DEEPARMOR®

A Cognitive Approach to Anti-Malware

RAISE MALWARE PREVENTION TO A COGNITIVE LEVEL

The Evolving Threat of Cybercrime

Cybercrime is an exponentially growing threat to the world's businesses, governments and citizens. For perpetrators, there is a low risk of prosecution and large potential gain, which doesn't bode well for victims. Estimates of the annual impact of cybercrime on the global economy reach as high as $600 billion. These estimates overtake the gross national income of most countries, yet governments and companies alike continue to underestimate how easily an unsophisticated cyber attack could disrupt their operations.

Making matters worse, the exponential growth in both connected devices and malware are overwhelming the capacity of enterprise security teams. Organizations are being asked to secure IT, mobility, IoT and OT assets all while staying on top of the latest zero-day and polymorphic threats. A new approach is needed to keep up with the evolving cybersecurity landscape.

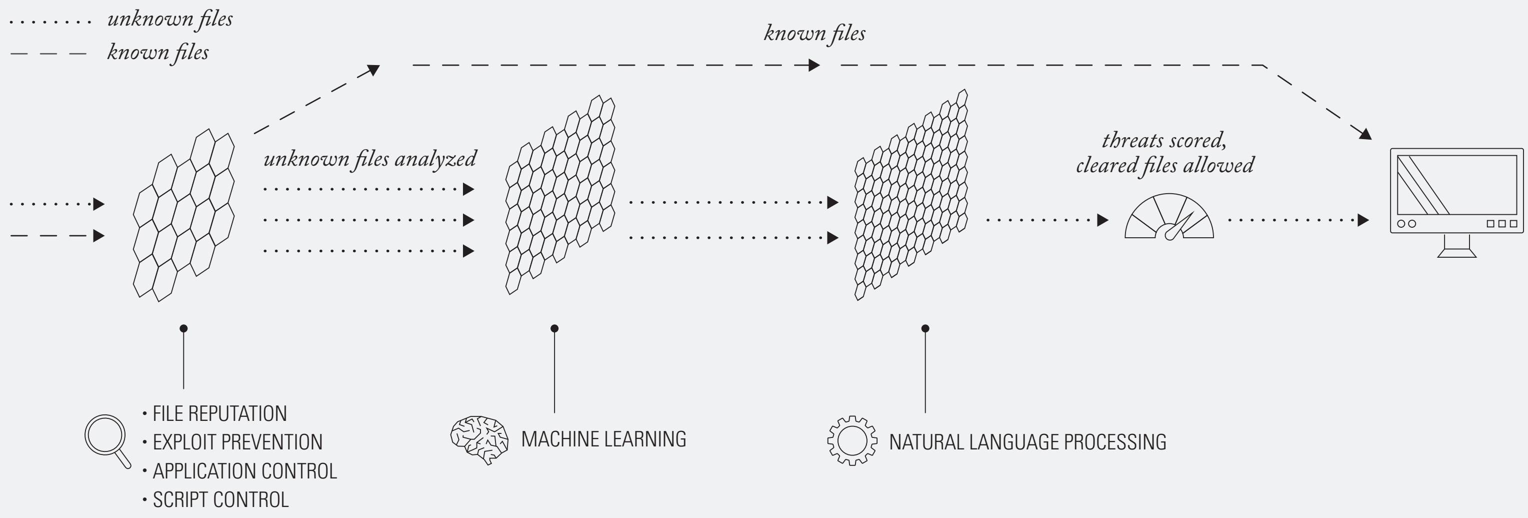
Next-Generation Endpoint Security

Attackers have been easily evading signature-based antivirus solutions for years, which is why 95% of cyber breaches originate at the endpoint. SparkCognition has redefined how endpoint security protects your organization by leveraging the power of artificial intelligence to both detect and prevent threats at machine scale.

Leveraging SparkCognition's patented artificial intelligence platform, DeepArmor is able to detect and prevent malware, viruses, worms, trojans, and ransomware in milliseconds. By taking a mathematical approach, we are able to provide industry-leading protection against zero-day and polymorphic threats, which can otherwise slip through the cracks of traditional antivirus solutions. Our unique approach is able to provide unified protection across client, mobility and IoT devices.

–Figure 1–

How DeepArmor Works



How It Works

DeepArmor's architecture consists of a small endpoint agent that integrates with the our cloud-based cognitive engine and threat intelligence platform.

