EDPR
NEXT GENERATION ENDPOINT SECURITY

> “Simplify Endpoint Security With Next Generation Endpoint Detection, Protection, Response”

CURRENT CHALLENGE

Today's evolving IT landscape is an amalgamation of businesses going digital, increase in cloud adoption for multitude of applications and end user compute devices becoming more heterogeneous than ever including IoT. The nature of cyber attacks and attackers have become more stealth and sophisticated. Advanced techniques are being adopted to infltrate enterprise networks with intent to cause service disruption, stealing sensitive information or to simply demand ransom.

ENDPOINT AS THE NEW PERIMETER

Enterprise endpoints today have more critical data and are susceptible to compromise and Security breach. Enterprise endpoints continue to be the most vulnerable and often the last line of defense to prevent attacks. The ever-increasing footprint of point products to detect, protect and respond to cyber attacks adds to the complexity of securing the enterprise. Each of the point product adds complexity of independent security telemetry, management and response.

- **Single Agent across heterogeneous systems**
- **Single management console.**
- **AI based detection & protection against advanced threats**
- **No daily content updates needed**
- **Contextual automated patch testing and roll out**
- **Dynamic Whitelisting**

ANTI APT

ANTI VIRUS

PATCH MANAGEMENT

APPLICATION WHITELISTING

DATA LEAK PREVENTION

EDPR VALUE PROPOSITION

Comprehensive centrally managed and cross platform technology to protect against advanced threats and improve end user productivity.

DETECTION
PROTECTION
RESPONSE

SUPERIOR DETECTION

External and Internal Threat Detection based on Artificial Intelligence and behavior technologies across attack chain. In memory exploit detection to identify suspicious data. Emulator to detect zero day attacks and hidden malware. File reputation to identify anomalous behavior

COMPREHENSIVE PROTECTION

Protect against ransomware, advanced persistent threats, data leaks, device control, application control and other threats. Protection for next generation threats. Lightweight agent to protect the business without slowing down end point performance

INTEGRATED RESPONSE

End to End Response mechanism including device control, application control, system patching, prevention of data leak and automated actions through a single management console and unified agent. Easy integration with Security Management solutions for better response

EDPR FEATURES

Detection based on Artificial Intelligence / Machine learning techniques

Sequretek's proprietary algorithms based on advanced detection models and tested machine learning algorithms helps to detect and protect against new and stealth threats. Our predictive algorithms probatively averts threats before execution in client environments. AI works in tandem with other detection technologies within EDPR to provide complete protection capabilities against all threats. Capability to off load AI security workloads to GPU units in latest processor platforms ensures that there is no performance penalty on endpoints.

- Self learning and Regressive algorithms deployed for predictive modeling
- Identify Zero day exploits, new malware variants, APT anomaly detection
- Eliminates the need for frequent content updates within the environment

Advanced Anti virus and Anti malware based on Machine learning, Behavior and Signatures

EDPR combines the power of machine learning to detect new and unknown threats with other technologies like Behaviour, Reputation and Signatures to ensure holistic detection and protection capabilities for your enterprise. Modular detection, protection and response logic built in the product delivers optimum performance. Thousands of behaviour patterns, strong reputation score algorithm and up to date signature database for known threats create an all round detection platform.

- No Need for Daily / frequent signature updates due to multiple technology layers for protection
- Monitors file behaviors across thousands of files based on file type, structure, file meta data and other parameters.
- Real time file analysis to identify behavior and eliminate false positives
- Rich content database of existing malware for faster and accurate protection from known malware. does not need daily content updates
- Reputation based on source, target, age, frequency, location, 3rd party validations and other rules

In-memory protection for new / unidentified threats

File less malware and browser based attacks are detected and prevented using this capability within the modular EDPR AV engine.

- Prevents host of attacks that exploit In-memory functions
- Effective protection against memory misuses and process injections.

Proactive Patch Management

Facilitates proactive management of patches and software updates. Scans and identifies endpoints which contain vulnerabilities and need to be patched. Policy based deployments to automatically apply updates to groups of endpoints at scheduled times

- Enables Faster response to ensure malware does not exploit know vulnerabilities
- Maintained comprehensive inventory and patch cycles for all endpoints
- Automatically identifies vulnerable endpoints and automatically schedules patching (as per defined policies) based on OEM patch releases
- Patching for OS, Popular applications.
- Audit and compliance trails and out of box reports.

Endpoint Data Leakage Prevention

Content inspection utilizing predefined dictionaries and pattern recognition to identify sensitive data thus preventing it from getting out of the organization. Pre-built categories with rules and dictionaries for common types of sensitive data.

- Notify and capture, quarantine, prevent any sensitive information
- Prebuilt industry templates for compliance & enforcement
- Exact data matching for unstructured and non-indexable data.
- Partial data matching and indexed data matching for structured data
- Finger printing of unstructured and structured data

Application Whitelisting

Designed to preemptively block applications, programs, software libraries, scripts, updaters and installers. Detects unauthorized software execution and permits execution of only whitelisted applications. Reputation based application whitelisting for categorization as Good, Unknown and Blacklisted with realtime analysis.

- Dynamic whitelisting
- Trusted Path / Directory / Certificate based whitelisting
- Kernel level whitelisting
- Reputation based execution
- Granular custom policy implementation
- User based exception management / Self authorization
- Offline & Online Endpoint monitoring for compliance

Granular Device control

Provides the capability to restrict access of storage and media devices. Monitor and control transfer of data from endpoints to removable storage devices.

- Complete control on external device connectivity in your environment
- Granular device control within a specific device class to allow company approved device access while blocking unauthorized access.
- Read Only / read write access based on policies
- Blocks malware and infections from entering the environment
- Strong policy engine that allows for group and device based granular control
- Central management and visibility of rogue devices