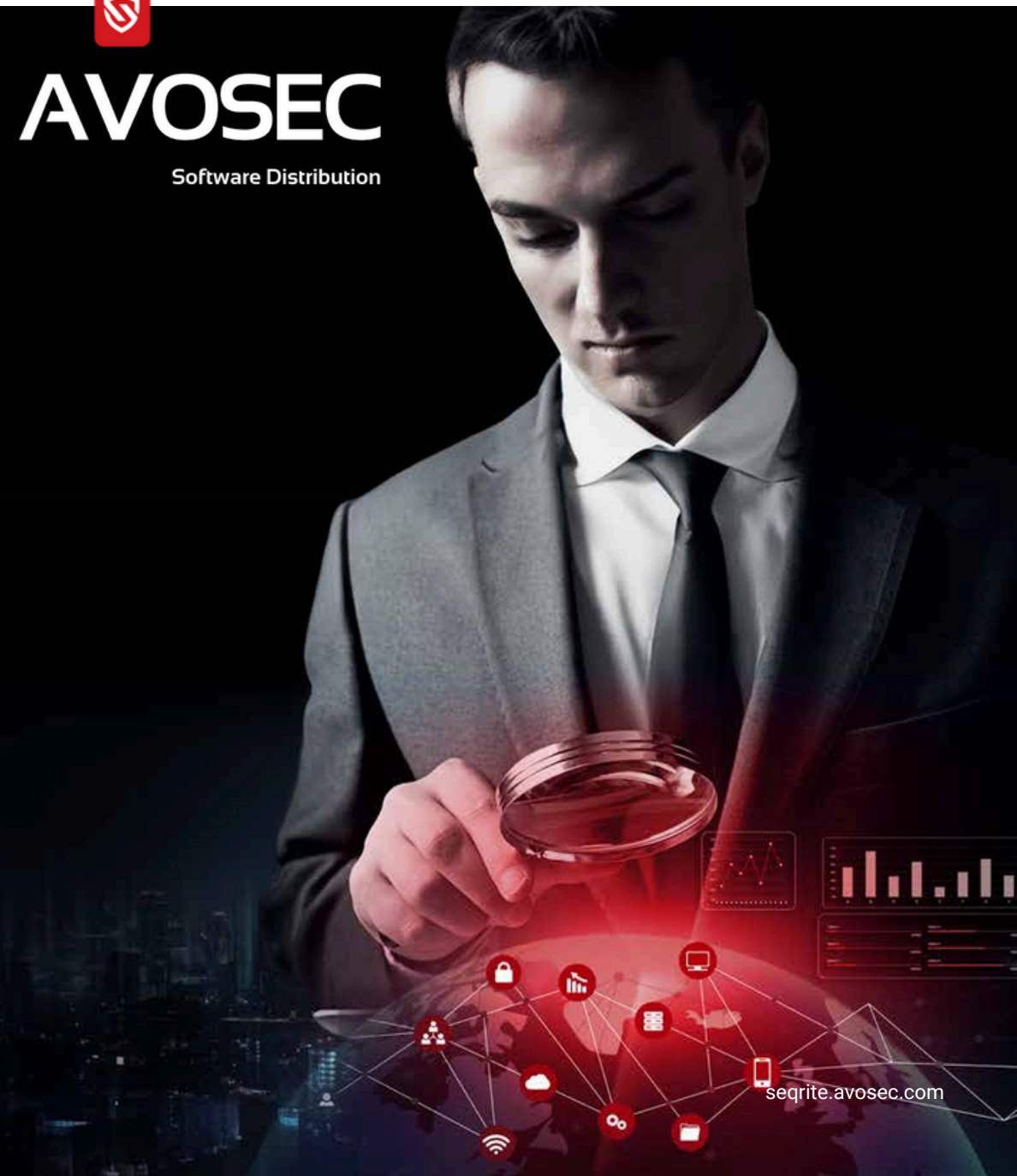
SeqriteXDR

SEQRITE



Bring holistic cyber protection to your enterprise using Seqrite XDR's automated threat hunting and remediation to identify, track, and eliminate stealthy threats across all data sources.

