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

Security Incidents and Data Risk on the Rise

In a 2016 survey, 65% of CIOs reported an increase in the past year, 25% for more than five years.

Publicly disclosed a record number of breaches in 2017, from July to December, 2017.

Where Are Your Endpoints?

Below COVID

17% of workers did most of their work remotely.

Since COVID

78% of workers do most of their work remotely.

Endpoints Are Weak Links

Endpoints are attractive targets

Endpoints are vulnerable

More than 90% of勒索软件 exploits endangers to gain network access.

46% of home networks in 2019 reported exploits leading vulnerabilities.

13% of remote endpoints remain exposed for more than 30 days.

51% of ransomware attacks happen through remote desktop protocols.

Endpoint attacks can move very fast

The North Korea attack launched a large cyberattack 1 hour before a server was exposed.

First-generation EDR Fails To Defray Hidden Costs of Attacks

Not fast enough

Vulnerability upgrades in remotes

Remotely detected and contained is often below 4 hours.

Costly remediation of remote endpoints

Remote users can lose an average cost of $217,000

76% of remote workers say working remotely increases time to identify and contain a breach.

Lost productivity

OT reveals the impact of endpoint attacks and “R and I productivity loss”

The Answer: Endpoint Resilience Through Second-generation EDR

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

Unleashed behavior-based protection without stopping endpoint processes.

Automated breach isolation and remote wipe, without impacting normal productivity.

Protection scores convey suspected vulnerabilities.

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

click here