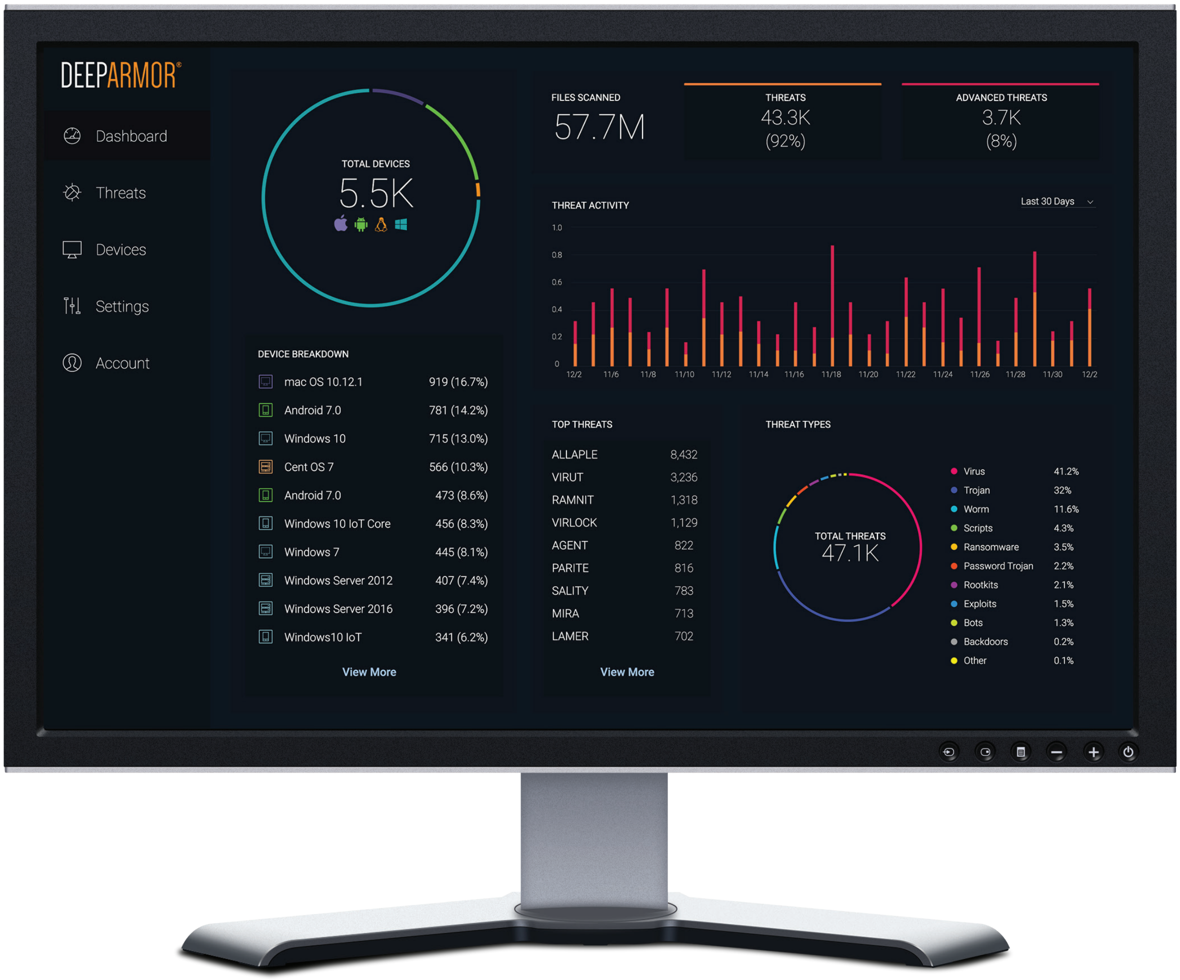
The low profile endpoint agent detects and prevents malware and advanced persistent threats, independent of signatures. Our agent is designed to protect client, server, mobile and IoT devices to provide unified protection across the enterprise. In addition, the agent can be configured to run in headless mode which enables automated protection for IoT devices without a user interface.

As shown in *Figure 1*, DeepArmor's cloud based cognitive engine uses a multi-layer filtering process to provide industry leading threat detection. Our first layer of protection includes File Reputation Analysis, Application Control and Script Control to quickly identify known malicious and anomalous files. Once known files have been filtered, DeepArmor applies an ensemble of cognitive algorithms to examine the DNA of unknown files to develop a Threat Confidence Score of each file. Our proprietary Threat Confidence algorithm is used to provide industry leading protection vs. zero-day, polymorphic threats and advanced persistent threats.

