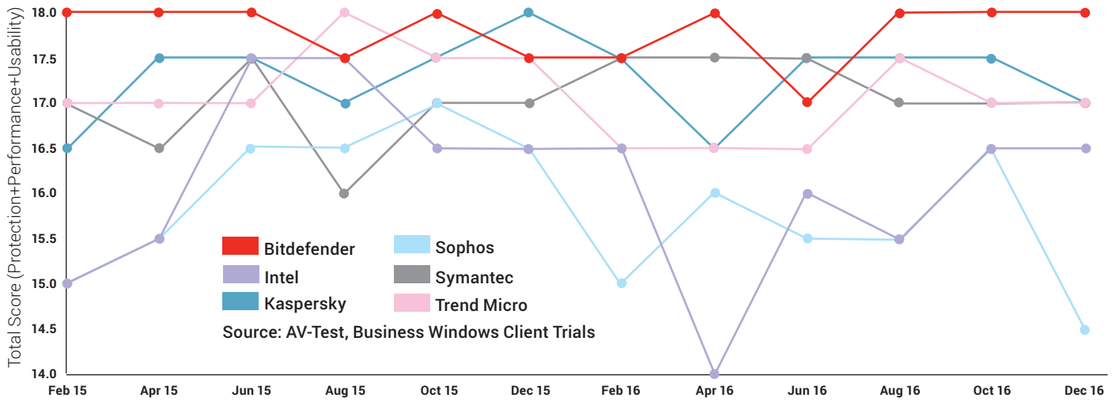
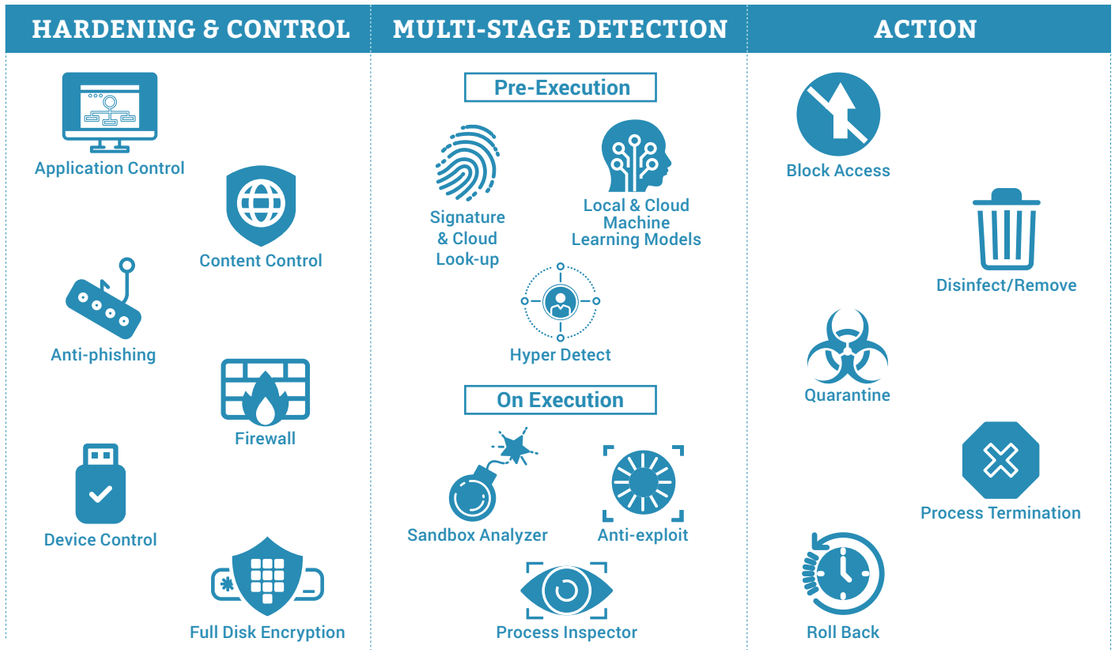
PROVEN CONSISTENCY IN SUPERIOR PROTECTION, PERFORMANCE, AND USABILITY



BITDEFENDER LAYERED NEXT GENERATION ENDPOINT PROTECTION PLATFORM

USES ADAPTIVE-LAYERED ARCHITECTURE THAT INCLUDES ENDPOINT CONTROLS, PREVENTION, DETECTION, REMEDIATION AND VISIBILITY.



