Ransomware & Endpoint Protection

Unify prevention, detection, and response in a single platform

Up to 95% breaches originate at endpoints. Adapt your defences against the most advanced cyber attacks by rapidly eliminating threats with fully-automated, integrated response capabilities.

Advanced Endpoint Protection

Dealing with today's cyber threats requires a fundamentally different approach. Our technology uses a major breakthrough in signature-less detection, based on machine learning.

Organisations collectively face billions of highly sophisticated attacks across multiple vectors. Exposure to ransomware and Trojan attacks are not easy to defend against using traditional anti-virus software, and if they are discovered the legacy technology cannot respond quickly enough to the volume or difficulty of threats.

We closely monitor all system activities to identify malicious behaviour and mitigate threats in real time. What's more, the pro-active endpoint protection is switched on before your system even starts up, tracking and scanning all activity to take action when needed.

Don't become a victim of ransomware and stop targeted attacks before they even begin. Our advanced Cloud-based protection causes no impact to performance, enables a multi-layered approach and provides the lowest total cost of operation (TCO) in the market.

SentinelOne Partners with savincom

We provide scalable services using the leading corporate endpoint security platform. SentinelOne technology is certified by AV-TEST as the replacement for antivirus solutions and recognised for the best TCO per protected agent and for highly effective Cyber Security.

NSS Labs rated SentinelOne as 'Recommended' in The NSS Labs Security Value Map, performing the industry's most rigorous test to date of leading Advanced Endpoint Protection (AEP) solutions.

To provide further confidence, the technology is recognised as leading next-generation endpoint protection. SentinelOne has been positioned by Gartner as Visionary in the Magic Quadrant for Endpoint Protection Platforms (EPP) for the second straight year. The integrated platform is compliant and proven with specific industries, recognised for ease of use and deployment.

A multi-layered approach

This multi-layered protection includes prevention, detection & response as a unified service. We provide the only platform that defends every endpoint against every type of attack, at every stage in

the threat lifecycle - before, during and after an attack. Our ransomware protection service takes action as early as possible to deal with threats and alerts effectively. This is the next-generation for mitigation, by containing malware and endpoints as your protection enables automated processes such as rollback and auto-immunisation.

Automated, pro-active protection which is customisable

A fully automated, policy-driven response provides zero-touch mitigation for decisive incident response of all endpoint devices. This includes robust containment, full remediation & rollback as you can react to the alerts accordingly.

Prevention

Advanced Static Analysis using a Deep File Inspection engine discovers known and unknown malware. A global intelligence base provides dynamic whitelisting and blacklisting with 31,000 unique file characteristics defined and referenced.

Detection

Behaviour-based threat analysis enables dynamic detection of anomalies and prevents the most advanced attacks from any vector. The solution includes context forensics in true real time and builds an intuitive attack storyline go visualise malicious behaviour.

Easy to deploy and simple to manage

Adaptive defences include settings for cloud intelligence and auto-immunisation. The solution can work in parallel with existing anti-virus software and is supported on all endpoint platforms such as Windows, MacOS, and Linux. Simple deployment across enterprise-scale environments, roll out and onboarding enables you to begin customising how your service automates policies and settings. A lightweight, autonomous agent causes no impact to performance continuously monitoring all activity on the user endpoint or server, online or offline.

Constant monitoring of all activity checks files and activity against policies to apply the intelligent defences available. Both static and dynamic analysis includes deep file inspection and behaviour-based detection to uncover known and unknown threats across any vector.

The endpoint protection platform detects common threats to national-grade advanced persistent threats (APTs).

- Malware – Ransomware, Trojans, worms, backdoors File-less / Memory-based malware
- Exploits – Document-based exploits Browser-based exploits Live/ Insider
- Attacks – Script-based: Powershell, Powersploit, WMI, VBS Credentials: credential-scraping, Mimikatz, tokens

Policy-driven responses close the gap between detection and mitigation. Options to include cloud-based global intelligence, what actions to take and how to alert IT personnel, and whether to disconnect from the Network and contain or decommission devices all reduce risk. Organisations are now adding new, behaviour-based endpoint security solutions to prevent advanced threats that aren't detected at the network level. The solution provides next generation technology and a multi-layered approach to unify endpoint protection.

The solution acts on attacks post execution should an attack successfully take place on one or more endpoints. Many technologies today are focused on identifying and alerting to the existence of a threat. This sends incident response personnel into a scramble attempting to find and quarantine infected systems. Machine-speed mitigation and remediation is critical, if not the organization remains vulnerable. Our protection service stops lateral spread with containment and eliminates it from affected devices to fully mitigate and remediate threats.