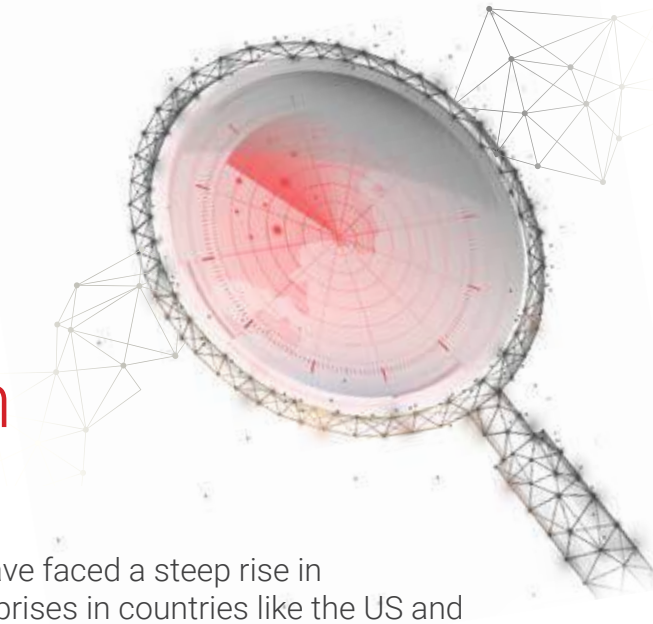
Seqrite **XDR**

SEQRITE

www.seqrite.com

Empower your enterprise with Seqrite XDR and SIA—your Gen AI-powered analyst for faster threat detection, smarter investigations, and automated remediation across all data sources.



Today's Attacks Are Smarter & Faster. Is Your Security Team Keeping Up?

Over the past few years, organizations worldwide have faced a steep rise in sophisticated cyberattacks, with nearly half of enterprises in countries like the US and India impacted. These attacks are evolving—faster, stealthier, and harder to detect.

According to threat research, most modern breaches fall into two high-risk categories:

1. **Evasive malware and Zero-day attacks**
2. **File-less attacks and targeted attacks**

The latter, in particular, are among the most destructive. They don't leave behind traditional malware footprints and often require historical context, behavioral analysis, and deep correlation to uncover. Unfortunately, most cybersecurity teams lack the unified visibility or intelligent tooling required to connect the dots.

Security operations centers (SOCs) are increasingly overwhelmed, facing an unmanageable volume of alerts, siloed systems that don't communicate, and a growing reliance on a few highly skilled analysts. Manual investigation workflows slow down response times, increase burnout, and leave gaps in protection.

With attackers exploiting speed and scale, the gap between detection and response continues to widen, highlighting the urgent need for smarter, faster, and more connected security operations.

The Solution: Seqrite XDR

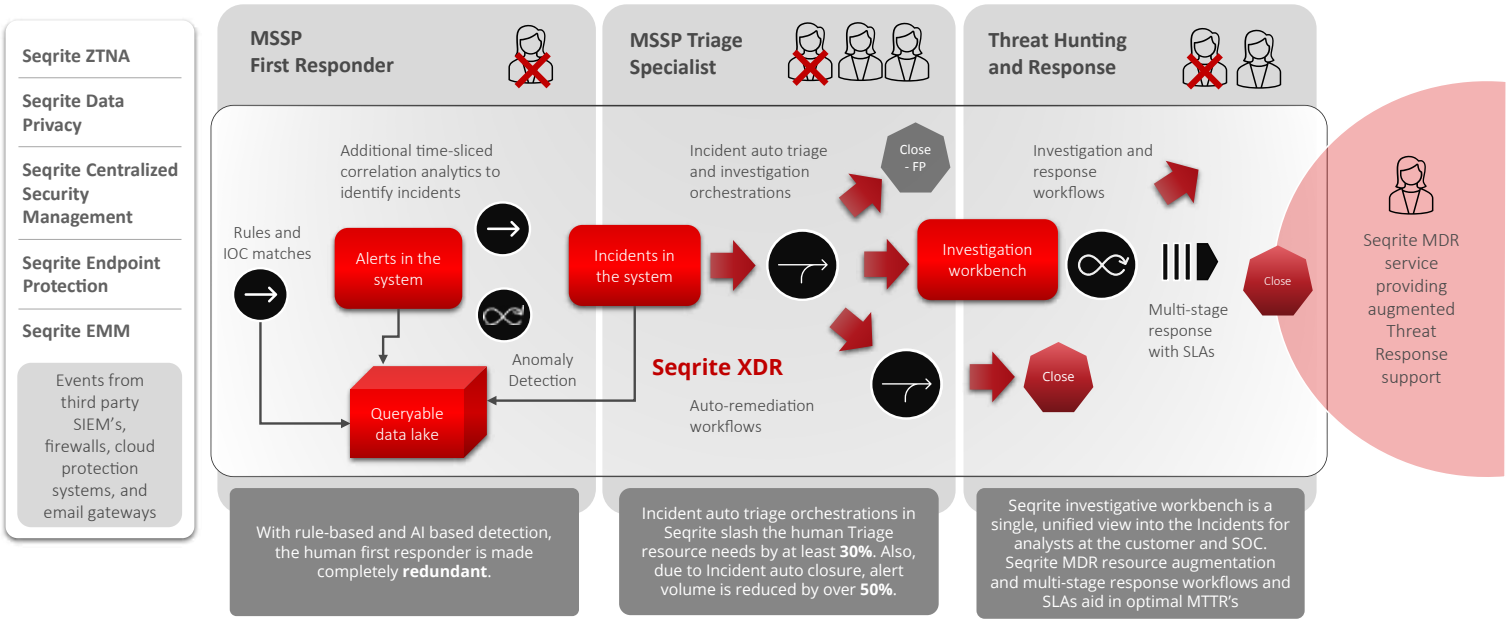
Extended Detection and Response with Built-In Gen-AI Asisstant

