BETTER SAFEGUARD YOUR SYSTEM FROM CYBER THREATS WITH ANTIVIRUS PROTECTION

Honeywell Advanced Endpoint Security
Powered By Deep Instinct™

Honeywell | deepinstinct

THE IMPORTANCE OF CYBERSECURITY

Buildings are rapidly embracing digitization. Today, an enterprise-wide view of integrated building control systems and sensors is typically essential to drive increased productivity, operational efficiency, and improved response time to events. More and more Operational Technology (OT) control systems such as heating, ventilation, and air conditioning (HVAC), energy metering and power management, lighting, fire protection and alarms, access control, CCTV surveillance, and voice and data communications, converge in a connected environment – transforming the way buildings and their occupants operate and interact with each other.

As organizations everywhere embrace the demand for connected environments, they often also acknowledge their increased exposure to cybersecurity threats. To better defend against potential financial loss or reputational damage caused by cyber-attacks, a strong cybersecurity strategy should be implemented.

Discover one of the most sophisticated, intuitive, and revolutionary real-time, next generation anti-virus solutions that uses a deep learning (DL) framework to help detect and deter cyber threats expeditiously. The proactive and prevention centric approach enhances protection, while helping to dramatically reduce costs.

THE DEEP LEARNING EVOLUTION

Honeywell Advanced Endpoint Security (HAES) is a pioneering technology that applies deep learning to OT cybersecurity. Deep learning is inspired by the brain's ability to learn. Once the brain learns to identify an object, its identification becomes almost second nature. As the artificial brain learns to detect certain cyber threats, its prediction capabilities become more instinctive. As a result, zero-day and Advanced Persistent Threats (APT) attacks are more readily detected and thus prevented in near real-time with enhanced accuracy.

Using an innovative deep learning framework, our solution offers a near real-time threat prevention platform with multi-layer protection against known and unknown threats from a file or a fileless attack. It can be applied on endpoints such as mobile devices, desktops, servers, and workstations with virtually any operating system.

THE DEEP LEARNING ADVANTAGE

PREDICTION

of future cyber threats based on innovative and pioneering deep learning framework designed for cybersecurity

REAL-TIME THREAT PREVENTION

Endpoint, mobile, server

WIDE SYSTEM COVERAGE

Windows, iOS, Android, ChromeOS, MacOS

EASE OF IMPLEMENTATION

Minimizing need for rip and replace

Fast and seamless deployment

HIGH DETECTION RATE

Industry low levels of false positives

AUTONOMOUS

On-device prevention

Real-time automated threat classification

Connectionless

ENHANCED OPERATIONAL EFFICIENCY

Augment high skilled staff

Typically 1-2 annual updates

User-friendly, one simple management console

VIRTUALLY ANY ENVIRONMENT

Online

Virtual desktop

Infrastructure (VDI)

Cloud/ On-premise

Multi-tenancy

THE STATE OF CYBERSECURITY

Our world is increasingly under cyberattack at the personal, organizational, and governmental levels. The volume and variety of cyberattacks is expanding almost every day, and so is the degree of devastation that can be caused. The need for a paradigm shift in cybersecurity has essentially never been greater.

Over **350,000** new malicious programs everyday

Source: AV test, 2018

Big breaches can cost an enterprise between **$40M – $350M**

Source: IBM 2018

THE DEEP LEARNING **PARADIGM SHIFT**

FALSE POSITIVES ARE NO LONGER ACCEPTABLE

Deep learning, also known as deep neural networks is one of the most advanced subsets of artificial intelligence, and takes inspiration from how the human brain works. It is a pioneering and unique AI method capable of training directly on raw data and does not require feature engineering by a human expert. It analyzes virtually 100% of the raw data and can scale well to hundreds of millions of training samples. It continuously improves as the training data set becomes larger and provides multiple levels of non-linear correlation between data features. Among other solutions to combat cyber threats, deep learning is considered one of the most effective, resulting in virtually unmatched detection rates and reduced false positives.