After a threat has been identified, our cloud-based management console provides unparallelled intelligence using SparkCognition's proprietary Natural Language Processing (DeepNLP) technology. Like a human security analyst, DeepNLP not only searches the internet for threat evidence, but understands the context around each threat. In doing so, DeepArmor is able to separate with confidence what is truly malicious from everything that is anomalous. Combined, our multi-layer cognitive approach provides organizations fast ROI by reducing breaches and providing greater visibility into threats across their endpoint population.

DeepArmor's management console can be hosted in SparkCognition's multi-tenant cloud architecture or can be deployed on-premise using a docker container. This flexible deployment architecture makes DeepArmor easy to deploy and easy to manage with enterprise-grade scalability.

Today's evolving cyber security landscape requires applying the best protection at the most vulnerable locations—the endpoint. No other anti-malware product compares to the efficiency, ease of management and intelligence of DeepArmor.



TOTAL DEVICES
5.5K

FILES SCANNED
57.7M

THREATS
43.3K
(92%)

ADVANCED THREATS
3.7K
(8%)

THREAT ACTIVITY
Last 30 Days

DEVICE BREAKDOWN

mac OS 10.12.1	919 (16.7%)
Android 7.0	781 (14.2%)
Windows 10	715 (13.0%)
Cent OS 7	566 (10.3%)
Android 7.0	473 (8.6%)
Windows 10 IoT Core	456 (8.3%)
Windows 7	445 (8.1%)
Windows Server 2012	407 (7.4%)
Windows Server 2016	396 (7.2%)
Windows10 IoT	341 (6.2%)

TOP THREATS

ALLAPLE	8,432
VIRUT	3,236
RAMNIT	1,318
VIRLOCK	1,129
AGENT	822
PARITE	816
SALITY	783
MIRA	713
LAMER	702

THREAT TYPES

TOTAL THREATS
47.1K

● Virus	41.2%
● Trojan	32%
● Worm	11.6%
● Scripts	4.3%
● Ransomware	3.5%
● Password Trojan	2.2%
● Rootkits	2.1%
● Exploits	1.5%
● Bots	1.3%
● Backdoors	0.2%
● Other	0.1%

Advantages of DeepArmor's Cognitive Approach

Accuracy: Our ensemble of machine learning algorithms automatically adapt to new malware variants, providing industry leading detection vs. zero-day and polymorphic threats. Our mathematical approach results in both a reduction of breaches and risk.

Speed: Every second counts. Our proprietary machine learning model is highly optimized to provide sub-second malware detection. Specialized static analysis optimization coupled with local and global caching provide even faster results, shrinking days or week-long malware remediation to seconds.

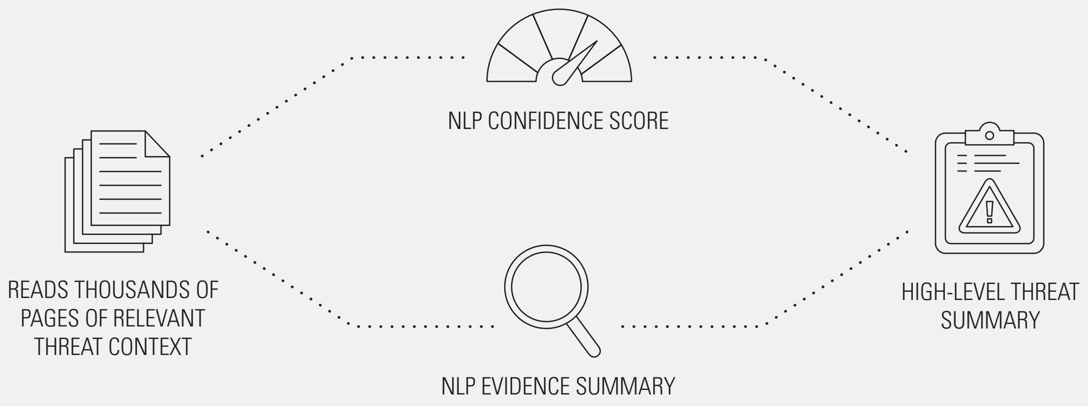
Unified Protection: Mobility and IoT devices have proliferated throughout the enterprise. Our cognitive threat detection engine provides unified protection for clients, servers, mobile and IoT devices.

