Deceptive Bytes

Active Endpoint Cyber Defense

Prevention by Deception

Datasheet

Current situation

It is estimated that 1 million new malware samples are created every day, causing damages to organizations & governments, interrupting business flow and increasing reputational risk with each attack.
This means defenders must be vigilant at all times and protected using a multi-layered approach across the organization.
Whether the defensive systems are antivirus/antimalware, SIEM, IDS/IPS, or EDR systems, today's cyber defenses suffer from a backward-looking pattern-definitions, and signature–matching design-construct.
The result: attackers are always ahead of defenders.

Why is that?

Malware authors know that once their malware is detected by various security systems, it becomes harder for them to achieve their intended target, meaning it's game-over!
So, malware is very clever and evasive, using different techniques to evade detection and analysis by security systems & researchers.
Recent research shows that *98% of malware uses at least 1 sandbox evasion technique*.
Every time that a malware sees such an environment, it knows it's being detected or investigated which causes it to stop its malicious activities in one way or another.
In Lastline's research on malware evasion techniques, it showed that most malware used at least 10 different evasion techniques to evade detection.

Shaping the attackers' decision making

Deceptive Bytes' patented technology is provided as a fully endpoint-centric deception platform that uses existing IT infrastructure, responds to the evolving nature of advanced threat landscape and interferes with attackers attempts to recon & take hold of enterprise IT, in a preventative solution which covers sophisticated malware techniques & defenses in several ways:

Preemptive Defense:
Making malware believe it's in an unattractive or hostile environment to attack, reducing its motivation to attack and the chance of infection.

Proactive Defense:
Dynamically responding to threats as they evolve, based on the current detected stage of compromise, and changing the outcome of the attack.

"Every day, new tactics and techniques are emerging, 'well established' attacks remain successful and the threat from cyber espionage continues to grow.

Deceptive Bytes' Active Endpoint Deception provides a means to shape attackers' decision making, manipulate their behaviors and ultimately disrupt their effort to attack organizations"

Deceptive Bytes
Prevention by Deception

Datasheet

Key advantages

- Very high prevention rates of unknown & sophisticated threats (in real-time)
- Extremely lightweight (<0.01% CPU, <20MB RAM & <1.5MB disk space)
- Fast deployment (<30 seconds)
- Auto-responds to attacks
- High-fidelity alerts (low to none F/P rate)
- Reduces operational burden & costs
- Multi-layered approach
- Easy to manage
- No constant updates & No signatures
- Operates in standalone/disconnected/VDI environments
- High stability - operates in user-mode

Key features

- Deception-based endpoint security
- Prevention first approach
- On-premise/cloud/hybrid deployment
- Multi-tenancy support
- Windows Defender & Firewall integrations
- Linux ClamAV & Firewall (UFW) integrations
- App control and automatic whitelisting
- Behavioral engine (Windows only)
- Device control - managing connected devices (Windows only)
- SIEM/Log integrations
- Threat Intelligence integrations
- Active Directory integration & AD-SSO
- Live endpoint forensics & control (Windows only)
- Multi OS platform support

Effective Against

- ✓ APTs
- ✓ Zero-Day attacks
- ✓ Evasive malware
- ✓ Viruses
- ✓ Ransomware
- ✓ Fileless attacks
- ✓ Malicious links *
- ✓ Worms
- ✓ CryptoMiners
- ✓ Trojans
- ✓ Malicious documents *
- ✓ Spyware
- ✓ And more...

* Protects: MS Office, browsers, email clients, etc...

About Deceptive Bytes

Deceptive Bytes, a leader in endpoint deception technology, provides its Active Endpoint Deception platform to enterprises & MSSPs which enables them real-time prevention of unknown and sophisticated threats. The solution dynamically responds to threats as they evolve, based on the current detected stage of compromise and changes their outcome, giving defenders the upper-hand in protecting their assets and data.

Recognized as a Gartner Cool Vendor in Security Operations and Threat Intelligence report.

Additional information

Website Email Phone LinkedIn Twitter

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