iTVoice ISO 9001:2015 ®

IT IN DEPTH

IT VOICE INTERACTS: DR SANJAY KATKAR, QUICK HEAL TECHNOLOGIES

IT Voice held an interaction with Dr Sanjay Katkar, joint managing director, Quick Heal Technologies Limited

IT Voice : Can you provide more insight into how SEQRITE emerged as the enterprise arm of Quick Heal Technologies? What motivated the establishment of a dedicated division for cybersecurity solutions tailored to businesses and enterprises?

Sanjay : SEQRITE emerged as the enterprise arm of Quick Heal Technologies Limited in August 2015 in response to the growing need for specialized cybersecurity solutions for businesses and enterprises facing increasingly sophisticated threats. The motivation behind establishing this dedicated step was to harness Quick Heal's nearly three decades of cybersecurity expertise and the advanced technology stack to create tailored, robust solutions for enterprises of all sizes. SEQRITE's portfolio includes cutting-edge products and solutions such as Endpoint Security, Extended Detection and Response, and Zero Trust User Access. These offerings are the result of our highly skilled R&D professionals and the country's largest Malware Analysis lab known as the SEQRITE Labs. Today, our primary mission is to simplify and fortify cybersecurity for businesses while ensuring compliance with industry regulations.

IT Voice : Innovation and continuous improvement are emphasized in SEQRITE’s approach. Could you share some examples of how your team has demonstrated innovation in addressing evolving cybersecurity threats and challenges?

Sanjay : In the cybersecurity realm, SEQRITE has been at the forefront to innovate and develop future-ready solutions using cutting-edge technologies like AI and machine learning. We apply the Zero Trust model, offering cloud security solutions post-COVID-19, specialized IoT security, and automated threat response. Our Threat Intelligence capabilities through SEQRITE Labs ensures trust and integrity amongst our customers keeping them a step ahead of threats. We are the first and only Indian company to have collaborated with Govt. of USA on its NIST – NCCoE’s data classification project. Our dedicated team of cybersecurity experts are the first and only globally to have cracked Expiro. We have been able to patch 2 Zero Day vulnerabilities on WordPress. And, these are just very few to mention.

IT Voice : Cyber threats are constantly evolving. How does SEQRITE stay ahead of the curve to ensure that its solutions remain effective against the latest and most sophisticated threats?

Sanjay : SEQRITE employs a multifaceted approach to stay at the forefront of cybersecurity. Here’s how:

- Continuous R&D: With substantial investments in research and innovation, SEQRITE ensures it remains on the cutting edge of cybersecurity.
- Threat Intelligence: SEQRITE maintains a robust threat intelligence program, monitoring global threats and vulnerabilities in real-time.
- SEQRITE Labs: The dedicated Labs team conducts in-depth research and develops countermeasures against emerging threats.
- Incident Response: Our dedicated Incident Response Team swiftly mitigates emerging threats.
- Innovation: SEQRITE uses advanced technologies like AI, ML, and behavioral analysis to detect sophisticated threats.

These measures collectively ensure that SEQRITE’s cybersecurity solutions remain effective against the most sophisticated threats.

IT Voice : Building trust is vital in the cybersecurity industry. How does SEQRITE establish and maintain its reputation as a trusted provider of cybersecurity solutions? What strategies do you employ to assure clients of the effectiveness of your products and services?

Sanjay : What differentiates SEQRITE from its competition is our customer-centric approach fostering trust in through continuous innovation, multi-channel 24×7 support, and cutting-edge tech stack. Like I mentioned earlier, with our heavy focus on R&D and quality threat intelligence, our solutions are capable to mitigate ever-evolving threats.

While serving millions of individuals across sectors and industries including government organisations, our comprehensive range of solutions meet all legal and industry compliances, which are often very stringent. We deeply empathize with the CISO & CIO’s challenges and extend our support to train their teams to integrate our solutions and further educate their workforce on safe digital practices. We also undertake, if required, frequent audits and share reports to ensure seamless security at all times.

IT Voice : What can we expect from SEQRITE in terms of future developments or expansions? Are there any upcoming innovations or initiatives you’d like to share?

Sanjay : Our immediate key focus is to move up across customer segments to attain greater market shares. In the mid to long term, we’re eying geographical expansions in markets like India, which would provide ample opportunities for our company.

We’re also investing substantially in sales and marketing to enhance our growth across sectors. Given the increasing competition from online channels, we believe a robust digital presence is essential. Therefore, we will continue to invest in not just R&D but also the marketing of our brand.

IT Voice : What is the significance of the latest version, 8.2, of End Point Security (EPS) unveiled by SEQRITE?

Sanjay : The significance of SEQRITE’s latest release, EPS v8.2, lies in its ability to provide organizations with a comprehensive cybersecurity solution in an ever-evolving threat landscape. By introducing state-of-the-art Endpoint Detection and Response (EDR) technology and advanced features like the Application Control Safelist, Google & YouTube Access Control, and Automated IoC search, EPS v8.2 empowers enterprises to defend against sophisticated cyberattacks proactively. This version’s adherence to the Zero Trust Methodology ensures that only authorized applications run, reducing the risk of security breaches. Additionally, its robust capabilities in web security, rapid threat detection, real-time response, and device control further bolster endpoint protection. With EPS v8.2, SEQRITE reaffirms its commitment to equipping organizations with the tools they need to thrive securely in the digital age, setting a new standard in endpoint security and solidifying its reputation as a leader in comprehensive cyber protection.

