Deceptive Bytes

Prevention By Deception

Active Endpoint Cyber Defense

About Us

- ✓ Israeli company founded by cyber security experts
- ✓ Patented technology
- ✓ Worldwide Customers & Partners

Gartner COOL VENDOR 2019

"Cool Vendor in Security Operations & Threat Intelligence"

SC MEDIA

"This an effective, prevention-focused product that's easy to operate, understand, and manage."

CYBERTECH100 2022
www.CyberTech100.com

One of The world's most innovative CyberTech companies

DATA INTELLIGENCE

Key Player in the market Deception Technology

CBINSIGHTS

"One of the most promising Startups in cybersecurity"

MarketWatch

"Top Key Players in the Endpoint Protection Platform market"

Analytics Insight

"Top 10 most Innovative cyber security companies"

Existing Solutions & Their Challenges

Antivirus Software
(Signatures)

- ✗ Stops only 20-40% of malware
- ✗ Doesn't protect against advanced & unknown attacks
- ✗ Can be evaded or used for attacks
- ✗ Resource intensive

Machine Learning/AI (EDRs)
(Patterns/Abnormality)

- ✗ Resource intensive
- ✗ Prone to errors & biased info
- ✗ Many F/P alerts - burdens IT/security
- ✗ Requires highly skilled professionals to handle
- ✗ Requires EPP and Patch, Vulnerability & Config management solutions
- ✗ Focus on detection

Network Deception
(Honeypots/Decoys)

- ✗ Lure attackers to a controlled server
- ✗ Overshadows real assets & data
- ✗ Increased system maintenance
- ✗ Doesn't protect endpoints!
- ✗ Focus on detection
- ✗ Mainly designed for large enterprises
- ✗ Hard to prove value of the solution

We don't rely on any of their methods!

Disclaimer: changes from vendor to vendor

Malware Behavior

Very clever and evasive:

- Get current location
- Check environment information
- Avoid/evade AV/EDR engines
- Evade security systems & researchers

"98% of all malware is using at least 1 sandbox evasion technique"

SecurityWeek

"Evasive malware is [...] using as many as 10 or more different techniques"

