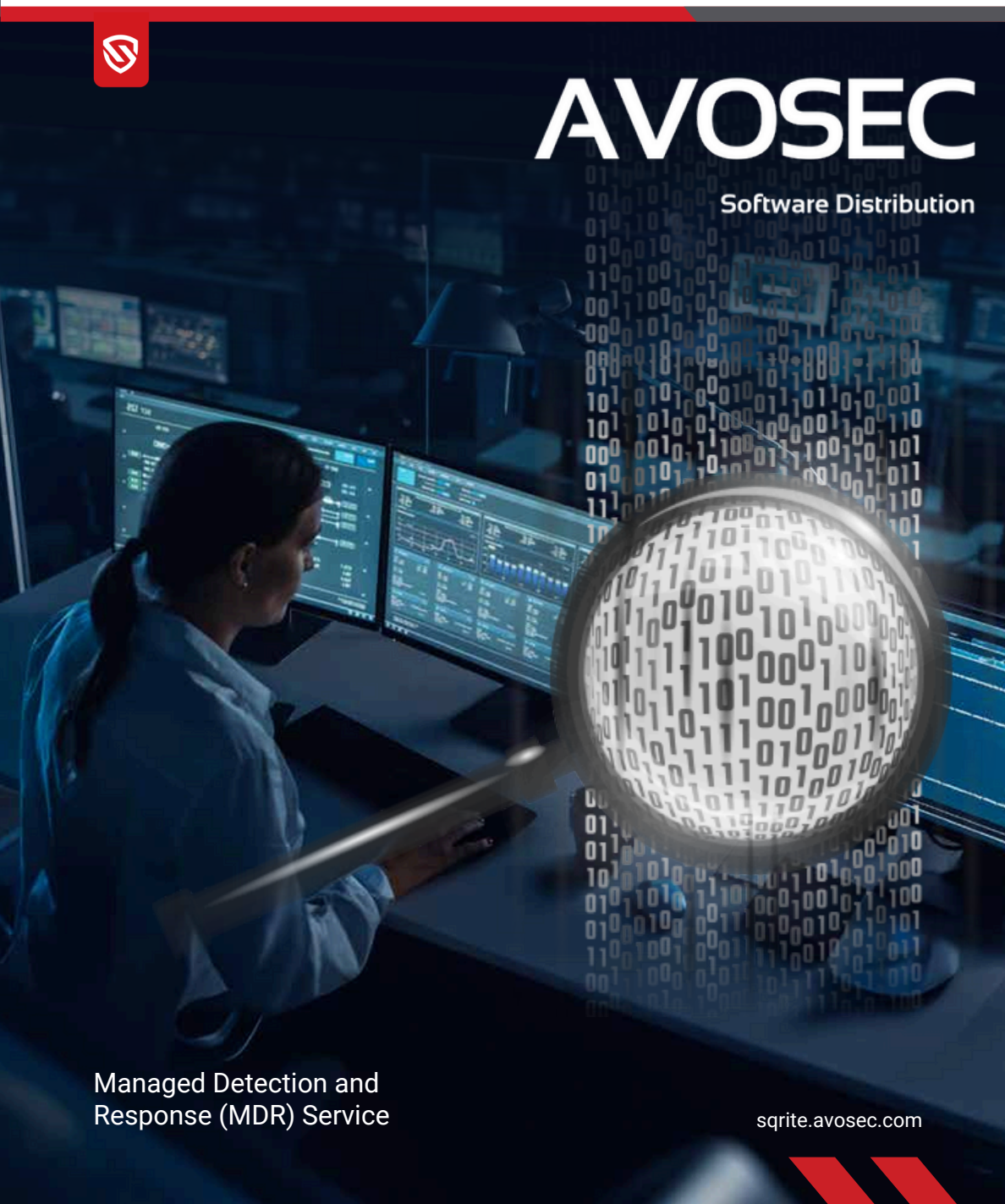
SeqriteMDR

SEQRITE



Managed Detection and
Response (MDR) Service

sqrite.avosec.com

Growing Cyberattack Landscape

Is your cyber defense system resilient enough?

As our world becomes increasingly digital, the threats are also growing in numbers and complexity. A new study reveals that over 300,000 new malware are created daily, while the average detection period of a cyberattack is 49 days. This means attackers are outsmarting the cyber defense teams and processes of most enterprises.

