DECEPTIVE BYTES
Distort Ransomware Perception

Datasheet

Current Situation

When an organization discovers a ransomware note demanding millions of dollars, it is not the beginning of the attack - it is the culmination of a much longer, covert process. The confusion and chaos at this moment often obscure the fact that the actual attack began long before the ransom demand appeared

Ransomware True Timeline

A ransomware attack unfolds over weeks or months, beginning with reconnaissance to identify vulnerabilities and initial access via phishing, exploit kits, or unpatched software. Attackers then establish persistence, escalate privileges, and move laterally across the network while exfiltrating data and disabling defenses. During this dwell time (often 90–180 days), they map critical systems, steal credentials, and prepare payloads. The final staging phase involves deploying ransomware, encrypting files, and triggering the ransom note-marking the attack's endgame, not its start. By the time demands appear, attackers have already compromised data, backups, and systems, leaving organizations to face operational paralysis, data leaks, and prolonged recovery

Think differently.
Protect proactively.
Stay ahead of the latest threats.

Preemptive defense: Create a hostile or unappealing environment for ransomware to operate, reducing its motivation and chances of infection.

Proactive defense: Continuously adapts the strategy based on the attacker's behavior, effectively countering evolving threats.

Multi-layered approach: Seamlessly integrate with your existing security stack, enhancing your overall defense posture and providing an extra layer of protection.

Never Let Your Business Down

How we do it

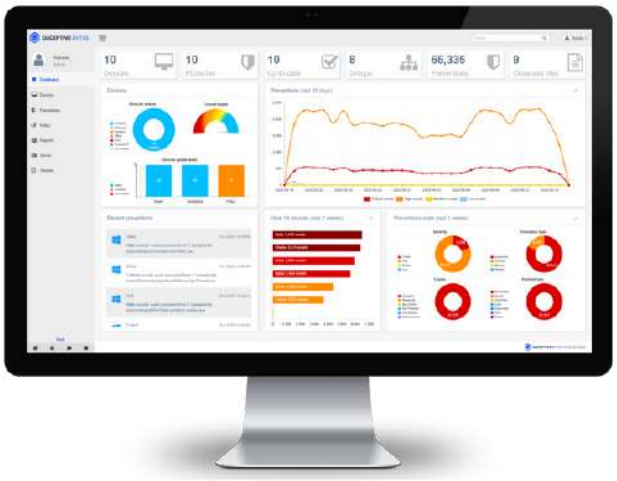
Create
Generates deceptive information to stimulate and trick the ransomware

Disrupt
Interferes with attackers' attempts to spy on and infiltrate the environment

Prevent
Manipulating the attacker's perception prevents the execution of malicious intent

Key Features

- Prevention first approach
- Business process protection
- On-premise, cloud and hybrid deployment
- Multi-tenancy support
- Anti-malware & Firewall integrations
- App control and automatic whitelisting
- Device control - managing connected devices
- SIEM/SOC integrations
- Threat Intelligence integrations
- Active Directory integration & AD-SSO
- Live endpoint forensics & control
- Operates in user-mode (high stability)



Key Advantages

- Patented technology
- Over 99.9% prevention rates of unknown threats
- 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 and VDI environments
- Multi OS platform support

Ransomware | APTs | Evasive Malware | Zero Day Attacks | Fileless Attacks

About

In today's rapidly evolving threat landscape, ransomware and advanced cyberattacks are becoming more stealthy and sophisticated, targeting vulnerabilities that traditional security tools often miss. Deceptive Bytes offers an innovative approach to endpoint security by turning ransomware's own evasive tactics against itself. Through its preemptive and proactive defenses, the solution distorts ransomware's perception of the environment, breaks ransomware logic and prevents attacks before they can even begin. This forward-thinking strategy not only reduces the risk of breaches but also ensures your business remains operational, resilient, and secure in the face of emerging threats - Never Let Your Business Down!

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

Never Let Your Business Down