ANTIVIRUS

	TRADITIONAL	MACHINE LEARNING	DEEP LEARNING
Accuracy	Low, signature based	Moderate with high false positives	High accuracy with a nearly zero false positive rate
Involvement of domain expert	Required for signatures and heuristics creation	Required for feature engineering and extraction	Not required; virtually autonomous
Amount of Data Analyzed	Analyzes known threat vectors	Analyzes small fraction of entire threat vector	Analyzes the entire threat vector
Type of files	Any	Mostly Portable Executable (PE)	Wide variety of files and fileless

OUR **OFFERING**

Our solution provides enhanced protection and is based on a prediction and prevention first approach, followed by detection and response, with high efficacy against cyber threats tailored for OT environments, using the following layers:

01 PRE-EXECUTION
Predict and Prevent

Deep Static Analysis on virtually any type of file helping to prevent the attack before the files are accessed or executed. Additional layer of protection based on deep learning to predict and prevent both known and never seen before malicious files.

Script Control: A compliance and policy infrastructure designed to reduce the script-based attack surface.

Time to predict and prevent

in Milliseconds

By D-Brain

02 ON-EXECUTION
Detect and respond

Deep Behavioral Analysis to mitigate enhanced ransomware threats, code injection techniques and known payloads, and applying automatic remediation.

Time to investigate

in Milliseconds

By Deep Classification

03 POST EXECUTION
Visibility and Analysis

Deep Malware Classification in real-time; without human involvement. Advanced Threat Analysis services for threats found in the organization.

Remediation

Quarantine files, restore and delete files remotely, terminate running processes, isolate the device from the network, whitelist and blacklist of files.

Time to remediate & contain

<1 Minute

BROAD PROTECTION AGAINST ATTACK VECTORS

FILE-BASED MALWARE

- Executables – Virus, Worm, Backdoor, Dropper, Potentially Unwanted Application (PUA), Wiper, CoinMiner
- Non-executables – Documents (Office, PDF, RTF), Images, Fonts, Flash, Macros
- Known shellcodes

MOBILE

- Applications
- Networks attack (MITM, SSL MITM)
- Compliance

RANSOMWARE

- Enhanced protection against various type of ransomware

FILELESS MALWARE

- Scripts and Powershells
- Code Injection
- Dual-use tools

EXPLOITS

- Documents
- Flash files
- Images
- Fonts

SPYWARE

- Banking trojans
- Keyloggers
- Credentials dumping

KEY DIFFERENTIATORS

THE DEEP LEARNING NEURAL NETWORK "BRAIN"

- Innovative DL framework
- Raw data, virtually 100% data
- Autonomous - no cyber expert is typically required
- Analyze multiple levels of non-linear correlation between data features

SINGLE THREAT PREVENTION PLATFORM

- Virtually any file type
- Cross-OS
- Endpoint, Mobile, Server
- Against file/fileless-based attack
- Predict and prevent, Detect and Respond
- Unique malware classification
- On-premise or cloud native by design

AUTONOMOUS ON-DEVICE AGENT

- Lightweight: <150MB, <1% CPU
- Connectionless protection
- Typically 1-2 updates a year

DIGITAL FORENSICS

Insights on detected and prevented file and script event activities such as:

- Certificate
- File Type/Path
- Hash
- Process Chain
- Size
- Threat Life cycle/Severity

