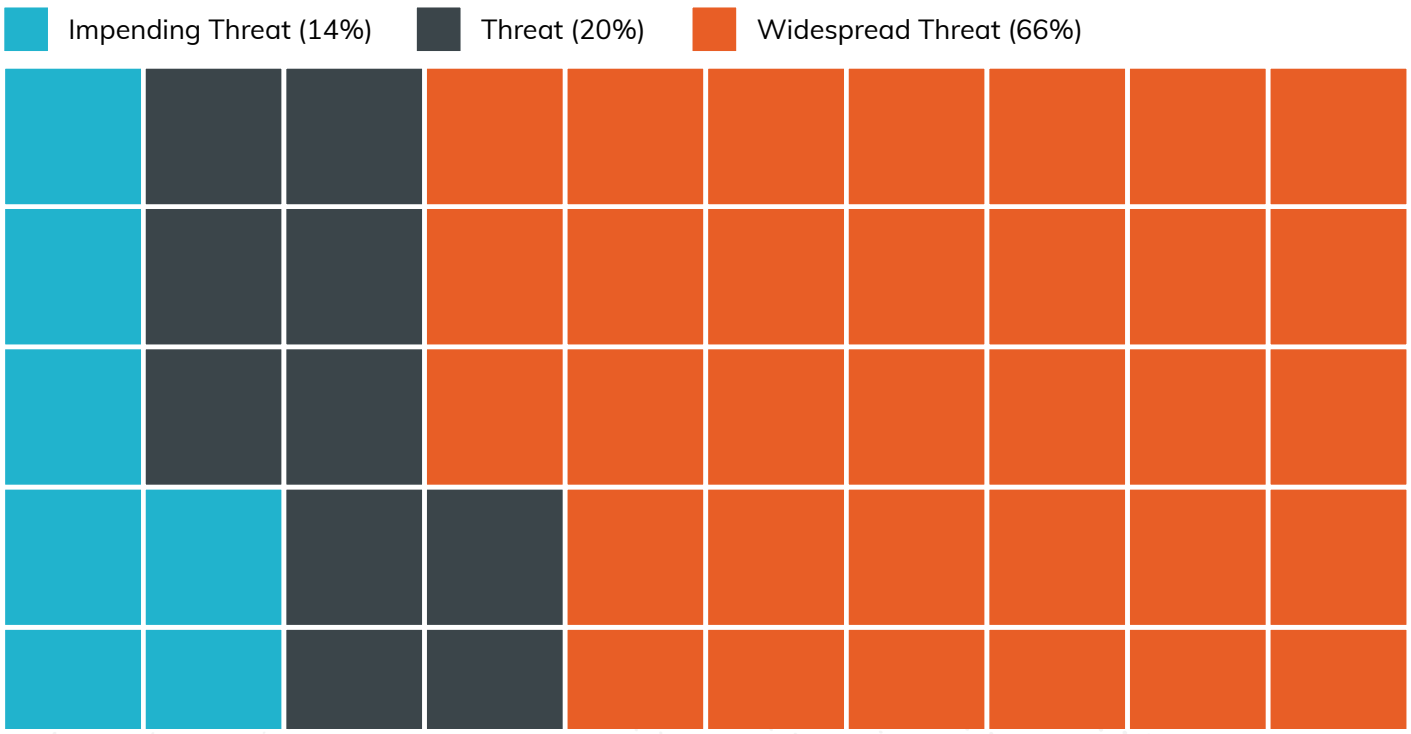
RAPID7

2021 Vulnerability Intelligence Report - The Difference A Year Makes

2021 was one of the most harrowing years on record for security teams. Starting with the remnants of the SolarWinds breach, it ended with Log4shell, one of the most far-reaching vulnerabilities impacting businesses. So how bad was 2021 exactly? If you look at the changes from the year before there are marked increases in some of the most important metrics we measure.

Below is a snapshot of the differences between the findings of the 2020 Vulnerability Intelligence Report and this year's report.

2021 VULNERABILITIES BY THREAT STATUS

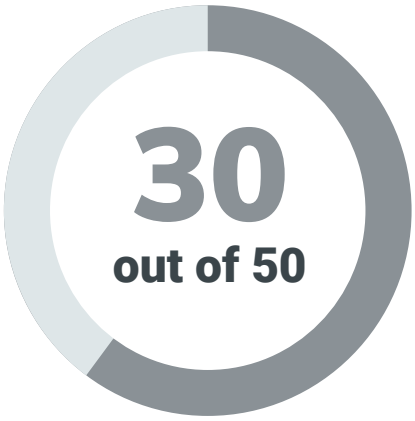


EXPLOITATION STATUS COMPARISON

2021

in report are
ACTIVELY exploited

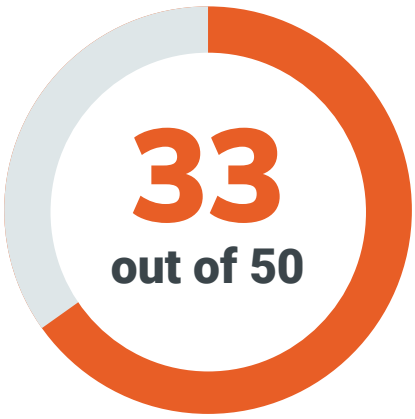
2020



in report are
ACTIVELY exploited

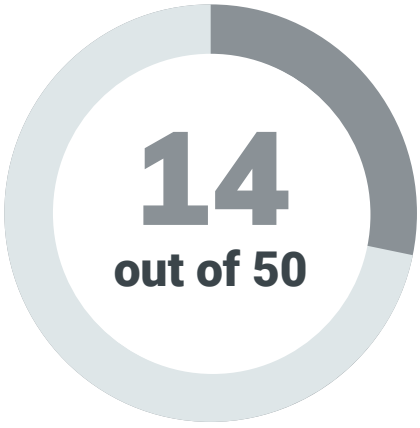
LEVEL OF EXPLOITATION COMPARISON

2021



in report are
WIDESPREAD exploitation

2020



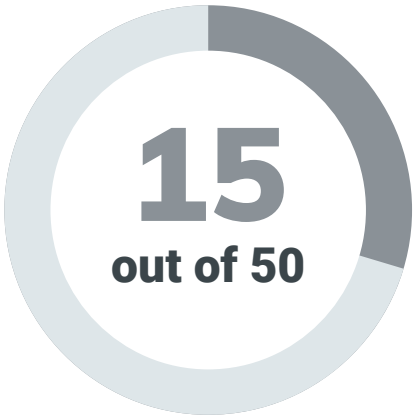
in report are
WIDESPREAD exploitation

TIME TO EXPLOITATION COMPARISON (7 DAYS TO BOOM)

2021

in report were exploited within
7 days of disclosure

2020



in report were exploited within
7 days of disclosure

THREAT TO AVERAGE BUSINESS

21
out of 33

of the 33 widely exploited 2021 vulnerabilities in the report (or just under two thirds) are known to have been **leveraged by ransomware groups**.

PERVASIVENESS OF VULNS IN POPULAR TECHNOLOGIES

7
out of 33

of the 33 widely exploited 2021 vulnerabilities in report are related to **Microsoft Exchange Server**

As you can see from these five key statistics, 2021 saw significant increases in some of the most important risk factors affecting your business. Download the entire report to get more in-depth investigation and analysis into 2021 and some guidance your teams can use to protect yourself in the future.

For the full Rapid7 Vulnerability Intelligence Report click here