



# Deceptive Bytes integrates Microsoft Defender and Windows Firewall to its Active Endpoint Deception platform

TEL AVIV, ISRAEL, January 21, 2020 /EINPresswire.com/ -- [Deceptive Bytes](#), a leader in Endpoint Deception, announces today its 2020 release of its flagship Active Endpoint Deception platform with enhanced capabilities and integration to both Microsoft® Windows Defender Antivirus™ and Windows Defender Firewall™.

"Deceptive Bytes enables enterprises, SMBs and MSSPs to bolster their security with a lightweight solution that reduces operational burden & costs and false-positive alerts in an easy to operate solution." says CEO Sagi Lamay, "With the new release, Deceptive Bytes' platform does more than just close the gap left by other security products and tools, it allows customers to manage their endpoint security under our platform which integrates to other security systems such as SIEM, eliminating the need for complex, ineffective products."

Alongside Windows Defender & Firewall, the latest version utilizes the cloud to block millions of known threats, it improves the behavioral capabilities to stop file-less and other advance attacks and it enhances its Deception capabilities to stop the most sophisticated threats that are able to evade current security products & systems.

Deceptive Bytes' Deception platform received major updates as well with Live Forensics to analyze endpoints remotely, additional integrations to 3rd party systems, including threat intelligence and SIEM & logging servers, improvements to MSSPs management and additional improvements to existing functionalities such as reports and remote management. [View the announcement in our blog.](#)

**DECEPTIVE BYTES**  
CYBER SECURITY

### Deceptive Bytes Cyber Security

The image displays two screenshots of the Deceptive Bytes management console. The top screenshot shows the 'Policy for group: Global' settings, divided into 'Basic settings', 'Real-time protection settings', and 'Scan settings'. The 'Basic settings' section includes options for 'Enable Microsoft Defender', 'Show Defender UI', 'Potentially unwanted app' (set to Block), 'Enable Microsoft's cloud protection (Microsoft MSP)', and 'Enable block of first seen'. The 'Real-time protection settings' section includes 'Enable real-time protection', 'Monitor behavior', 'Monitor downloads & attachments', 'Monitor file access & programs', and 'Monitor processes'. The 'Scan settings' section includes 'Scheduled scan' (set to Daily), 'Update signatures before running scans', 'Use heuristic signatures', 'Scan results', 'Scan packed executables', 'Scan network files', 'Scan network drives (for full scans)', 'Scan mapped drives (for full scans)', 'Scan archives', 'Max. scanned archive size (in MB)', 'Max. archive depth', and 'Max. CPU % usage'.

### Deceptive Bytes' Microsoft Defender integration

The bottom screenshot shows the 'Corporate network settings' and 'Firewall rules' sections. The 'Corporate network settings' section includes 'Enable Corporate Firewall', 'Default inbound action' (set to Block), 'Default outbound action' (set to Allow), and 'Show interactive notifications'. The 'Public network settings' section includes 'Enable Public Firewall', 'Default inbound action' (set to Block), 'Default outbound action' (set to Allow), 'Show interactive notifications', and 'Block all inbound traffic'. The 'Firewall rules' section displays a table of rules:

Name	Local IP's	Local Ports	Remote IP's	Remote Ports	Protocol	Direction	App Name	Service Name	Profile	Allowed	Enabled	Description	Actions
fw1					TCP	Both			Public	Allowed	Enabled		[X] [E]
fw2	20.40.80.0/24		30.30.30.30		Any	Outbound			Corporate	Allowed	Disabled		[X] [E]
fw3	100.100.100.100		200.200.200.200		ICMP	Inbound			Public	Allowed	Disabled		[X] [E]
fw4	10.0.0.1		10.0.0.2		UDP	Both			Public	Blocked	Disabled		[X] [E]

#### About Deceptive Bytes:

Deceptive Bytes proactively prevents cyber attacks using deception technology on the endpoint. 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 & data!

Deceptive Bytes was recently recognized as a [Gartner Cool Vendor 2019: Security Operations and Threat Intelligence](#).

For more information, contact us or visit our website at [deceptivebytes.com](http://deceptivebytes.com)

Hen  
Deceptive Bytes  
+972 52-888-2356

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

---

This press release can be viewed online at: <http://www.einpresswire.com>

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases. © 1995-2020 IPD Group, Inc. All Right Reserved.