Deceptive Bytes

Active Endpoint Cyber Defense

Prevention by Deception

How We Help
Protect Organizations

Current situation

It is estimated that 1M new malware samples are created every day, causing damages to organizations & governments, interrupting business flow and increasing reputational risk with each attack.
Security & IT teams are overwhelmed by complex & costly deployments and management of endpoint products, by alerts and information about attacks and by too many false positives.
Understaffed, they're unable to handle every alert given and they're under a heavy burden of operating such solutions (which mostly focus on detection), delaying in giving proper response time and fixing issues raised by various attacks.

Shaping the attackers' decision making, and helping reduce the burden

Deceptive Bytes provides 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.

How We Help

- The solution closes the security gap left by other security products that malware knows how to bypass (including AVs, Next-gen AVs & sandbox), making sure you're protected at all times.
- The solution uses the same defenses & techniques used by malware in a way that prevents the malware from attacking the system by creating a deception environment on the endpoint that is hostile to 98% of malware.
- The solution deceives malware during real-time attack attempts by changing the outcome, making the malware believe it was successful whilst safeguarding the organization's data and assets before any damage is done.
- The solution operates in user-mode, it reduces the potential attack surfaces on the endpoint and can not be used to breach the kernel of the OS.
- The solution can operate outside the organizational network & without the need for constant updates, helping you stay protected no matter where you are.
- The solution also uses a behavioral engine so the endpoint remains safe and protected during fileless attacks and even if common/whitelisted applications are used to attack it.

Website Email Phone LinkedIn Twitter

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

© Copyright of Deceptive Bytes Ltd., 2023 - All Rights Reserved