Seqrite XDR delivers the power of unified detection and response—supercharged by AI. Get full-spectrum visibility across endpoints, networks, and servers, with real-time threat correlation and automated defense.

At the core is SIA (Seqrite Intelligent Assistant)—an AI-driven virtual security analyst that transforms security operations with natural language interaction, instant insights, and intelligent triage. Analysts resolve threats faster, reduce noise, and act decisively—without switching tools.

Built for agility and scale, Seqrite XDR with SIA helps you build a high-performance, hybrid SOC—faster response, lower cost, stronger protection.

How our unified platform enables the MSSP to perform Managed Detection and Response with 50% resource reduction.



Product Highlights

Gen AI-Powered: Seqrite XDR is enhanced by the Gen AI Virtual Security Analyst, SIA, which provides smart incident insights, predefined prompts, and seamless threat investigations.

Convenient: A single, holistic platform for advanced threat detection, investigation, and response—streamlined through SIA's intuitive query handling and contextual awareness.

Precise: Focused, source-specific logic minimizes false positives. SIA provides context-aware insights, helping analysts quickly verify and prioritize incidents.

Next-gen: Comes with enhanced properties like SOAR automation for Triage and Response, threat hunting workbench, IOC search and kill, and many more.

Multi-level Protection: ML/AI for 24/7 awake vigilance. Behaviour Anomaly detection for additional protection against unknown threats. Automated Incident correlation and enrichment for severity assignment.

Response Management: Ensures optimal response times through Incident Management, SLA management, and detailed SOC Dashboards.

Playbook-based Automation : Warrants optimized resource utilization through automation.

Shared Threat Intelligence: Lets the customer source global threat intelligence and Seqrite's in-house research-generated intelligence to tackle zero days and advanced persistent threats.

Historical Data Search: Enables IOC lookup across past data. SIA allows analysts to surface historical context in seconds through simple queries.

Support: Seqrite MDR team available for response assistance and SOC resource augmentation.

Product Highlights

Automated Incident Correlation: Automatically enriches and correlates alerts for severity-based prioritization. SIA assists by surfacing key details instantly and recommending next step

Real-Time Behavioral Analytics: Continuously monitors user activity to detect unusual logins, such as impossible travel or unexpected locations, for instant threat identification.

AI-Powered Anomaly Detection: Leverages machine learning to identify abnormal activities like logins from non-compliant devices or single-factor authentication attempts.

Insider Threat Alerts: Provides real-time notifications on potential account compromises caused by risky or unusual user behavior.

Integrated Data Insights: Correlates user anomalies with endpoint and network data to accelerate incident response and reduce downtime.

Reduced Alert Fatigue: Focuses on high-risk activities, minimizing false positives to streamline security operations.

Why Choose Seqrite XDR?

01 **Active Vigilance with SIA**: Utilizes ML, behavioral anomaly detection, and automated searches, enhanced by SIA's real-time insights and auto-triggered remediation for round-the-clock threat defense.

02 **Years of expertise in cybersecurity** : Leader in the endpoint protection space for over 20 years, secured four million+ endpoints, and has an in-house research lab providing up-to-the-minute IOCs and rules for locally and regionally active threat actors.

03 **Focus on process orientation** : Tackling threats across the enterprise, attack vectors and sources require single-minded process orientation. Seqrite XDR provides comprehensive incident management and SLA definition capabilities for procedure orientation of the SOC.

04 **Affordable price point** : Seqrite has developed highly optimized storage algorithms that enable upto 180 days events and alert storage at a fraction of the cost of competitive offerings in the market.

05 **Advanced User Behavior Analytics (UBA)** : Leverages machine learning and behavioral modeling to detect sophisticated threats, such as compromised credentials and insider attacks, that traditional tools often miss.