Enterprise Scalability: Our low-profile client agent and cloud-based management console enables security teams to deploy and secure large client populations with ease. DeepArmor can be deployed in both public and on-premise architectures including isolated networks.

Threat Intelligence with NLP: Our cloud-based threat intelligence platform provides unparalleled insights into the threats occurring across your endpoint population. Threats are automatically researched using Natural Language Processing (NLP) to reduce false positives and close security gaps quickly.

–Figure 2–

DeepArmor Features SparkCognition's Deep NLP Technology


NLP CONFIDENCE SCORE
READS THOUSANDS OF PAGES OF RELEVANT THREAT CONTEXT
HIGH-LEVEL THREAT SUMMARY
NLP EVIDENCE SUMMARY

Deployment Options

DeepArmor offers two deployment options, Detect and Prevent from a single solution. This allows organizations to choose the deployment model that best fits their business requirements.

Deployment Option 1: In *Detection Only mode*, DeepArmor runs silently to identify compromised endpoints using SparkCognition's patented artificial intelligence platform, including compromises that existed prior to deploying DeepArmor. Our endpoint agent, combined with our Threat Intelligence platform, provides visibility into all threats across the end user population. DeepArmor leverages SparkCognition's NLP capabilities to automatically research threats and accelerate remediation. Threat data can also be exported to SIEMs and other security tools.

Deployment Option 2: In *Detect and Prevent mode*, DeepArmor includes all of the threat detection and intelligence capabilities provided in Detection Only deployments, and also automatically prevent threats before they can breach the endpoint. DeepArmor will block malware, viruses, worms, trojans and ransomware before execution, in milliseconds. The DeepArmor agent also includes additional layers of security features including memory protection to prevent exploits, script control, and robust application control to block breaches before they start.

Endpoint Protection Features

EXECUTION CONTROL	Monitors all active executables and processes to block malicious threats in milliseconds, before they can compromise a user's system
BACKGROUND THREAT DETECTION	Analyzes executables sitting dormant on the user's system to identify and quarantine dormant threats before they can execute
REAL-TIME FILE MONITORING	DeepArmor monitors activity on the file system in real-time to detect threats before they execute
APPLICATION CONTROL	Has the ability to control application execution based local or global whitelists which provides superior protection for low change systems like servers, POS, industrial controls, ATM's, and kiosks
SCRIPT CONTROL	Has the ability to control script execution-based local or global whitelists
MEMORY PROTECTION	Analyzes file executions in memory layer (in addition to OS layer) looking for behaviors that are indicative of compromise
HEADLESS MODE	Has the ability to run in headless mode on devices without a user interface (e.g., Windows IoT Core, AndroidThings). Device security posture can be administered and monitored from the management console
OS SUPPORT	Supports Windows 7, 8 & 10 as well as Windows Server 2008, 2012 & 2016. Support for Android Mobile, AndriodThings and MacOS are coming in early 2016

Enterprise Management Features

CLOUD CONSOLE	The Cloud Console is a multi-tenant management console designed for enterprise customers. The console can be hosted or deployed on-premise.
THREAT DASHBOARD	Includes a centralized dashboard that displays a summary of the user population and threats encountered by DeepArmor on all clients (agents) within the user population
THREAT INTELLIGENCE WITH DeepNLP	Has comprehensive threat intelligence and analytics capabilities enabling the security team to quickly identify emerging threats and accelerate threat research using SparkCognition's patented NLP capabilities
DEVICE GROUPS	Can create groups of clients that can be administered together for policy setting and threat analysis
POPULATION INTELLIGENCE	Enables the security teams to drill-down to the individual system to identify where breaches are initiated and ensure individual systems are secured
ADMINISTRATION	Enables the security team to set global security policy across the entire user population of clients or refine that policy for individual groups or systems

About SparkCognition

Austin, Texas-based SparkCognition develops cutting-edge machine learning that models physical and virtual assets, continuously learns from data, and derives intelligent insights to secure and protect infrastructure around the clock. The company's cybersecurity solutions analyzes structured and unstructured data and natural language sources to identify potential attacks in the IT and IoT environments. The uniqueness of the cognitive platform is underscored by the fact that it can continuously learn from data and derive automated insights to thwart emerging issues, without the need to build manual models.

Learn More About DeepArmor®

To learn more about how SparkCognition's DeepArmor can add a cognitive layer to improve your security posture, please email **sales@sparkcognition.com** or request a demo on our website **www.sparkcognition.com/deeparmor/**