GravityZone Endpoint Security HD Value Proposition

GravityZone Endpoint Security HD is the **Next-gen endpoint protection platform (EPP)** that accurately protects enterprises against **sophisticated** cyber threats. Using advanced **machine learning** technology and **threat detection sandbox, HD** prevents and detects unknown threats and targeted attacks with **precision.** With improved threat behavior context, **HD automatically responds** to threats and prevents compromises of enterprise endpoints. All delivered in a single agent managed with one integrated console.

SECURITY EFFICACY

Accurate protection against sophisticated threats

- Detect threats that evades traditional endpoint security
- Accurate prevention at pre-execution
- No-false positive – built-on adaptive layered architecture
- Zeroes-in on advanced hacking tools, exploits, ransomware and gray-ware/ potentially unwanted programs (PUP)

INTELLIGENT RESPONSE

Immediate action to prevent breach and limit damage

- Immediate and automatic actions
- Prevent damages caused by advanced attacks
- Automatically sandbox submission
- Terminate malicious processes
- Roll back malicious changes

BETTER INSIGHT

Provide better context on threats

- Remote detonation (Sandbox)
- Provide better context on threats
- Connect threats with threat actions
- Enhanced endpoint optics for future analysis and further actions
- Expose suspicious threats (HD reports)

Bitdefender
KEY DIFFERENTIATORS

NON-SIGNATURE RELIANT TECHNOLOGIES

HyperDetect: Additional layer of detection at the pre-execution stage features new machine learning models, behavior technology

Trained to block unknown malware and advanced threats

Proven Machine Learning algorithms trained for more than 8 years on the biggest sample size: 500M endpoints-sensors, trillions of samples

LAYERED NEXT-GENERATION PROTECTIONS

Hardening and Control: Application Control, Content Control, Device Control, Anti-phishing, Firewall, Full Disk Encryption

Multi-stage detection: Pre-Execution, On-Execution

Protective Action: Block Access, Quarantine, Disinfect/Remove, Process Termination, Roll Back

Visibility and Management

PROCESS INSPECTOR

Protection against file-less attacks

Always monitors running processes at zero trust

Maintains behavior-based leger for all running processes

Process Termination: Convict when process reaches given threshold

Revert changes made by malicious process

ADVANCED EXPLOIT PREVENTION

Protection against zero-day threats

Protects commonly used Microsoft and Third-Party applications

Focuses on attack tools and techniques

Serves as an additional layer of security for unpatched known and zero-day vulnerabilities

Works out of the box and is designed for precision

SANDBOX ANALYZER

Protection against zero-day and unknown threats

Automatic submission of suspicious files from endpoints for sandbox analysis

Options to use blocking or monitoring mode

Verdict in real-time

Insight into behavior of unknown files

How we fare compared to...

SYMANTEC

Proven Machine Learning technology – We are using ML technologies since 2007, our technologies are matured and perfected vs. Symantec's unproven.

Prevention against advanced exploit techniques – Protects from advanced exploit techniques such as ROP, Symantec only protects from limited exploit techniques.

Modular, fast and light-weight agent – Our endpoint agent is modular, light-weight and fast vs. Symantec endpoint agents is bloated.

Simple and intuitive User Interface – We have simple, consistent and intuitive management console for cloud and on premise vs. Symantec (does not have cloud management). Symantec UI is complex and tedious, it has steep learning curve.

Protection against runtime threats – Our real-time Process Inspector technology operates at zero trust and kills malicious processes in their tracks vs. SONAR, a real-time protection technology that suffers from HIGH False Positives'. Most customer often disable it.

INTEL SECURITY (MCAFEE)

Proven Solution Efficacy – Bitdefender consistently ranked high in AV-Comparatives Heuristic Protection tests for new or zero-day threats vs. mediocre performance by McAfee solution.

Single Modular Endpoint Agent: Bitdefender has a modular, light-weight and fast agent vs. McAfee uses multiple bloated agents to provide protection.

Powerfully Simple Management – Simple, intuitive and single pane of glass management for on-premise and cloud deployments (policy management through ePO is tedious and complex, many key features need additional components to install).

TREND MICRO

Proven Solution Efficacy – Bitdefender consistently ranked high in AV-Comparatives Heuristic Protection tests for new or zero-day threats.

