DECEPTIVE BYTES

Active Endpoint Cyber Defense

Prevention by Deception

Shaping the attackers' decision making
Beating the bad guys in their own game

"98% of malware use at least 1 sandbox evasion technique".
Malware is very clever and evasive, using different techniques to evade detection and analysis by security systems & researchers.

Deceptive Bytes uses malware own sophisticated defenses and techniques, against it.
By providing an Active Deception platform that responds to the evolving nature of advanced threat landscape and interfere with attackers attempts to recon & take hold of enterprise IT.

Preemptive Defense

Making malware believe it's in an unattractive/hostile environment to attack, reducing the malware motivation to attack and the chance of infection.
For example, creating detonation sandbox environment which deters malware.

Proactive Defense

Dynamically responding to threats as they evolve, based on the current detected stage of compromise and changing the outcome of the attack.
For example, deceiving & stopping Ransomware, thinking it succeeded encrypting files as the solution safeguard them.

We Help

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

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

C Level
- Improve employees productivity
- Reduce operational costs & resources
- Protect remote employees

Gartner COOL VENDOR 2019

"One of the most promising startups in cybersecurity"
CBINSIGHTS

Contact Us
company@deceptivebytes.com

Follow Us

Current Situation

One million new malware is created daily for espionage, theft, ransom and more, causing damages in billions of dollars.

CISOs and IT managers are overwhelmed by complex & costly deployments of endpoint security products, by alerts and information about attacks and by too many false positives (F/P).
Understaffed, they're unable to handle every alert and they're under heavy burden of operating such products, delaying in giving proper response time and fixing issues rose by various attacks.

See below how Deceptive Bytes helps tackle these issues with its Active Endpoint Deception platform

Dynamically responding to threats as they evolve and protecting through the entire Endpoint Kill Chain!

Preemptive & Proactive

Prevents unknown & sophisticated threats
The deception based solution uses common behaviors malware use against it and prevents threats without using signatures, patterns or prior knowledge

Very high prevention & detection rates
More than 98% of all malware use evasion techniques, deploying these techniques against malware helps increase prevention & detection rates substantially

Real time detection & response
The solution identifies malicious behavior during execution even if no evasion technique was used, stopping it as it happens

Lightweight

System-wide protection with pinpoint handling
The solution doesn't need to scan everything, it only handles unknown processes

Deploys in seconds
The thin agent (<1.5MB) deploys in seconds and operates instantly without rebooting

Easy to Operate
The solution operates automatically and doesn't require constant intervention, making it very efficient to operate

Extremely low resource consumption (CPU, memory, storage)
The solution doesn't impact user experience and uses <0.01% of CPU, <20MB of memory & <1,5 MB of disk space

Signature-less

NO constant updates
The solution doesn't need to be updated frequently since it uses common behavior malware use which doesn't update often

Can operate as stand-alone
No constant updates means that the solution can operate in air-gapped, isolated environments or by remote employees - keeping the endpoint secure

Stop millions of threats using only 1 evasion technique
Integrating 1 evasion technique can potentially stop millions of malware that use the same technique, even future ones

Reliable

High stability - operates in User-mode
The thin agent operates in user-mode, meaning it can't cause system failure or used as a point of entry to potential attackers & gain full access to the OS

Automatically whitelist legitimate processes
Making sure your environment is running smoothly, the solution automatically whitelists OS processes and other security solutions

Low to non-existing false positive rate
The solution creates various environments/tools against malicious behaviors, triggering high-fidelity alerts and reducing the F/P rate close to none