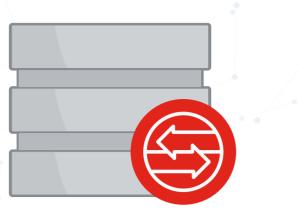


BEYOND Endpoint Protection

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 report at least one intrusion in the past year; **22%** had more than five.ⁱ



Industry analysts see a **600%** increase in phishing attacks in Q1 of 2020ⁱⁱ

Where are YOUR Endpoints?

Before COVID



of workers did most of their work remotelyⁱⁱⁱ



Since COVID



of workers do most of their work remotely^{iv}



Endpoints are WEAK LINKS

Endpoint are attractive targets



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



60% of corporate data is stored at endpoints^{vi}

Endpoint are vulnerable

60% of breaches in 2019 involved UNPATCHED VULNERABILITIES^{vii}

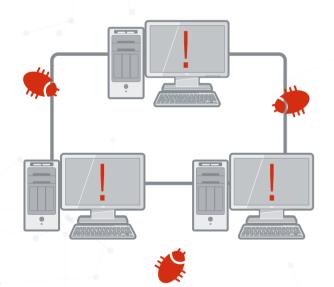


17% of remote endpointsREMAIN UNPATCHED formore than 30 days^{viii}



57% of RANSOMWARE attacks happen through remote desktop protocol^{ix}

Endpoint attacks can move very fast



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

First Generation EDR Fails To Defray HIDDEN COSTS of Attacks

Not Fast enough



Ransomware spreads in minutes



EDR's manual research and containment often takes hours

Costly remediation of remote endpoints



Remote work INCREASES AVERAGE COST of a data breach by **\$137,000**^{×i}



76% of remote workers say WORKING REMOTELY increases time to identify and contain a breach^{xii}

Lost Productivity



#1 ECONOMIC IMPACT of endpoint attack: END-USER and IT PRODUCTIVITY LOSS^{xiii}

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 and FortiEDR can secure your remote workforce.

click here



Source:

ⁱ "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.
ⁱⁱ Sophie Dowdell, "600% increase in COVID-19 related phishing attacks" IT Security GURU, April 16, 2020.
ⁱⁱⁱ "CSO Pandemic Impact Survey," IDG, April 1, 2020.
^{iv} Ibid.

^v Ironscales, "Email Security, 2017 Report," October 17, 2017.

- ^{vi} Rick Orloff, "Is GDPR-regulated data lurking in unexpected pockets of your organization?" Help Net Security, February 26, 2018.
- * Filip Truta, "60% of Breaches in 2019 Involved Unpatched Vulnerabilities," Security Boulevard, October 31, 2019.
- ^{viii} "Organizations struggle with patching endpoints against critical vulnerabilities," Helpnet Security, March 26, 2020.
 ^{ix} Bill Siegel, "Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate," Security Boulevard, January 23, 2020.
- * Andy Greenberg "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," WIRED, August 22, 2018.
- xi Penomen Institute, "Cost of Data Breach report 2020", IBM Security, July 29, 2020.

^{xii} Ibid.
 ^{xiii} Penomen Institute, "The Third Annual Study on the State of Endpoint Security Risk," Penomen Institute, January 2020.