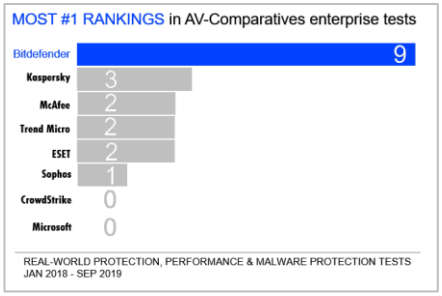
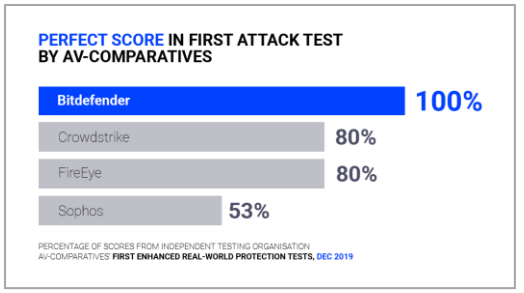
Bitdefender MSP Battle Card

THE CONTEXT: Sophisticated cyberattacks routinely evade AV detection, causing MSPs and customers to lose data, money, time, and reputation. Adding new, unproven security layers from different vendors, increases costs and operational efforts with limited security gains





Why Bitdefender

- Stop more ransomware and elusive threats with **AV and Endpoint Security consistently ranked 1st for protection** across major real-world independent tests
- Global cybersecurity innovator, **technology used by 38% of endpoint security vendors** (Gartner 2018)
- Reduce operational efforts automate protection with **Unified Advanced MSP Security**, multitenancy, monthly licensing, and RMM/PSA Integrations
- Reduce Attack Surface with **extra risk, hardening, prevention, and detection layers** that others don't include or charge extra for

World's most effective AV and Endpoint Sec.

- Perfect 6/6 Protection score in every AV-Test trial since 2016
- Most #1s in AV-Comp
- Perfect score against advanced attacks

How to win against AV, Traditional Endpoint Security and Next-gen vendors

Webroot	Sophos, Trend, McAfee, Symantec, ESET, Kaspersky	Sentinel One, Carbon Black, Cylance
• **Webroot has very light but very weak protection, either scoring very low or avoiding independent tests** • **Bitdefender Content Control filters unwanted websites and categories on the endpoint without charging extra for DNS Security** • **Bitdefender Risk Analytics simplifies and automates mitigation of vulnerable system configurations** • **Bitdefender delivers advanced security add-ons Webroot does not offer such as cloud sandboxing, Tunable Machine Learning, or EDR**	• **Bitdefender Risk Analytics simplifies and automates mitigation of vulnerable system configurations** • **Reduce attack surface with extra layers such as Risk Analytics, Exploit Defense, Process Inspector, that are included free** • **Bitdefender consistently ranks ahead in detecting advanced attacks** • **Bitdefender advanced security layers are more competitively priced and managed using the same console and agent** • **Bitdefender uses a simple yet powerful cloud console, more RMM integrations and optimized security for virtual and cloud workloads**	• **Bitdefender Risk Analytics simplifies and automates mitigation of vulnerable system configurations** • **Bitdefender has more mature machine learning or next-gen capabilities, perfected since 2008, before many so called next-gen competitors existed** • **Early prevention and automatic detection with extra hardening and prevention layers** • **RMM integrations significantly simplify deployment, management, reporting and ticketing** • **Bitdefender consistently ranks ahead in detecting advanced attacks**

Vendor functionality comparison

Functionality	Bitdefender	Webroot	Microsoft	Sophos	Sentinel One	ESET	Kaspersky	McAfee	Trend Micro
Risk Analytics	✓	X	✓	X	X	X	X	X	X
Content Control	✓ (Included)	V (Separate DNS product)	Web filtering	✓	X	X	✓	X	✓
Device Control	✓	X	X	X	X	X	✓	X	✓
Network Attack Defense	✓	X	X	HIPS	X	✓	HIPS	IPS	IPS
Anti-exploit	✓	X	✓	✓ (Extra cost)	X	✓	✓	X	X
Process Inspector (0-trust automatic detection)	✓	✓	✓	✓ (Extra cost)	✓	✓	✓	✓	✓
Tunable ML	✓	X	X	X	X	X	✓	X	X
Cloud Sandbox	✓	X	✓	X	X	X	✓	X	X
Full Disk Encryption	✓	X	✓	✓	X	✓	✓	X	✓
Patch Management	✓	X	✓	X	X	X	✓	X	X
Email Security	✓	X	✓	✓	X	X	✓	X	✓
EDR	✓	X	✓	✓	✓	X	✓	✓	✓
RMM Integrations	Kaseya, CW, Datto, Ninja RMM, SolarWinds	Kaseya, CW, Datto, Ninja RMM, Atera, Continuum, PulseWay Syncro	X	Datto, CW	SolarWinds	Kaseya, CW, Datto, Ninja RMM, SolarWinds	Kaseya, Datto, CW, SolarWinds, Tigerpaw® One	X	Kaseya, CW, Datto

Key Differentiators by product

Product	Landscape	Differentiators
AV and Endpoint Security (Core)	MSPs look for new AV/Endpoint security when dissatisfied with the protection rates, inefficient management or performance of the current solution, or are looking to expand capabilities	• #-1 for protection consistently in major independent tests • Reduce attack surface area and costs with extra layers such as risk analytics, content control, device control, exploit defense, network defense • Simple monthly usage-based licensing, single cloud web console and integrations with all major RMM /PSA tools to automate security
Overall differentiator: Switching and consolidating any new security product to Bitdefender enables MSPs to streamline security, improve performance, and reduce overhead and cots with one console and agent.		
Full Disk Encryption	MSPs often use different vendors for endpoint security and full disk encryption, while smaller ones sometimes store encryption keys manually to reduce costs	• Centrally deploy encryption with pre-boot authentication, manage and restore encryption keys • Uses native encryption technologies to avoid performance and compatibility issues: BitLocker on Windows, FileVault on Mac • Generate encryption reports to track policy enforcement and demonstrate compliance
Patch Management	MSPs mostly use disparate tools Windows patching and may use dedicated tools for 3rd party patching but they are often behind on patches because their tools are inefficient	• Easy manual and automatic vulnerability patching with scanning, scheduling, reports and option to postpone reboot • Largest database of Windows and 3rd party security and non-security patches • Fastest scan for missing patches, detailed and prioritized patch information
Email Security	MSPs rely on Microsoft's basic email protection but breach stats show it is not working, email is involved in 90+% of successful attacks. Proofpoint and Mimecast are two other competitors.	• Full security technology stack and unparalleled protection with multiple leading scanning engines to bloc advanced threats that basic email protection misses • Detects threats that don't involve malware such as credential phishing and impostor email preventing Business Email Compromise scams • At least as powerful and more cost-effective than Proofpoint or Mimecast.
Security for Virtualized Environments	Sometimes MSPs use solutions that are inefficient in catching threats or that are too resource intensive, impacting user experience and costs	• Optimized scanning and security for Virtual Machines without compromise in protection • Best performance for virtualized desktops or servers according to tests with independent benchmarking tool LoginVSI • Works with any hypervisor or cloud environment unlike competing solutions
Advanced Threat Security	Some vendors provide some fileless protection and cloud sandboxing with only one or two including tunable machine learning. Bitdefender includes all in one efficient product against advanced attacks	• Tunable Machine Learning prevention of advanced ransomware, fileless, and other attacks • Blocks PowerShell and other script based attacks, with proven efficacy (100% in AV-Comparatives advanced tests, December 2019) • Automatic and manual submission for to cloud-hosted sandbox for advanced analysis, threat context, and visibility
Endpoint Detection and Response	Specialized EDR vendors like Carbon Black provide powerful but more difficult to use capabilities, Webroot lacks EDR capabilities, others like Sophos provide unified AV and EDR	• Full visualization of security incidents revealing security gaps • Detects threats that manage to elude prevention layers and is easy to use, avoiding alert fatigue with alerts prioritized by risk level • Delivers in-depth visibility of suspicious activities, one-click resolution