SANDBOX ANALYSIS

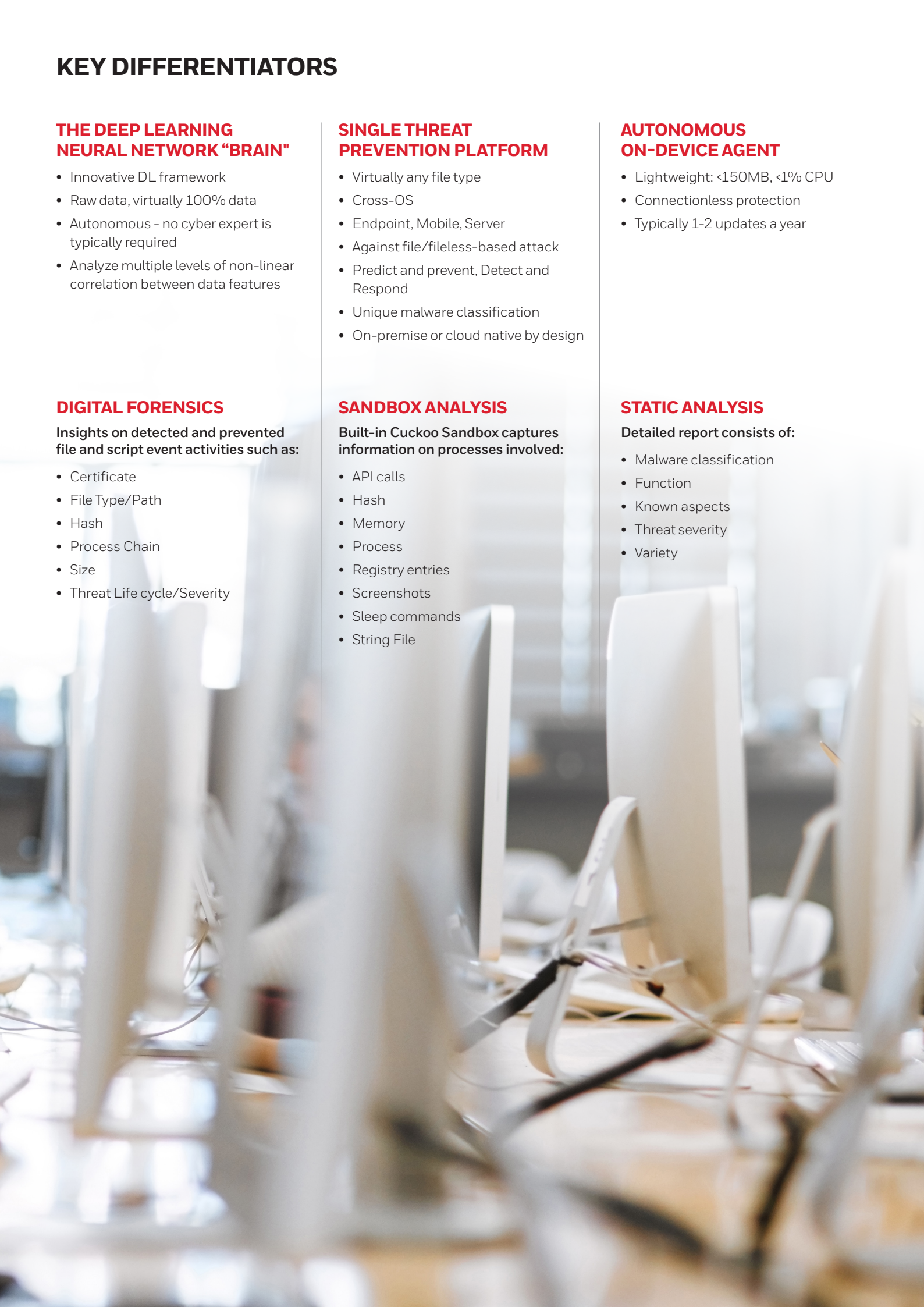
Built-in Cuckoo Sandbox captures information on processes involved:

- API calls
- Hash
- Memory
- Process
- Registry entries
- Screenshots
- Sleep commands
- String File

STATIC ANALYSIS

Detailed report consists of:

- Malware classification
- Function
- Known aspects
- Threat severity
- Variety



Honeywell Building Technologies
715 Peachtree St NE
Atlanta, Georgia 30308
buildings.honeywell.com

BMS-BR-HAES | 01-00316 | 2022-04-04

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell