advanced malware prevention

Malware multi-scanning & CDR technology that eliminates threats & zero-day attacks

Evolving threats are being designed to evade traditional signature-based and behaviour-based anti-malware defences. Your IT and OT infrastructures need an advanced multi-layer threat prevention to beat zero-day attacks, advanced persistent threats (APT) and advanced malware.Our solution allows the integration of advanced malware prevention and detection capabilities into an existing infrastructure for improved management of common attack vectors. Secure web portals from malicious file upload attacks, augment existing cybersecurity products, and develop your own malware analysis platform.

With 230,000 new samples being produced daily, malware continues to bypass existing defences due to evolving sophistication, and organisations deploying ineffective protection.

Platform & capability features

Deep Content disarm & reconstruction

Deep CDR is an advanced threat prevention technology that does not rely on detection. It assumes all files are malicious and sanitizes and rebuilds each file ensuring full usability with safe content. The technology is highly effective for preventing known and unknown threats.**File type verification**

Verify over 4,500 file types to determine the actual file type based on the content of the file, not the unreliable extension to combat spoofed file attacks. A spoofed file usually indicates malicious intent, so mitigate this risk by blocking files with incorrect extensions.**File-based vulnerability assessment**

Scan and analyse binaries and installers to detect known application vulnerabilities before they are executed on endpoint devices, including IoT devices. Using our patented technology to correlate vulnerabilities to software components, product installers, firmware packages and many other types of binary files, which are collected from a vast community of users and enterprise customers.**Proactive data loss prevention**

Content check 30+ common file types for personally identifiable information (PII) and redact or add a watermark to this sensitive data before they are transferred. This aids compliance with PCI, HIPAA, Gramm-Leach-Bliley, FINRA regulations.**Archive extraction**

Multi-scanning and Deep CDR for more than 30 types of compressed files. Archive handling options are configurable, and encrypted archives are supported. Custom workflows can order the process in which files are handled.**Multi-scanning**

An advanced threat detection and prevention technology that increases detection rates, decreases outbreak detection times and provides resiliency to anti-malware vendor issues. Choose from over 35 leading anti-malware engines to deliver enhanced protection and detects 99% of malware threats by using signatures, heuristics and machine learning techniques.

An advanced platform to protect critical

infrastructure

No longer can an organisation rely solely on detection-based cybersecurity systems to provide adequate protection for your most valuable business assets. Zero-day malware learns how to bypass these defences.Organisations are challenged in tracking and securing all data transfer channels that expose them to security threats, especially large enterprises with thousands of employees and contractors. Data transfer channels, such as file uploads, portable media devices, and email attachments, all have the potential to carry targeted attacks that can damage the organisation’s reputation, financial standing, and client relationships, and for critical infrastructure, sensitive equipment and the facility itself.