Intellesec

CYBER SECURITY SIMPLIFIED

www.intellesec.co.uk

Get real-time protection against advanced threats driven by machine learning and intelligent automation.

box

"With the onslaught of malicious actors deploying advanced malware and the limitations of existing antivirus software, this software is providing a critical solution to this problem. A solution that will benefit the entire industry."

Justin Somaini, Chief Trust Oficer, Box

Last year, enterprise organizations collectively faced over three billion cyber-attacks. When you consider the growing diversity and sophistication of these attacks, it's only natural to question your ability to detect all of them, and whether your organization's response is effective enough.

Dealing with today's cyber threats requires a fundamentally different approach.

The truth is, static, AV-based solutions just don't cut it.

Today's advanced malware, exploits, and other cyber attacks will blow right by AV-based protection in a fraction of the time it takes to get updated with the latest threat signatures.

Furthermore, vulnerability exists in the gap between detection and response.

Even if an attack is successfully detected, lack of integration with incident response tools forces manual attempts to neutralize it. In the meantime, that attack can still proliferate to other areas of your infrastructure.

The key to effective endpoint protection lies in the ability to dynamically analyze and predict any threat's behavior and respond intelligently at machine speed.

Recognized as a Visionary on the 2016 Gartner Magic Quadrant for Endpoint Protection Platforms.

AV TEST
av-test.org 06/2015

APPROVED
CORPORATE
ENDPOINT
PROTECTION

Certified replacement for AV-based solutions.

MALWARE

Real-time, Unified Endpoint Protection

IT unifies prevention, detection, and response in a single platform driven by sophisticated machine learning and intelligent automation. It enables you to predict malicious behavior across major threat vectors in real-time, rapidly eliminate threats with fully automated, integrated response capabilities, and adapt your defenses against the most advanced cyber-attacks.

Predict malicious behavior.

Continuous System-level Monitoring

Deployed on each endpoint device with a lightweight autonomous agent monitors all activity in both kernel and user space (including files, processes, memory, registry, network, etc.). The Agent is virtually silent and will never degrade precious user productivity.

Behavioral Detection of Advanced Malware, Exploits and Live Attacks

Endpoint Agents leverage the software's Dynamic Behavior Tracking (DBT) Engine which uses sophisticated machine learning to predict threats across any vector against a full context of normal behavior.

Real-time Forensic Analysis

Dramatically enhances your investigative capabilities with detailed analysis reports, sent from the Agent to the cloud-based management console in real-time.

Attack Storyline Visualization

Shows you a 360-degree view of an attack, mapping out its point of origin and progression across endpoints and other systems for complete forensic insight.

Rapidly eliminate threats.

Zero-Touch Mitigation

Fully integrated, automated response protocol covers all endpoints – local and remote.

You can swiftly kill or quarantine malicious processes, making dwell time a thing of the past.

Robust Containment

Upon threat detection, the software immediately stops its lateral spread cold by disconnecting the infected endpoint device from the network, but still maintains the Agent's connection to the management console.

Full Remediation

Easily reverse attack-driven modifications and restore manipulated files to their last known trusted states.
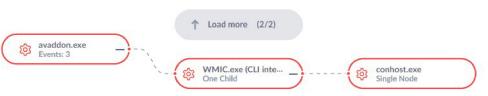
Seamlessly adapt defenses.

Auto-Immunization

Each time the Dynamic Behavior Tracking Engine finds a new, never- before-seen malicious binary, the software engine instantly flags it and notifies all Agents on the network, rendering other endpoints immune to the attack.

Cloud Intelligence

Further extends your protection by leveraging up-to-the- minute cloud intelligence and data from select reputation services to proactively block known threats.

↑ Load more (2/2)

avaddon.exe
Events: 3

WMIC.exe (CLI inte...
One Child

conhost.exe
Single Node

"IT unifies prevention, detection, and response in a single platform driven by sophisticated machine learning and intelligent automation.

It enables you to predict malicious behavior across major threat vectors in real-time, rapidly eliminate threats with fully automated, integrated response capabilities, and adapt your defenses against the most advanced cyber-attacks"

Marco Essomba
CTO BlockAPT

The Platform

Protects Major Endpoint Platforms

Ensures universal protection across endpoint devices running Windows, OS X, and Linux.

Integration with Enterprise Security Infrastructure and Tools

Offloads indicators using industry standard formats (CEF, STIX, Open-IOC) for seamless integration with SIEMs, firewalls, and leading network security solutions.

GET IN TOUCH!
_____

System Requirements

CLIENTS
Operating Systems: Windows 7, 8, 8.1, 10
Windows Server 2008 R2, 2012
R2
.NET
4.5
OS X 10.9.x, 10.10.x, 10.11

109 Coleman Road
Leicester, LE5 4LE
_____

hello@intellesec.co.uk
0116 3266123

Intellesec
CYBER SECURITY SIMPLIFIED