Active Endpoint Cyber Defense
Prevention by Deception

Datasheet

https://deceptivebytes.com
company@deceptivebytes.com

	Deceptive Bytes	Other AVs
Deployment & Resources		
Installer size	1-1.2MB	100MB+
Install time	< 30 seconds	Minutes / Hours
Installation requirements	Same as OS	Usually higher
Installation dependencies	MS VC, .NET (part of the OS)	Depends
Full enterprise deployment	Minutes / Hours	Days / Weeks / Months
Manageability	Easy	Complex
CPU usage	< 0.01%	1-100%
Memory usage	< 20MB	100MB+
Disk usage	< 1.5MB installed ~10-50MB logs	1000+MB installed 100+MB logs
	Min. read/write ops	Constant access/scans
No. of processes	1 agent 1 UI (per user)	Usually 5-10, can reach 20-30+
Installed components (services, drivers, startup, COM, ...)	3	30+
Scans	Running processes	All Processes All File operations All Network traffic All Registry operation etc...
Operates from	User-mode	Kernel-mode & User-mode
Compatibility issues	None (automatically whitelisted your AV)	Existing
Updates	Rare	Constantly
Special CPU or processor features (Hardware requirements / limitations)	None	Depends
System stability	High	Depends (drivers increase the chance of Blue Screens)
Prevention & Detection		

Prevention rate	Min. 70% Usually 90+%	20-30% At best (estimated numbers)
Unknown & new threats	Min. 70%	Depends, mostly none
Sophisticated threats	Min. 70%	Depends, mostly none
Evasive malware	90+%	< 30%
False positives (F/P)	Minimum	Many
Detection rate	~50% (estimated)	< 30% at best
Incorporating 1 new threat behavior/pattern/signature to product	Stops potentially millions of future malware	Usually 1 sample up to a dozen from same family
Effectiveness	Very High	Very Low
Can be bypassed by malware?	Unlikely	Common
Operates during	All stages of an attack	A specific stage of the attacks, sometimes after the damage occurred
Additional		
Standalone, air-gapped systems	Yes	Usually no
Biased to small changes / errors	NO	Yes (ML/AI)
Proactive	Yes	No
Requires recovering data / system	NO (prevents in the first place)	Yes
Threat types	All, including Ransomware, CryptoMiners, APTs, Trojans, etc...	Most / All* (if they know them, or if it was calibrated to recognize them)
Virtual desktop infrastructure (VDI) environments	Supported	Limited at best, not resource friendly
Operational burden	Reduced	Remains / Increases
ROI	High - less operational burden, less F/P, less...	Low - still vulnerable, ...
Reduce bad reputation	Yes	Not necessarily
Required personnel	1 suffices	Min. 5-10 Dozens in large enterprises

DB vs. Network Deception

	Deceptive Bytes	**Network Deception**

Operates from	Endpoint / Device	Network
Type of operation	Agent	Agent / Most are agentless
Visibility over device	Full	Limited
Control over device	Full	Limited
Allows Lateral Movement	NO - prevented in the first place	Yes, to lure threats to a controlled server
Prevention / detection phase	From the initial reconnaissance of the environment	Only after a decoy was access / used (environment seemed legitimate to attack)
Uses decoys / honeypots	No	Yes
Effective against	All malware types (Ransomware, Cryptominers, Trojans, APTs, Viruses, etc…)	Mainly APTs and insider threats
Effectiveness	Very High (90+%)	Limited (threats might not look for their decoys or perform an initial reconn before attacking)

DB vs. Agentless

	Deceptive Bytes	**Agentless**
Operates from	Endpoint / Device	Network
Operates by	Agent	Utilizing existing OS services to operate*
Visibility over device	Full	Limited
Control over device	Full	Limited
Resource usage	Minimal	Minimal (via used OS services)
Exposes (encrypted) user credentials	NO	Depends on product
Always on protection	Yes	Yes*
Reduces operational burden	Yes	Yes*
Easy to manage	Yes	Yes*
Standalone, air-gapped environments	Yes	NO
Special hardware / CPU features	NO	Usually YES*
Just for VM or cloud environment	NO	Usually YES*
VDI environments	Yes	Yes
Effective against	All malware types, including fileless	Mainly file-based attacks (usually only checks file-related operations)

	attacks	
Effectiveness	Very High (90+%)	Depends on the back-end engine but usually Limited* (uses a regular AV on host server)

* (asterisk) means it still depend on the implementation and the dedicated (on-premise) server

DB vs. EDR

	Deceptive Bytes	**Endpoint Detection & Response**
Requires recovery	NO (prevented in-place)	Yes
Forensics capabilities	Yes (relevant only to the attack itself)	Everything, potentially includes private user data being sent to external/cloud servers
Resource friendly	Yes (doesn't scan everything, only relevant data, sends only detections / telemetry)	Less, scans everything and sends to management server (affects the endpoints and its server)
Depended on Endpoint protection platform	No	Yes
Depended on Patch management solution	No	Yes
Depended on Vulnerability management solution	No	Yes
Depended on Configuration management solution	No	Yes
Biased to small errors/changes	No	Yes
Operates from	User-mode	Kernel & User-mode
GDPR-compliance	Yes	Depends

* Some figures mentioned in the tables above are based on information published by the security vendors & assumptions of standard usage.