IT Voice : How does EPS v8.2 leverage Endpoint Detection and Response (EDR) technology to enhance endpoint protection?

Sanjay : EPS v8.2’s Endpoint Detection and Response (EDR) technology significantly enhances endpoint protection by proactively searching for and mitigating threats. EPS v8.2 achieves this by:

- Proactive threat identification by continuously scanning endpoints for known malicious files, IoCs, or suspicious patterns, preventing potential harm.
- Swift detection of hidden threats, reducing dwell time and minimizing attackers’ chances to remain undetected.
- Customizable scans, while users can initiate scans, promoting collaborative threat reporting.
- Integration with external threat intelligence feeds ensures up-to-date threat detection.

- Automated responses, like isolating threats, are triggered upon detection, streamlining threat mitigation.
- Continuous monitoring maintains real-time threat visibility and protection.

Endpoint Detection and Response (EDR) technology eliminates the risk of potential cyberattacks through continuous monitoring, rapid detection, automated responses, and integration with threat intelligence.

IT Voice : What are some of the advanced features included in EPS v8.2, besides Application Control Safelist?

Sanjay : Here are some of the advanced features newly introduced in EPS v8.2:

Google & YouTube Access Controller, Automated IoC Search and Real-time IoC Blocking, USB Tethering, Roaming for Linux Endpoints, Temporary Device Access Duration Improvement, etc.

IT Voice : Can you explain how Endpoint Detection and Response (EDR) in EPS v8.2 works to provide real-time information gathering and threat blocking?

Sanjay : Endpoint Detection and Response (EDR) in EPS v8.2 provides comprehensive real-time information gathering and threat-blocking capabilities through several key features. Here’s how these features work together to enhance security:

Endpoint Threat Hunting (ETH): This proactive approach involves continuous searching for files matching known malicious hashes across all endpoints within a network. When a user identifies a suspicious file or hash, ETH uses this information to detect potential hidden attacks and actively hunts down these files before they can execute and cause harm to the endpoints or the network.

Rapid Query to Endpoints: This real-time data gathering feature connects to endpoints to retrieve information from predefined data sources, thus enabling security teams to identify potential security breaches and take immediate action

Automated IoC Search: EPS v8.2 integrates with a Threat Intelligence Platform (TIP) like MISP (Malware Information Sharing Platform & Threat Sharing) server to send regular queries for Threat Feeds, including file hashes associated with known threats. These IoCs (Indicators of Compromise) are searched on endpoints daily or weekly, and any matches between the IoCs and files on endpoints are recorded and reported.

Real-time IoC Blocking: This is a critical feature for immediate threat containment. When a potentially malicious file hash is detected on an endpoint, it can be submitted for further investigation, during which the system can also block the execution of this file in real-time to prevent any harm or lateral movement across the network.

In short, EPS v8.2's EDR system provides robust real-time information-gathering and threat-blocking capabilities. This multifaceted approach enhances the organization's ability to detect, respond to, and mitigate cybersecurity threats efficiently, helping to safeguard endpoints and the overall network infrastructure.

IT Voice : How does the Endpoint threat-hunting technology in EPS v8.2 allow administrators to proactively search for hidden attacks?

Sanjay : EPS v8.2's endpoint threat-hunting technology empowers administrators to seek out hidden attacks through crucial mechanisms proactively.

1. It utilizes Hash-Based File Detection by referencing a database of known malicious file hashes and IoCs, enabling administrators to identify files linked to known threats across all network endpoints.
2. User-initiated scans allow administrators to promptly investigate suspicious files or hashes identified by users or external sources.
3. Continuous Monitoring ensures ongoing vigilance, swiftly detecting new or concealed threats.

Swift Detection promptly flags potential threats, triggering automated responses for isolation or quarantine. The integration with Threat Intelligence platforms like MISP equips administrators to hunt for emerging threats effectively. Ultimately, this proactive approach significantly reduces dwell time, minimizing the window of opportunity for attackers to operate unnoticed within the network and reinforcing the network's overall security posture.

IT Voice : How does EPS v8.2 reaffirm SEQRITE's commitment to empowering enterprises with comprehensive cyber protection tools?

Sanjay : EPS v8.2 is a testament to SEQRITE's unwavering dedication to empowering enterprises with comprehensive cyber protection tools. This latest release reflects SEQRITE's commitment to staying at the forefront of cybersecurity innovation, as it introduces state-of-the-art features like Endpoint Threat Hunting and Application Control Safelist. These advanced capabilities enable organizations to take a proactive stance against evolving cyber threats, reduce dwell time, and bolster their security posture. By offering a wide array of functionalities, including web security enhancements, rapid threat detection, automated response mechanisms, and device control features, EPS v8.2 demonstrates SEQRITE's holistic approach to safeguarding enterprises from a multitude of cybersecurity challenges. This commitment to excellence underscores SEQRITE's mission to provide organizations with the robust cybersecurity solutions they need to thrive securely in an increasingly digital world.