Futurism Managed Endpoint Detection Response (EDR)

Futurism

→ Did you know?

- More than 550,000 new pieces of malware are detected every day.
- There are now more than 1 billion malware programs out there!
- Every minute, four companies fall victim to Ransomware attacks.
- Trojans account for more than 50% of all computer malware
- 28 million mobile phones were attacked during the first half of 2020.
- 20 million IoT malware attacks were detected in the first half of 2020.
- More than 80% of organizations face difficulties in hiring and retaining skilled cybersecurity talent

Futurism's Managed EDR helps you to hunt down and stop threats before they begin and strengthen your IT security posture. EDR helps you block a wide majority of novel threats before they need any manual investigation. This leads to reduced workload and less noise for your security analysts and IT admins.

Powered by AI and Deep Learning, Futurism's EDR offers multiple layers of defense against:

- Known threats
- Unknown executables/threats
- Quarantine Ransomware before it runs
- Anti-exploits: File-less attacks
- Stop malicious encryption

EDR Service Built on the Strongest Protection Tactics

Predictive Security

- Stop unknown threats
- Block malware before it executes
- Prevent known and unknown malware

Anti-Ransomware

- File protection
- Isolate malicious processes
- Disk and boot protection

Anti-Exploit

- Exploit prevention against credential theft, code caving, macros, APC injection, etc.
- Block exploits and script-based attacks
- Protection against software vulnerabilities
- Stop real-world hacking techniques

Why Futurism EDR?

- Identify unauthorized chrome extensions
- Check device licensing and compliance
- Remotely access devices to remove unlicensed software or files
- Check failed login attempts
- Isolate devices and terminate processes as required
- Identify users that have clicked on suspicious link or phishing mail

Threat Hunting

- Identify processes that are trying to make a network connection on non-standard ports
- Find known vulnerabilities, outdated versions, bad certificates, etc.
- Identify detected IOCs mapped to MITRE ATT&CK
- Monitor processes that have recently modified files or registry keys
- Get details about PowerShell executions
- Identify processes disguised as services.exe
- Check for unusual login attempts
- Analyze cloud security groups
- Get detailed threat intel
- Close security gaps by determining root cause

Threat Response

- 24x7 human-led threat hunting
- Hunt potential threats and incidents
- Determine the scope and severity of threats
- Initiates actions to remotely disrupt, quarantine, and neutralize threats
- Security health check and activity reporting
- Synchronized endpoint security and visibility

+1(512)422-4868 www.futurismtechnologies.com