Deceptive Bytes
Prevention by Deception

Endpoint Cyber Defense

Prevention by Deception

Current Situation

An estimated 1 million new malware samples are created every day. The damages and workflow interruptions caused by malware impact organizations and government agencies with each attack. This means defenders must always be vigilant and protected, using a multi-layered approach across the organization.

Today's Cyber-Defense tools use pattern definitions and signature–matching design constructs.

The result: attackers are always ahead of defenders.

Why is that?

Malware uses clever and evasive techniques to avoid detection and analysis.

Most Malware use at least 1 Sandbox evasion technique and 10 other evasion techniques to elude detection. Once a Malware detects such an environment, it knows it's being monitored, and ceases its malicious activities, only to resurface and attack when it lands on a friendly network asset.

Shaping the Attackers' Decision Making

Deceptive Bytes' patented technology is provided as an Endpoint-Centric Deception platform. It uses existing IT infrastructure, responds to the evolving nature of the advanced threat landscape, and interferes with the attacker's attempts to recon, and control the enterprise. It does this by implementing a preventative solution that covers sophisticated anti-malware defense techniques:

Preemptive Defense

Making malware believe it's in an unattractive or hostile environment to attack, reducing its motivation to strike, 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.

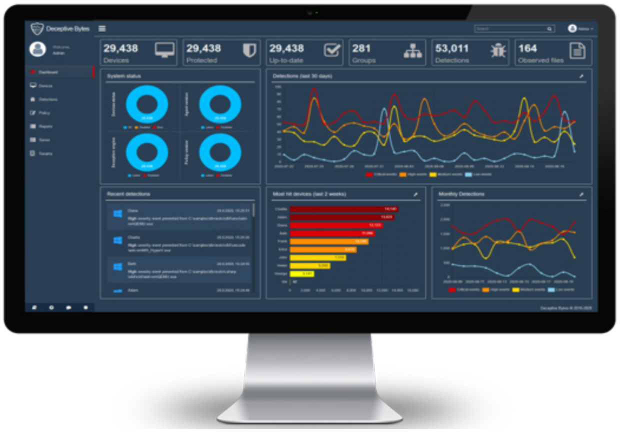
Deceptive Bytes
Prevention by Deception

BAVELLE TECHNOLOGIES

Deceptive Bytes Protects Against...

- ✓ APTs
- ✓ Ransomware
- ✓ CryptoMiners
- ✓ Zero-Day attacks
- ✓ Fileless attacks
- ✓ Trojans

- ✓ Evasive malware
- ✓ Malicious links
- ✓ Malicious documents
- ✓ Viruses
- ✓ Worms
- ✓ Spyware
- ✓ And more...



Deceptive Bytes Management and Monitoring Console

Key Advantages

- High, real-time prevention rates of unknown & sophisticated threats
- Lightweight (<0.01% CPU, <20MB RAM & <1.5MB disk space)
- Deployment within 30 seconds
- Auto-responds to attacks
- Low to no false-positive rates
- Reduces operational burden & costs
- Multi-layered approach
- Easy to manage
- No constant updates or 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
- App control and automatic whitelisting
- Behavioral engine
- Device control – managing connected devices
- SIEM/Log integrations
- Threat Intelligence integrations
- Active Directory integration & AD-SSO
- Live device forensics & control

About Deceptive Bytes

Deceptive Bytes provides an Active Endpoint Deception platform for Enterprises and MSSPs. The solution dynamically responds to threats based on the evolving stage of compromise by manipulating the outcome. This gives defenders the upper hand in protecting their assets and data.

Recognized as a **Gartner Cool Vendor** in Security Operations and Threat Intelligence, 2019 report.

Gartner
COOL
VENDOR
2019