Organizations can face a range of impacts from advanced cyber-attacks, affecting them for months and sometimes years. The consequence may vary from monetary losses, damage to reputation and productivity, and legal disputes. In the worst-case scenarios, businesses may even perish for the reasons mentioned earlier. Hence, companies urgently need a team of skilled cybersecurity professionals armed with the latest attack Tactics and Techniques to defend themselves against advanced attackers. However, finding and retaining security experts with such skills is challenging due to the general shortage of experienced cybersecurity personnel worldwide.

Fortunately, Seqrite is here to help.

Unveiling
Seqrite MDR

Bringing Seqrite Labs
experts to care take your IT infrastructure.

Seqrite Labs has been researching the modus operandi of advanced threats, finding methods to contain them, and sharing threat intelligence with the world for many years. Now, we have also decided to utilize this expertise to take care of our customers' enterprises directly via the flagship Seqrite MDR service.

The MDR team has been carved out of the elite Seqrite Labs squad, which has access to the latest information about attacks happening worldwide. Introduced as an add-on to our very efficient Seqrite XDR, MDR analysts will help the customers' security team by performing alert monitoring, enrichment and triage, incident handling and remediation, and proactive threat hunting.

Seqrite MDR

Our customers' security is our top priority

Seqrite MDR is a comprehensive managed detection and response service, designed to help strengthen and augment our customers' security team.

Our MDR team works in multiple zones, and are always on the alert, tracking attackers and active threat campaigns in different industries and geographies.

It acts as an extended arm of the customers own Security Team.

The MDR team provides advisory service to help the customer respond to critical threats, and can even take containment and remediation actions on their behalf.

Core Attributes of Seqrite MDR

Incident Triage

- Investigates alerts and incidents on hosts regularly with endpoint telemetry, network traffic, & logs.
- Correlates alert attributes with Seqrite's Global Threat Intelligence to determine actual alerts and false positives.
- Performs Threat Hunting on historical data with the latest active Threat Indicators.
- Contains malware on individual endpoints identified during the activity and subsequently aids in remediating any malware identified and provides reports on all activity performed.

Emergency Response Services

- Aids the cyber security team by performing immediate end-to-end investigation, RCA, and remediation of endpoints for any critical, crippling, or breach incident reported by XDR or the customer.
- The MDR team follows all CSIRT procedures required by law for this purpose and follows strict SLAs in rendering the service.

General Service

- Updates detection and response automation workflows and rules with additional capabilities from time to time.
- Performs tuning of XDR for better detection, lower noise, and customized reporting and response suitable for the enterprise.
- Generates monthly reports on Threat activity & Response preparedness and performance; suggests training & improvement.

Benefits of Seqrite MDR

Avanced Technology

Powered by cutting-edge XDR technologies that leverage machine learning, behavioural analytics, and threat intelligence to detect and respond to threats in real time.

Proactive Monitoring

Our security experts proactively monitor your network, endpoints, and cloud environments, identifying and responding to threats before they can cause damage.

Tailored Services

We understand that every organization has unique security needs. That's why we work closely with you to customise our MDR services to your specific requirements, ensuring you get the most out of our solutions.

Compatibility

Seqrite MDR and Seqrite XDR services are compatible with your existing cybersecurity tools and solutions through our Connector technology. However, you can also choose the latest technology from our award-winning product portfolio for a seamless experience.

Security Simplified

With our MDR services, your security team can focus on your core proactive prevention needs while we care for your active detection and response activities. Our expert team manages and monitors your attack surfaces, freeing you up to concentrate on business as usual.

SLAs for the service

Standard Assistance Requests	For medium and high severity Incidents	6 hours from creation/updation time of Incident
Minor Assistance Requests	For low priority Incidents	24 hours from creation/updation of the Incident
Critical Assistance Requests	For Critical Incidents raised by Seqrite XDR or customer SOC	Engineer shall be made available within 30 mins of Request
Number of Standard Assistance requests that can be serviced in a calendar month	Beyond this, it will be on a best effort basis without any standard penalty	20
Number of Minor Assistance Requests that can be serviced in a calendar month	Beyond this number, it will be on a best effort basis without any standard penalty considerations	100
Number of Critical Assistance Requests that can be serviced in a calendar month	Beyond this number, it will be on a best effort basis without any standard penalty considerations	4