Last Line

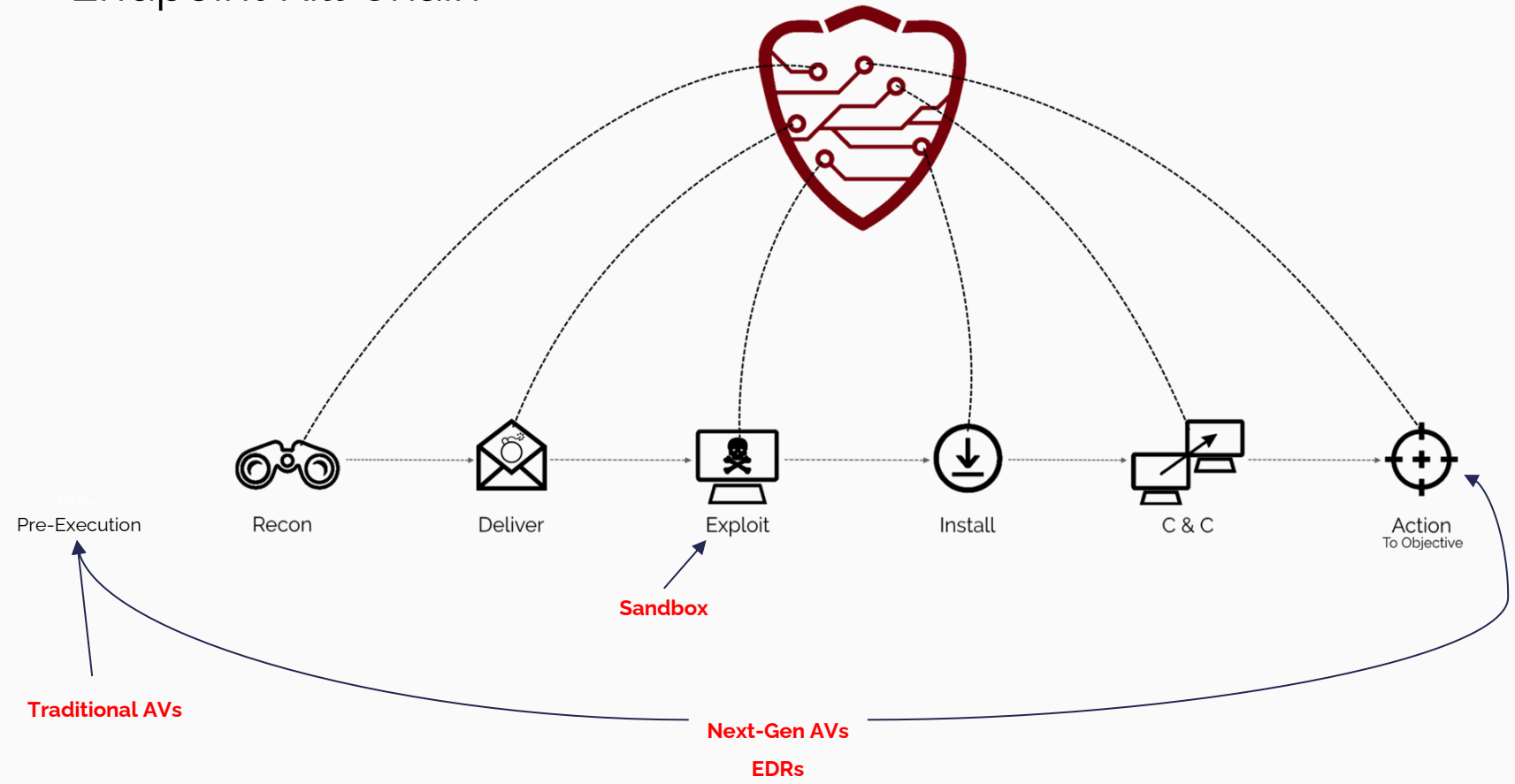
Our Deception Solution

Uses the same defenses & techniques malware is using against it

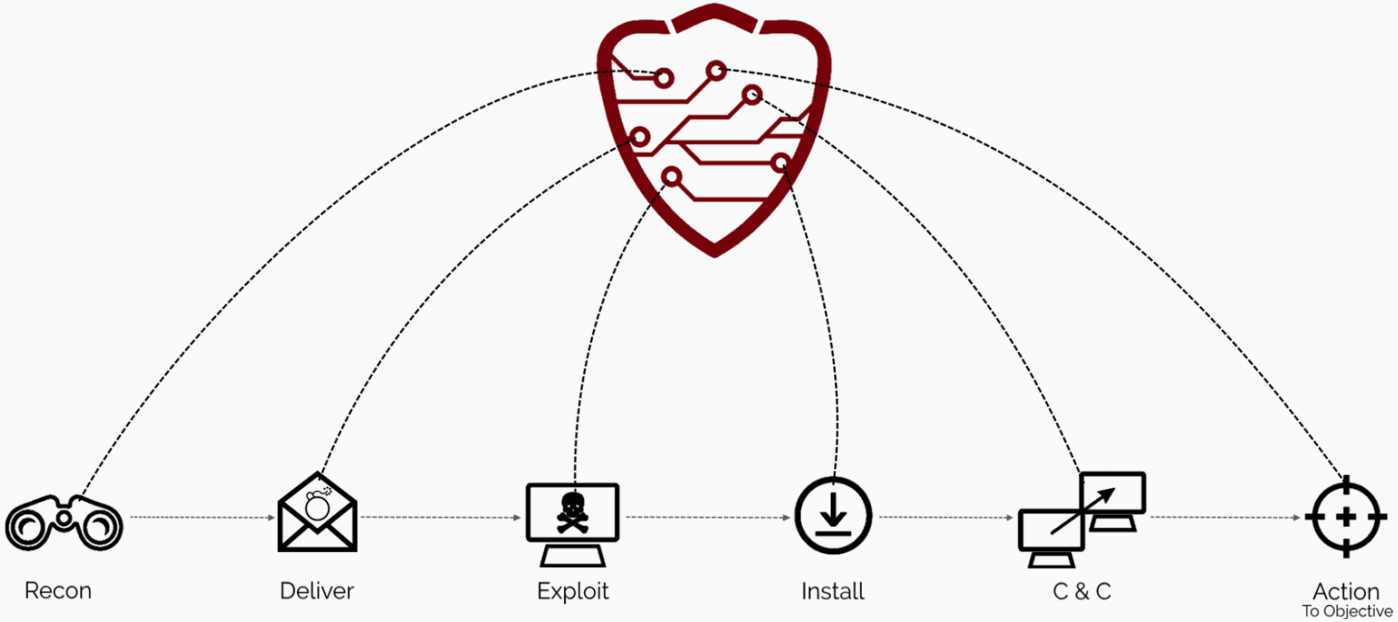
Shaping the attackers' decision making

Beating the bad guys at their own game

Endpoint Kill Chain



Endpoint Kill Chain



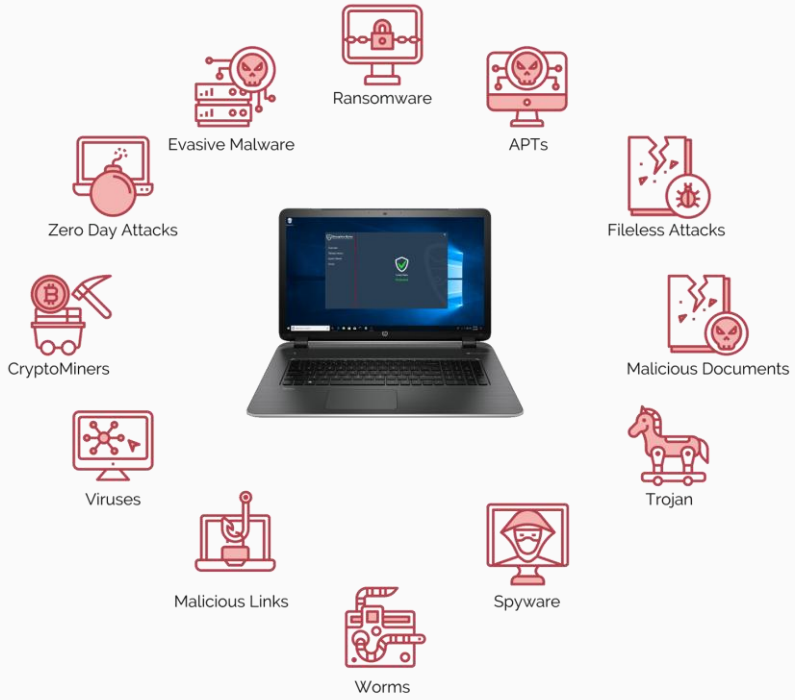
Providing multi-stage protection by

dynamically responding to threats as they evolve!

