DEEPARMOR®
by SPARKCOGNITION

Antimalware Software Development Kit (SDK)

"DeepArmor® helps you transform security solutions with the power of AI"

With $172B lost to hackers in 2017 and over 333,000 new malware variants discovered every day, financial gain is driving malware growth and malware sophistication exponentially. Fast-changing technologies and heterogeneous environments only exacerbate vulnerabilities, as they open up additional weak links that malware actors seek to exploit.

Threats are designed to go undetected for the greatest period of time possible, and malware actors seek to use all vectors at their disposal (exploits, virus, Trojans, hacks, phishing attacks, and in many cases a combination) to be as effective as possible and stay off the radar. These multiple vectors and persistent attacks are driving an industry demand for layered protection solutions.

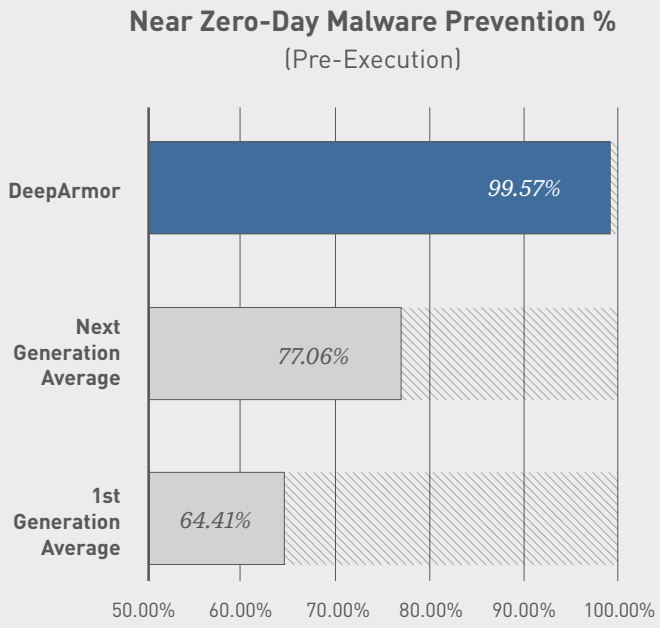
DeepArmor® Antimalware SDK

DeepArmor's Antimalware SDK benefits customers looking to augment existing solutions and those looking for a complete protection suite. It offers multi-layered protection technologies built from AI that can be integrated into existing solutions as a value add. The Antimalware SDK also addresses new business opportunities leveraging market demand for protection suites. DeepArmor's Antimalware SDK can be easily implemented at the endpoint, network, perimeter, or gateway, and on cloud-based platforms.

Multiple Technologies

The Antimalware SDK implements multiple technologies and detection methods to ensure industry-leading detection accuracy and performance for known and unknown threats that leverage zero day scenarios.

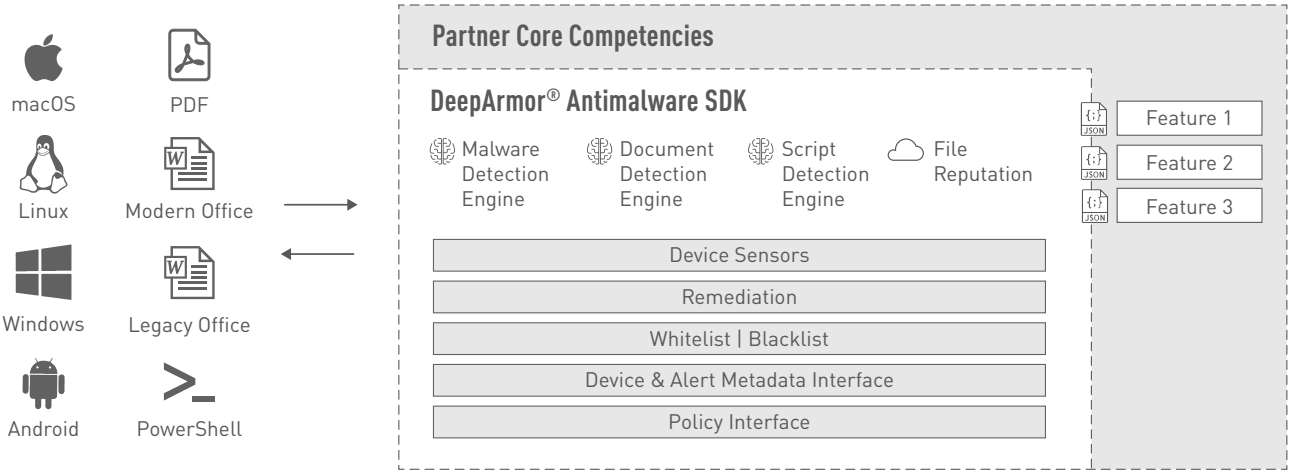
- ***AI-Based Executable Detection Engines:*** *Detects new, unknown executable malware (e.g., Windows, macOS, Linux, Android) variants including ransomware, cryptominers, Trojans, worms and polymorphic threats*
- ***AI-Based Document Detection Engines:*** *Detects new, unknown weaponized documents files with embedded scripts and macros including PDFs, modern Office documents (e.g., .docx, .pptx, .xlsx) and legacy Office documents (e.g., .doc, .xls, .ppt)*
- ***AI-Based Script Detection Engines:*** *Detects new, unknown weaponized scripts including PowerShell*
- ***File Reputation:*** *Detects known malware families and other variants based on overall file use*



Common Use Cases

- Web Gateway Security
- Network Protection
- Cloud Access Security Broker
- Email Protection
- Next Generation Firewall
- System Management Platforms
- Endpoint Detection & Response

DeepArmor® Antimalware Software Development Kit



The DeepArmor® Advantage

With more information at stake and new, innovative ways for malware to circumvent traditional AV, AI-based malware detection offers a paradigm shift in protecting organizations from the latest security threats. DeepArmor® is the industry's leading provider of AI based antimalware technology and the first to use the technology to detect weaponized documents, macros and scripts. Our groundbreaking algorithms and patented model building tools differentiate DeepArmor from other pure-play cybersecurity vendors in terms of performance and user impact. This commitment to innovation in AI is enabling DeepArmor to detect 99.6% of zero-day attacks, outperforming current first generation and next generation solutions on the market.

About SparkCognition™

SparkCognition builds leading artificial intelligence systems to advance the most important interests of society. We help customers analyze complex data, empower decision making, and transform human and industrial productivity with award-winning machine learning technology and expert teams focused on defense, IIoT, and finance.

List of Awards

CNBC DISRUPTOR 50 2017

2018 FORTRESS CYBER SECURITY AWARD

CBINSIGHTS ai.100 2018

Which Antimalware SDK is right for your needs?

NAME	USE CASE	INTERFACE	SUPPORT
SERVER ANTIMALWARE SDK	Can be integrated on network appliances solutions, gateways and or cloud services	C#, C++ and Objective-C interface bindings; allows integration via the shared library	Multiple platforms (ARM, MIPS, X86, PowerPC) and OSes (Windows, MAC and Linux) from the same API; native 32-bit and 64-bit platform support
ENDPOINT ANTIMALWARE SDK	Typically implemented on endpoint security solutions	C#, C++ and Objective C interface bindings; allows integration via the shared library	x86/x86_64 architecture; multiple operating systems (Windows, MAC, Linux); native 32-bit/64-bit platform support
ANTIMALWARE CLOUD API	Can be integrated on endpoint, network appliances solutions, gateways and or cloud services	Cloud hosted, RESTful API interface	