Powerfully Simple Management – Simple, intuitive and single pane of glass management for on-premise and cloud deployments (DeepSecurity and OfficeSecurity have separate consoles).

Hypervisor Agnostic and Memory Introspection Solution for Data Center – Bitdefender SVA solution is hypervisor agnostic and HVI for Citrix is unique in the industry.

SOPHOS

Proven Machine Learning technology – We are using ML technologies since 2007, our technologies are matured and perfected vs. Sophos and Invincea's claims.

Industry proven efficacy and performance – Bitdefender consistently ranked top in AV-Comparatives Heuristic Protection tests for new or zero-day threats vs. mediocre performance by SOPHOS.

Hypervisor Agnostic and Memory Introspection Solution for Data Center – Bitdefender SVA solution is hypervisor agnostic and HVI for Citrix is unique in the industry.

KASPERSKY

Powerfully Simple Management – Simple, intuitive and single pane of glass management for on-premise and cloud deployments. Kaspersky uses outdated master-slave architecture, which is not scalable and adds complexity. It requires separate MS SQL or Oracle database Policy management that is tedious and time consuming.

Ease of deployment – GravityZone installation is non-intrusive, it does not require host reboots or placed into maintenance mode.

Hypervisor Agnostic and Memory Introspection Solution for Data Center – Bitdefender SVA solution is hypervisor agnostic and HVI for Citrix is unique in the industry.

ESET

Powerfully Simple Management – ESET does not have a cloud solution. Instead, it offers a web-based "Remote Administrator" console that customer must deploy and maintain. The user must click minimum of 12 times from the main dashboard in order to create a basic policy without customizing any options. To customize options, the user will need to click several dozen times more.

Ease of deployment – ESET requires the customer or partner to arrange their own hosting and carry the overhead and associated costs.

Hypervisor Agnostic and Memory Introspection Solution for Data Center – Bitdefender SVA solution is hypervisor agnostic and HVI for Citrix is unique in the industry.

AV TEST DECEMBER 2016

AV TEST RESULTS SHOWING BITDEFENDER'S PERFECT SCORE VS MICROSOFT

NAME	PROTECTION	PERFORMANCE	USABILITY
BITDEFENDER Endpoint Security 6.2	✦✦✦✦✦✦	✦✦✦✦✦✦	✦✦✦✦✦✦
INTEL SECURITY McAfee Endpoint Security 10.2	✦✦✦✦✦✧	✦✦✦✦✦	✦✦✦✦✦✦
KASPERSKY LAB Endpoint Security 10	✦✦✦✦✦✦	✦✦✦✦✦	✦✦✦✦✦✦
SOPHOS Endpoint Security and Control 10.6	✦✦✦✦✦	✦✦✦✧	✦✦✦✦✦✦
SYMANTEC Endpoint Protection 14.0	✦✦✦✦✦✦	✦✦✦✦✦✧	✦✦✦✦✦✧
TREND MICRO Office Scan 11.0	✦✦✦✦✦✦	✦✦✦✦✦	✦✦✦✦✦✦

AV COMPARATIVES TEST 2016

2016 SUMMARY RESULTS PUBLISHED ON 4TH FEB 2017

✦ STANDARD / ✦✦ ADVANCED / ✦✦✦ ADVANCED+

	FILE DETECTION	PERFORMANCE	REAL WORLD PERFORMANCE	MALWARE REMOVAL	FILE DETECTION	PERFORMANCE	REAL WORLD PERFORMANCE
	MARCH 2016	MAY 2016	FEB-JUN 2016	MAR-SEP 2016	SEPT 2016	OCT 2016	JUL-NOV 2016
BITDEFENDER	✦✦✦	✦✦✦	✦✦✦	✦✦✦	✦✦✦	✦✦✦	✦✦✦
KASPERSKY LAB	✦✦✦	✦✦✦	✦✦✦	✦✦✦	✦✦✦	✦✦✦	✦✦✦
ESET	✦✦✦	✦✦✦	✧✧	✧✧	✧✧	✦✦✦	✦✦✦
MCAFEE	✧✧	✧✧	✦		✦✦✦	✦✦✦	✦
TREND MICRO	✧✧	✦	✧✧	✧✧	✧✧	✦	✧✧
SOPHOS	✦	✧✧	✦	✧✧	✧✧	✦	✦
MICROSOFT	✦	✦	✦	✧✧	**Tested**	✦	✦