Cyber threats are getting smarter. Is your enterprise equipped to defend them?

Over the past few years, there has been a tremendous influx in advanced cyberattacks affecting nearly 47% and 27% of organizations (small, medium, and big) in the US and India. The trend shows no sign of slowing down as high-profile breaches are making regular headlines globally.

As per a study by Seqrite's data scientists, the attacks are majorly categorized into two sections:

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

The latter two are the hardest to detect and the most destructive as they require historical analysis and correlation, along with machine learning techniques to be identified. Cybersecurity teams are aware of such targeted attacks but didn't have a simple yet powerful tool that could caution them by providing visibility across all data sources.

Basic Endpoint protection is insufficient to detect the most elusive malware and targeted attacks. Advanced detection and response mechanisms, strengthened with behaviour anomaly detection and historical events search, are necessary to combat them. In addition, you would need advanced automation mechanisms, as the volume of generated alerts can overwhelm the SOC team.

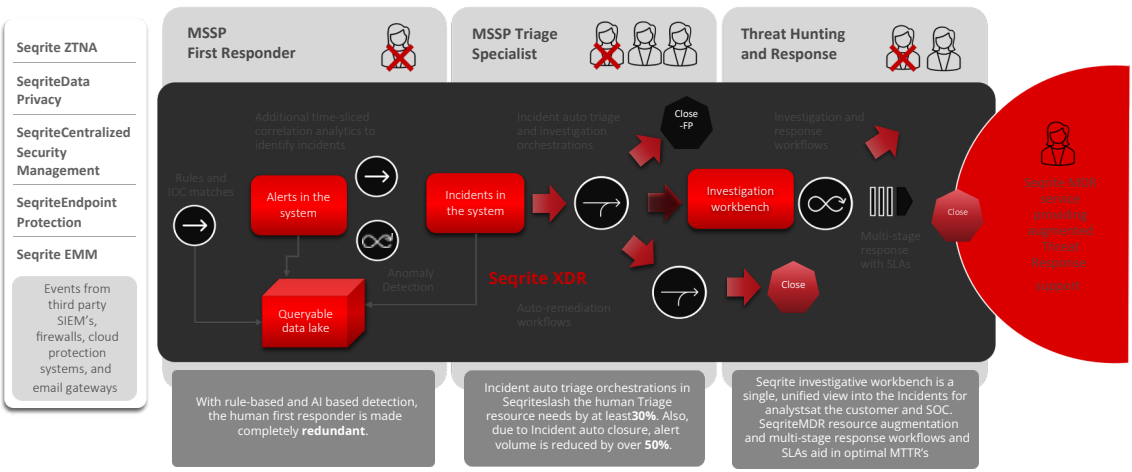
The Solution:
Seqrite XDR

An Extended Detection and Response Platform that enables a secure, hybrid SOC at a relatively lower price-point

Seqrite XDR is an advanced incident response tool that incorporates data from multiple security products into a unified security operations system to deliver holistic protection against cyberattacks. Using analytics and automation, It Seqrite XDR centralizes, normalizes, and correlates data from various sources, thus enabling real-time cross-control-point protection while simplifying and strengthening the security processes.

Seqrite XDR blocks cyber threats by detecting malicious encryption processes and shuts them down before they disrupt any network.

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



AVOSEC
Software Distribution

roduct Highlights

Convenient: A single, holistic platform for Advanced Threat Detection and Response.

Precise : Throws fewer false positives due to focused source-specific logic.

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: Allows IOC lookup for events that may have been missed earlier.

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

AVOSEC
Software Distribution

Why Choose Seqrite XDR?

01 Active vigilance : Emphasis on Machine Learning, Behavior Anomaly Detection, automated IOC/IOA search, auto triggered remediation workflows for superior 24/7 active vigilance for the organization.

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.