Solution Effectiveness

Effective against all types of malware

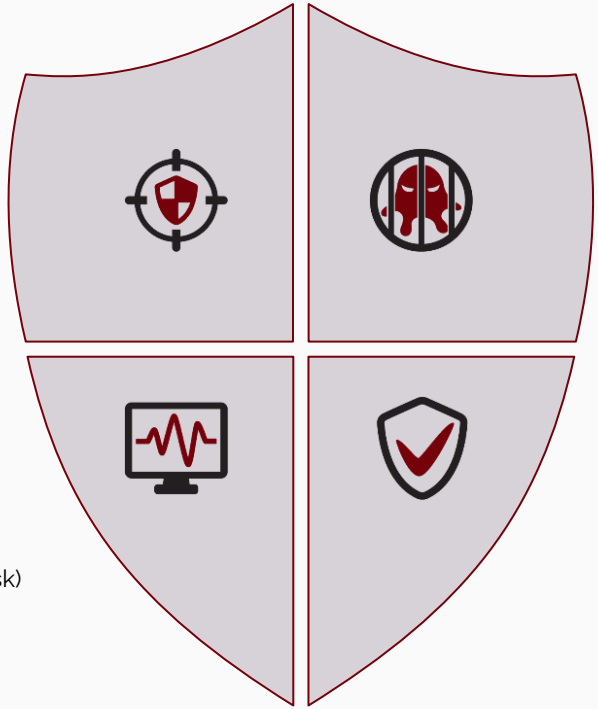
Over 99.9% success rate



Solution Advantages

Preemptive & Proactive

- Prevents unknown & sophisticated threats
- Very high prevention & detection rates
- Real time detection & response



Signature-less

- NO frequent updates
- Operates in standalone/VDI environments
- Stop millions of threats using only 1 evasion technique

