiple disconnected security tools, creating visibility and response gaps.
- Security teams waste time correlating alerts manually, leading to alert fatigue and delayed incident response.

Seceon's Advantage:

✅ Fully Integrated SIEM + XDR + SOAR – No need for separate security tools.

✅ 850+ API, Log & Flow Integrations – Creates a cybersecurity mesh across cloud, network, endpoints, identities, and applications.

✅ SOAR-Driven Auto Remediation – Isolates threats, block malicious IPs, and revokes access automatically.

Misconfigurations: The Silent Threat

Simple missteps like open ports or default credentials can expose you—continuous assessment uncovers hidden weaknesses before attackers do.

Faster Detection & Response vs. Traditional SIEMs & XDRs

Problem with Best-of-Breed Solutions:

- Traditional SIEMs require manual rule writing and tuning.
- The dwell time for threats is often 200+ days before detection.
- XDRs focus only on endpoint threats, lacking network & cloud-wide visibility.

Seceon's Advantage:

✅ AI-Based Auto Detection Without Manual Rules – Reduces dwell time from months to minutes.

✅ Detects & Responds in Real-Time – AI-driven risk scoring prioritizes critical threats instantly.

✅ Covers Endpoints, Networks, Cloud & Identities – Full-spectrum threat coverage.

Seceon's Unified AI-Driven Security Approach

How Seceon Outperforms Best-of-Breed Solutions:

- AI/ML-Based Threat Detection: Uses behavioral analytics to detect threats before damage occurs.
- Unified SIEM + XDR + SOAR Approach: Eliminates the need for multiple security tools.
- End-to-End Visibility: Covers endpoints, networks, cloud, and identities, unlike EDR/XDR-focused solutions.
- Automated Threat Remediation: AI-driven SOAR isolates threats, blocks malicious IPs, and revokes access automatically.

Compliance and Continuous Monitoring

Seceon simplifies security compliance by:

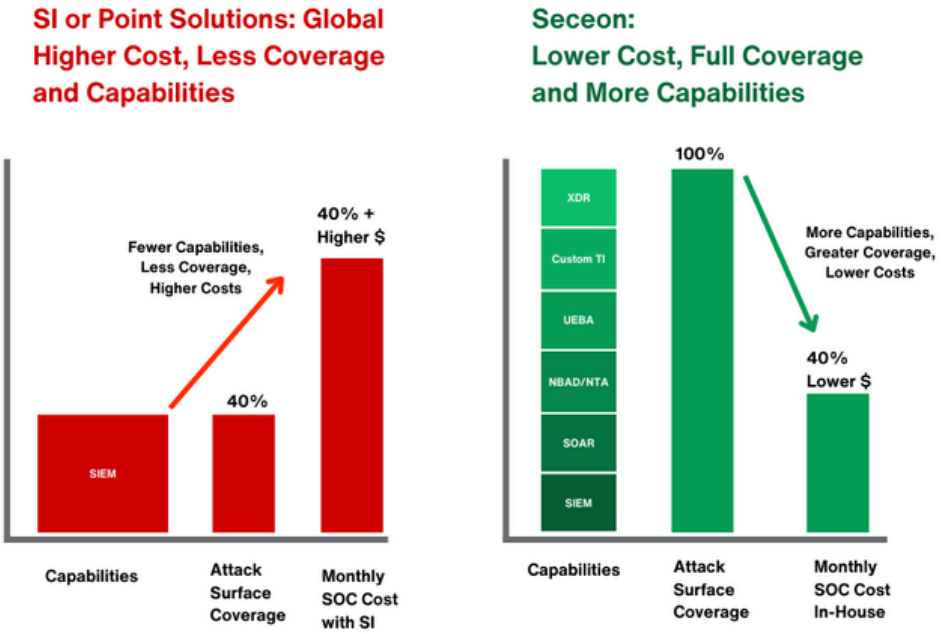
✓ Offering pre-configured compliance reports for major frameworks.

✓ Continuous risk monitoring with real-time security posture updates.

✓ Automated compliance checks to streamline audits and reduce manual efforts.

Important Note:

Compliance is no longer just a requirement—it's a necessity for risk reduction.



Cost-Effective Security for Organizations

- **Flat Pricing Model** – Unlike Splunk & QRadar, Seceon does not charge based on log volume.
- **All-in-One Platform** – SIEM + XDR + SOAR + Compliance = No need for multiple tools.
- **Lower Operational Costs** – AI-driven automation reduces the burden on security teams.

Conclusion:

Traditional best-of-breed security stacks rely on disconnected tools, leading to inefficiencies. Seceon's unified AI-driven approach provides:

✓ Proactive threat detection with AI-driven analytics.

✓ Automated threat response with built-in SOAR capabilities.

✓ Lower cybersecurity costs by eliminating multiple security tools.

✓ Seamless compliance readiness with continuous risk monitoring.

Further Reading:

Seceon Resources:

Read our Buyer's Guide to SIEM platforms and learn how to determine how AI/ML should be a part of your selection criteria (SIEM Buyer's Guide).

Seceon Blog:

Read how Seceon is Transforming Cybersecurity: Why Partners Trust the Seceon Platform

https://www.seceon.com/msp-vs-mssp-is-there-a-distinction-anymoreread-the-blog/

About the Authors

Sunday McDickson

CEO, SMSAM Systems Ltd.

As CEO at SMSAM, Sunday McDickson brings over a decade of leadership experience in cybersecurity. With a focus on innovation and strategic growth, he has led numerous initiatives that help organizations navigate complex security challenges and adopt scalable, forward-thinking solutions.

Kriti Tripathi

Designer & Technical Marketing Executive, Seceon Inc.

As a Designer and Technical Marketing Executive at Seceon, Kriti plays a pivotal role in bridging the gap between technical expertise and clear communication. She contributes her creativity and knowledge to produce compelling marketing materials that help convey Seceon's advanced cybersecurity solutions in a user-friendly and engaging manner.

Tom Ertel

SVP Technical Sales & Strategic Accounts, Seceon Inc.

With over 30 years of experience, Tom helps organizations protect their networks from evolving cyber threats using Seceon's OTM platform. He brings leadership in technical sales and strategic account management for key customers globally.