Beyond Endpoint Protection
Remote Work Is the New Normal, Are Your Remote Endpoints Secure?

Security Incidents and Data Risk on the Rise

- In 2018 and 2019, 85% of DDoS impact shifted to endpoint. In the past year, 22% had more than five.
- FortiLabs: 85% of DDoS attack on remote corporate systems from June to December 2020.

Where Are Your Endpoints?

- 17% of monitors did most of their work remotely.
- 78% of monitors did most of their work remote.

Endpoints Are Weak Links

- Endpoints are attractive targets.
- 90% of all systems larger and phishing emails that can compromise to gain network access.
- More than 60% off-schedule data is stored at endpoints.

Endpoints are vulnerable

- 64% of monitors in 2019 incurred exploits (vulnerabilities).
- 13% of remote endpoints remain exploited for more than 30 days.
- 51% of compromise attacks happen through successful exploit.

First-generation EDR Falls To Defray Hidden Costs of Attacks

- Not fast enough
  - Real-time detection and first response.
  - Real-time remediation and containment.
- Costly remediation of remote endpoints
  - Real-time detection.
  - Real-time security analysis.
- Lost productivity
  - Real-time detection.
  - Real-time remediation.

The Answer: Endpoint Resilience Through Second-generation EDR

FortiEDR is a modern endpoint security solution with behavior-based prevention, detection, and response.

- Interactive behavioral environment — without stopping endpoint processes.
- Autonomous remediation model to speed to close.
- Automated isolation: to ensure your network environment.
- Proactive response to prevent targeted vulnerabilities.

To learn more Fortinet and FortiEDR can secure your remote workforce, click here.