Lightweight

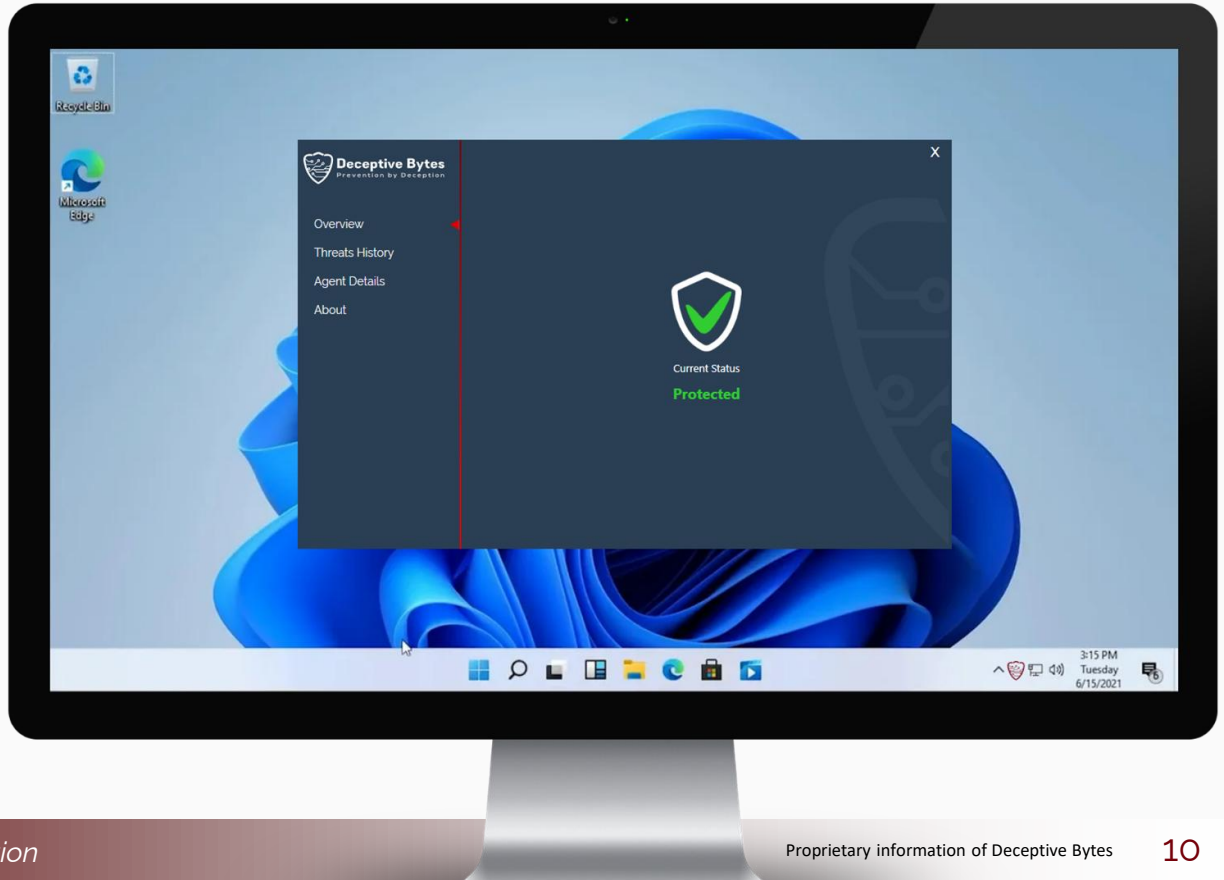
- System-wide protection with pinpoint handling
- Deploys in seconds (<1.5MB)
- Easy to operate
- Low resource consumption (CPU, memory & disk)

Reliable

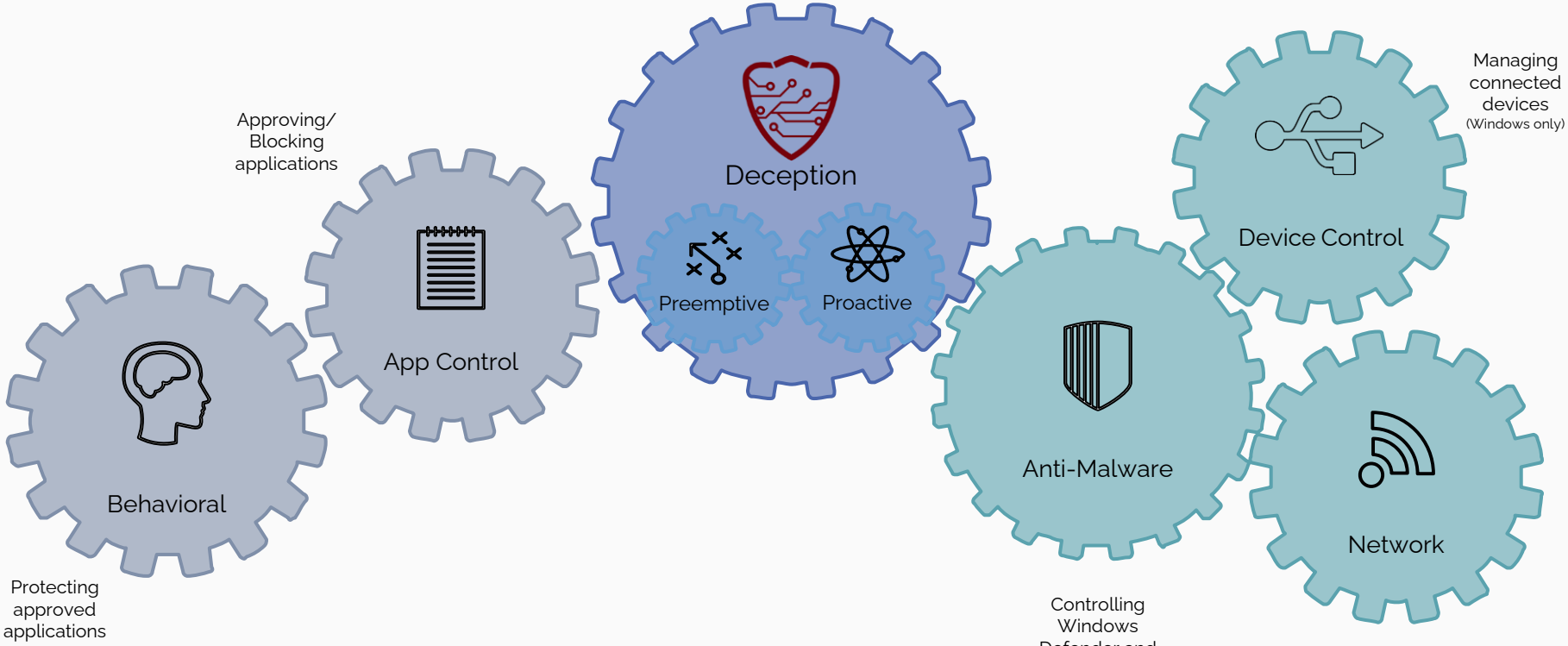
- Low to non-existing false positive rate
- High stability
- Operates in User-mode
- Automatically whitelist legitimate processes