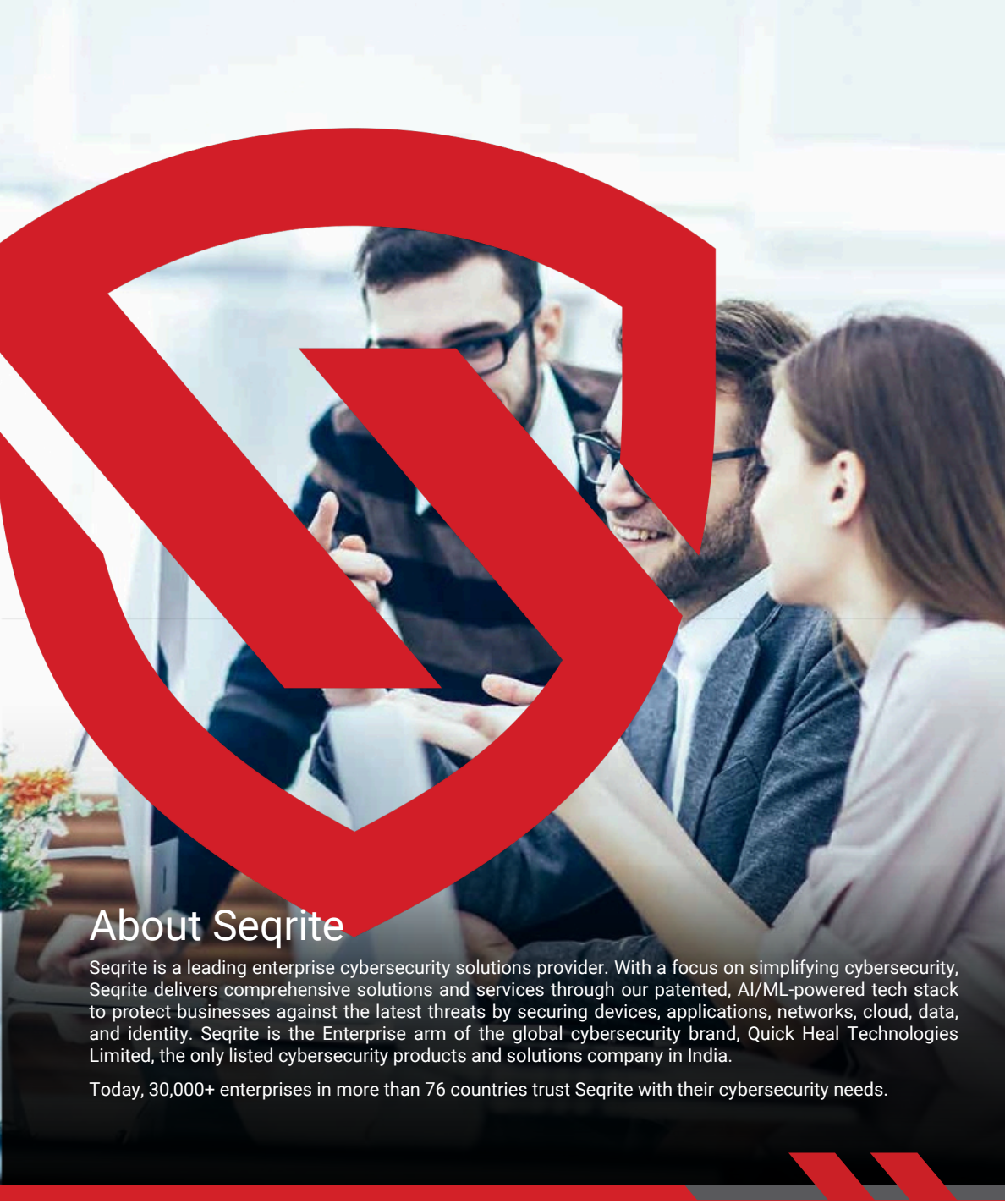
03 Focus on process orientation : Tackling threats across the enterprise, attack vectors and sources require single-minded process orientation. Seqrite XDR provides comprehensive incident management and SLA definition capabilities for procedure orientation of the SOC.

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.

Automation and ML for 24/7 lookout for APTs

Upto 180 days historical data search for missed IOCs

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 76 countries trust Seqrite with their cybersecurity needs.

SEQRITE | AVOSEC
Software Distribution

seqrite.avosec.com