5 COMMON CYBER SECURITY THREATS THAT BYPASS YOUR ANTI VIRUS

ADVANCED THREATS

Today, adversaries have access to nation grade hacking tools. To face such capabilities, your team needs to include a technology that was built to do so, unlike legacy AV that is relying on prior knowledge to sign and detect new malware.

POLYMORPHIC MALWARE

Attackers can easily defeat signature-based AV tools that rely on checking a file's hash against a known database of malware hashes.

MALICIOUS DOCUMENTS

Sometimes a maliciously-formatted document is used to exploit vulnerabilities in the opening application to achieve code execution, and legacy AV cannot detect such by reputation.

FILELESS MALWARE

In the last few years attackers have realised that traditional AV solutions have a gaping blindspot: malicious processes can be executed in-memory without dropping telltale files for AV scanners to find.

ENCRYPTED TRAFFIC

Malicious actors can hide their activities from inspection by ensuring, just like regular websites, that traffic between the victim and the attacker's command-and-control (C2) server is protected by end-to-end encryption.

Read more on the SentinelOne Blog

The SentinelOne Endpoint Protection Platform unifies prevention, detection, and response in a single purpose-built agent powered by machine learning and automation. It provides prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into the endpoint environment with full-context, real-time forensics.

Autonomous Endpoint Protection That Saves You Time

SentinelOne™