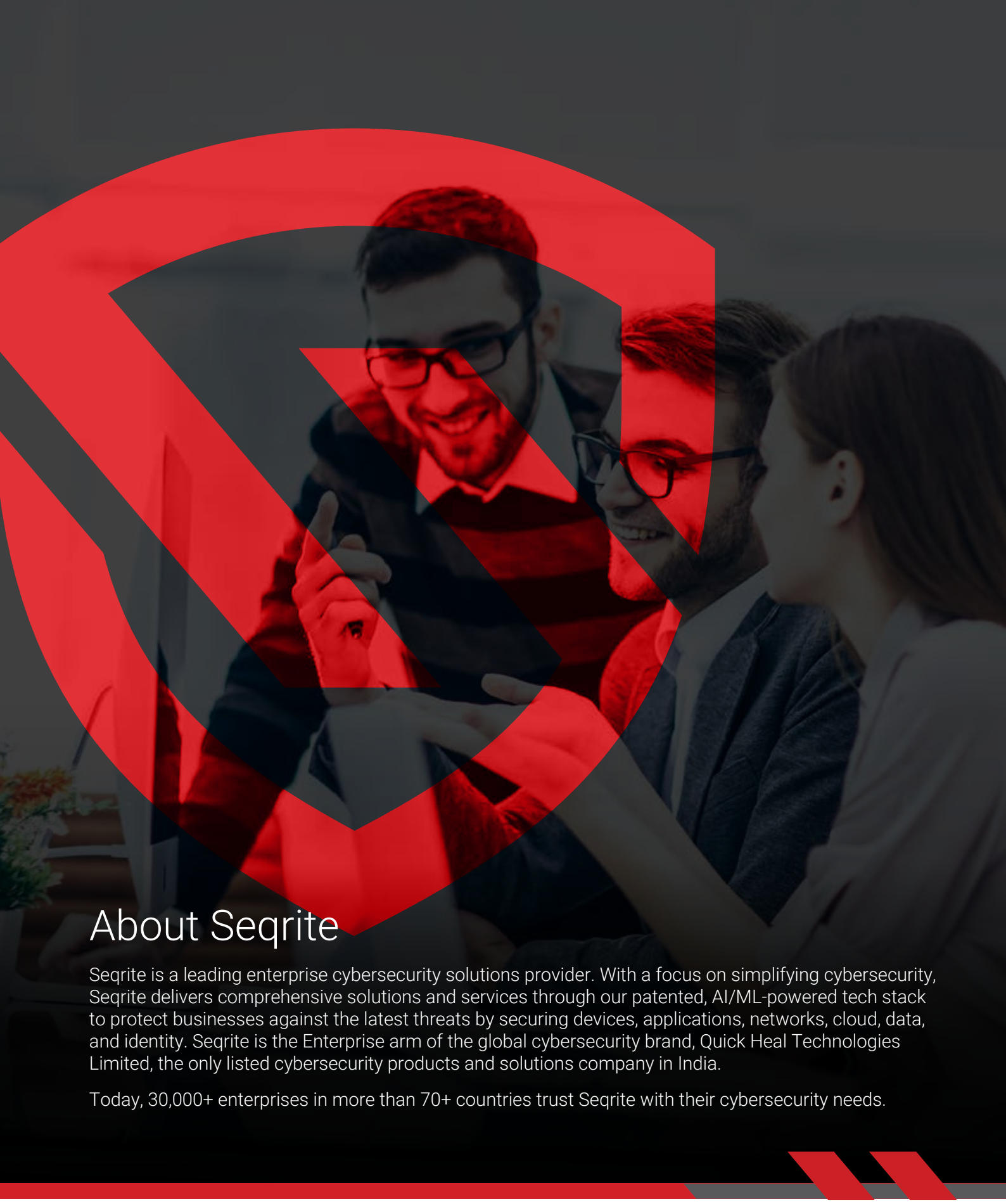
06 **Enhanced Security Visibility**: Combines endpoint, network, and user data to provide comprehensive insights, allowing you to respond to complex attacks with precision.

07 **Stay Ahead of Sophisticated Threats**: Detect, analyse, and neutralize advanced risks overlooked by conventional tools with cutting-edge UBA capabilities.

Automation and ML for **24/7** lookout for APTs

Historical IOC search: **30** days default; extendable to **180** with add-on.

Incident and SLA Management at 50% resource reduction



About Seqrite

Seqrite is a leading enterprise cybersecurity solutions provider. With a focus on simplifying cybersecurity, Seqrite delivers comprehensive solutions and services through our patented, AI/ML-powered tech stack to protect businesses against the latest threats by securing devices, applications, networks, cloud, data, and identity. Seqrite is the Enterprise arm of the global cybersecurity brand, Quick Heal Technologies Limited, the only listed cybersecurity products and solutions company in India.

Today, 30,000+ enterprises in more than 70+ countries trust Seqrite with their cybersecurity needs.

SEQRITE | Quick Heal Technologies Limited
Phone: 1800-212-7377 | info@seqrite.com | www.seqrite.com | /seqrite