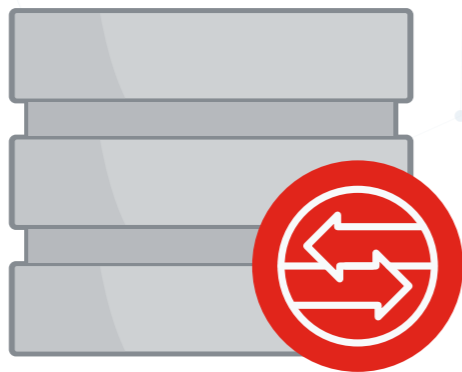# FORTINET®

BEYOND Endpoint Protection

Remote Work Is the New Normal
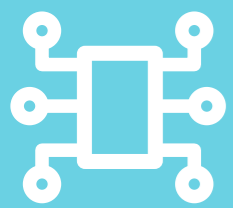## Are Your REMOTE ENDPOINTS Secure?

Security Incidents and Data Risk on the Rise

In a 2019 survey, **81%** of CISOs reported at least one intrusion in the past year; **22%** had more than five.[1]

Industry analysts saw a **600%** increase in phishing attacks in Q1 of 2020[2]

Where are YOUR Endpoints?

Before COVID

17%

of workers did most of their work remotely[3]

Since COVID

78%

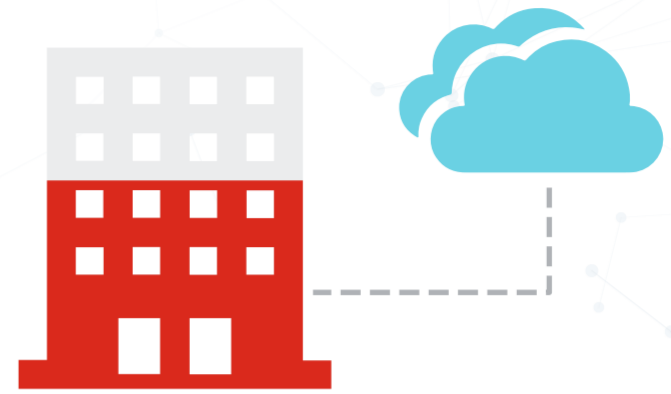of workers do most of their work remotely[4]

Endpoints are WEAK LINKS

Endpoints are attractive targets

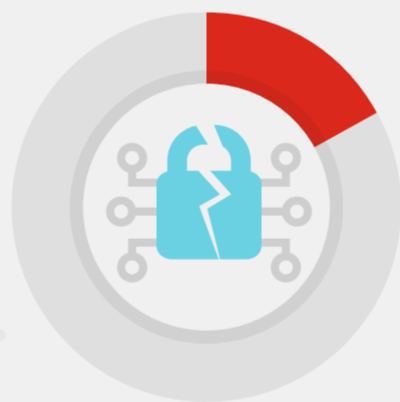More than **90%** of all breaches BEGIN WITH PHISHING EMAILS that steal user credentials to gain network access[5]

60% of corporate data is stored at endpoints[6]

Endpoints are vulnerable

60% of breaches in 2019 involved UNPATCHED VULNERABILITIES[7]
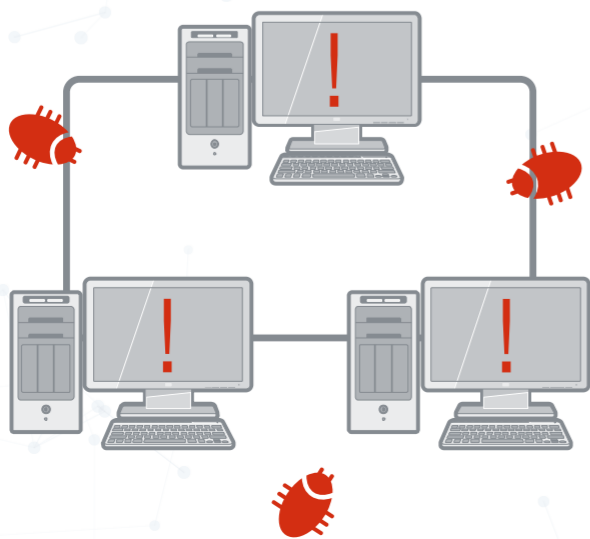
17% of remote endpoints REMAIN UNPATCHED for more than **30 days**[8]

57% of RANSOMWARE attacks happen through remote desktop protocol[9]

Endpoint attacks can move very fast

The *NotPetya* attack destroyed a large Ukrainian bank's entire network in **45 seconds**[10]

First Generation EDR Fails to Defray HIDDEN COSTS of Attacks

Response is **too slow**

Ransomware spreads in minutes

EDR's manual research and containment often takes hours

Remediation of remote endpoints is **costly**

Remote work increases average cost of a data breach by **$137,000**[11]

76% of remote workers say working remotely increases time to identify and contain a breach[12]

Productivity is **lost**

#1 economic impact of endpoint attacks: end-user and it productivity loss[13]

THE ANSWER: **Endpoint Resilience through 2ⁿᵈ Generation EDR**

FortiEDR is a next-generation EDR solution that automates real-time detection, containment, and remediation

☑ **Instantaneous detection**, **blocking**, and **containment** without disrupting endpoint processes

☑ **Full visibility** into contained incident for attack forensics

☑ **Automated roll-back** to a known good state eliminates lost productivity

☑ **Automated preemptive controls** eliminate unpatched vulnerabilities

To learn how Fortinet a FortiEDR can secure your remote workforce

click here

F⚡RTINET®

[1] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

[2] Sophie Dowdell, "600% increase in COVID-19 related phishing attacks," IT Security GURU, April 16, 2020.

[3] "CSO Pandemic Impact Survey," IDG, April 1, 2020.

[4] Ibid.

[5] Ironscales, "Email Security, 2017 Report," October 17, 2017.

[6] Rick Orloff, "Is GDPR-regulated data lurking in unexpected pockets of your organization?" Help Net Security, February 26, 2018.

[7] Filip Truta, "60% of Breaches in 2019 Involved Unpatched Vulnerabilities," Security Boulevard, October 31, 2019.

[8] "Organizations struggle with patching endpoints against critical vulnerabilities," Helpnet Security, March 26, 2020.

[9] Bill Siegel, "Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate," Security Boulevard, January 23, 2020.

[10] Andy Greenberg "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," WIRED, August 22, 2018.

[11] "Cost of a Data Breach report 2020," Ponemon Institute, July 29, 2020.

[12] Ibid.

[13] "The Third Annual Study on the State of Endpoint Security Risk," Ponemon Institute, January 2020.