Solution - End User Interface

- ✓ Extremely lightweight
  (<0.01% CPU, <20MB RAM, <1.5MB Disk space)
- ✓ Easy deployment – Install < 30 sec
- ✓ Operates immediately, no restart
- ✓ Signatureless (updates once in 3-6 months)
- ✓ User-mode (more stable, less vulnerable)
- ✓ Supports standalone & VDI environments
- ✓ Invisible to malware
- ✓ Co-exists with other security tools



Solution Capabilities



Solution - Management Server

- ✓ Easy deployment
- ✓ Remote solution deployment on devices
- ✓ Multi-tenant support
- ✓ On-premise / Cloud / Hybrid management
- ✓ Remote control over devices
  (WMI, PowerShell, WinRM/S, PsExec or SSH2)
- ✓ Live endpoint forensics (files, processes, etc..)
- ✓ Custom and automated reports
- ✓ 3rd Party Integrations

Solution Integrations

SIEM/LOG

ArcSight An HP Company
elastic
splunk>
QRadar
syslog-ng
ALIEN VAULT

Threat Intelligence

VIRUSTOTAL
OPEN THREAT EXCHANGE
HYBRID ANALYSIS

Sandbox

FIREEYE
McAfee
Symantec
cape
cuckoo
VMRAY
CROWDSTRIKE

Microsoft

Linux

Value Proposition

Organizations

- Protect against unknown & sophisticated threats
- Prevent damage to data & asset
- Reduce reputational risk
- Reduce operational burden

CISOs, IT Managers & MSSPs

- Automate responses against detected malware
- Adapt to changes in IT environments
- Reduce alerts & false positives
- Use built in security tools:
  Windows Defender & Firewall or
  Generic Linux AV & FW
- Operate in unpatched / vulnerable environments

C Level

- Improve employees' productivity
- Protect remote employees
- Reduce operational costs & resources

Deceptive Bytes

Thank you!

www.deceptivebytes.com

info@deceptivebytes.com

+1-844-806-9069

Deceptive Bytes

@DeceptiveBytes

Azrieli Holon Business Center, 26 Harokmim St, Holon, Israel

Customer Security Stack

	AV	AV + EDR	Deceptive Bytes & EDR	Deceptive Bytes & AV	**Deceptive Bytes & Windows Defender**
Prevention	Low	Medium	Very High	Very High	Very High
Detection	Low	High	Very High	Very High	Very High
Unknown Threats	Low	High	Very High	Very High	Very High
AVG Time to Detect	Slow	Medium	Very Fast	Very Fast	Very Fast
Update Rate	Very High	Very High	*Low	*Low	*Low
False Positives	Medium	Very High	Medium	Low	Low
IT Load	Medium	Very High	High	Medium	Low
Costs	$$$	$$$$$	$$$$$	$$$$	$$
ROI	Low	Low	Medium	High	Very High
					

* Refers to Deceptive Bytes only.