Backed by Seqrite Labs

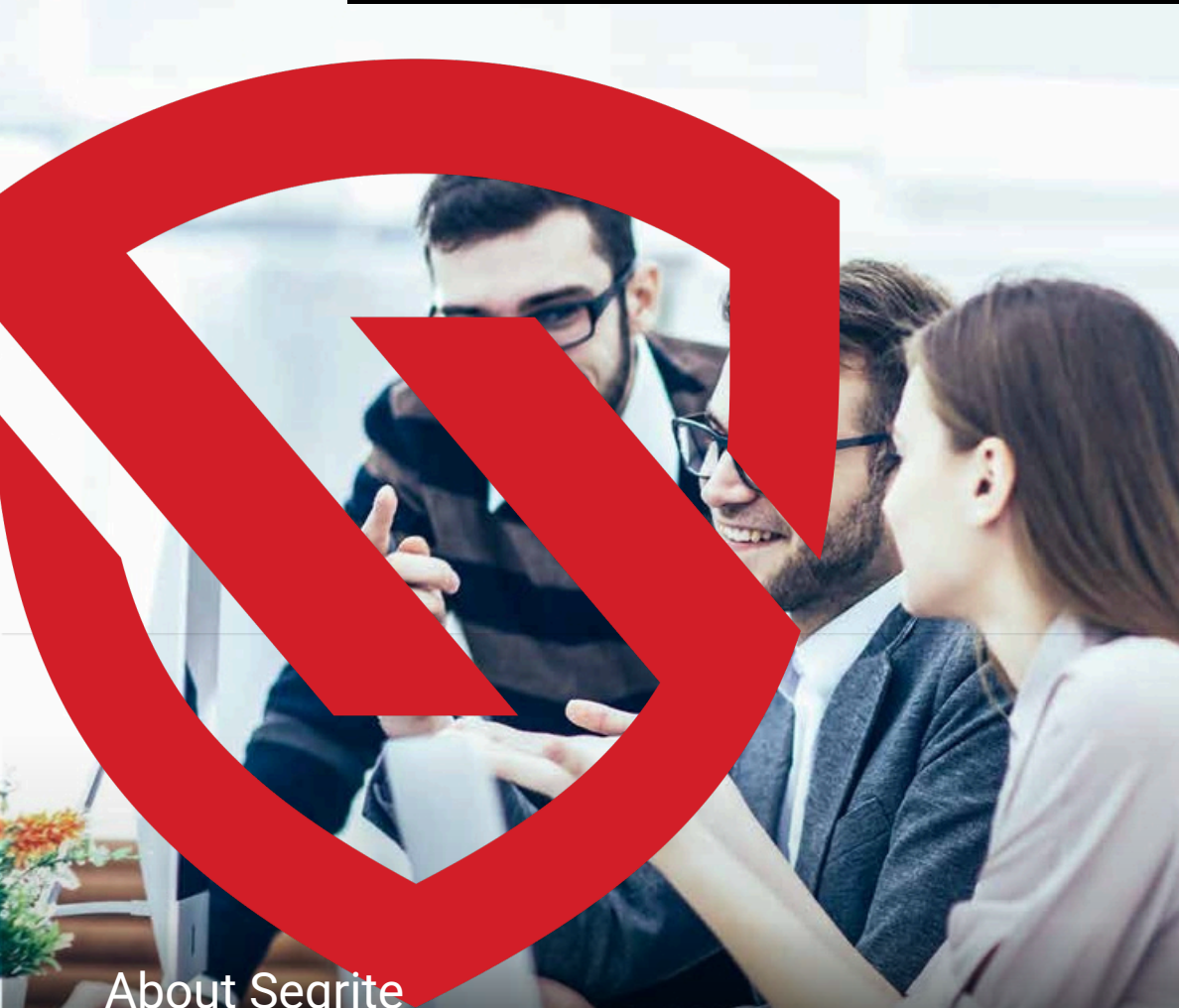
115+ member team

Total	Daily
2B Known Files	**1M** New Samples Processed
390M Classified & Categorized URLs	**500K** New Classification & Categories
100TB Size of Data Lake Used for ML training & Analytics	**500GB** New Security Telemetry

Platforms
- Windows
- Linux
- Macintosh
- Android/ iOS

Technologies
- Kernel Drivers
- Network Packet Inspection
- Big Data Mining
- Machine Learning

AVOSEC | CYBERSECURITY
ENDPOINT DEFENCE



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