CONNECTWISE

Evolve to Next-Level Endpoint Defense

A hacker's first step is to find vulnerable endpoints to gain control of user accounts and credentials to access more valuable data. Appearing as normal user activity, malicious actions go undetected, increasing the likelihood of a disastrous data breach or business shutdown.

Hackers are adept at bypassing firewalls and signature-based antivirus

Too many organizations rely on traditional firewall and signature-based antivirus for endpoint security. With no ability to detect internal attacker movement, the risk of a data breach increases significantly. Organizations can substantially strengthen and deepen their defense with the addition of an endpoint detection and response (EDR) solution. EDRs record and store endpoint/system-level behaviors and use various data analytics techniques to detect a broader range of suspicious behavior. Once a threat is known, remediation measures may include isolating the machine in question and system rollback to a pre-attack state. Rich forensics provide visibility into how the threat occurred and insights for improving ongoing defensive measures. EDR should be part of any organization's progression for more complete endpoint security.

EDR detects and contains malicious endpoint activity other tools miss

Strengthen your defense for more complete endpoint security.

Join us for a live demo of EDR in action today!

ConnectWise | 4110 George Road, Suite 200 | Tampa, FL 33634 | 800.671.6898 | connectwise.com