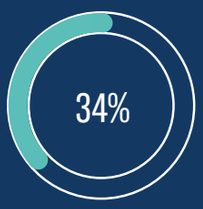
TODAY'S STATE OF VULNERABILITY RESPONSE

PATCH WORK DEMANDS ATTENTION

The severity and volume of cyberattacks continue to increase

15%
increase in cyberattack volumes over the last 12 months

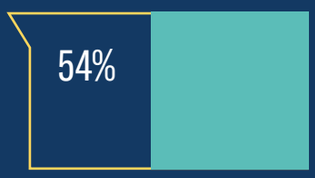
23%
increase in cyberattack severity over the last 12 months



34% of breach victims knew they were vulnerable before they were breached

57% of breach victims said they were breached due to a vulnerability for which a patch was available

Hackers are outpacing security teams



54% say attackers are outpacing enterprises with technology such as machine learning and artificial intelligence

37% of organizations that were breached don't scan for vulnerabilities

2 MILLION
global shortage of cybersecurity professionals by 2019*

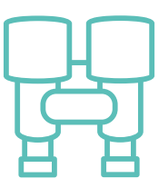
30%

cybersecurity jobs don't receive a single view online

50% headcount increase in the next 12 months

SECURITY'S PATCHING PARADOX:

Hiring more people does not equal better security



NO COMMON VIEW OF ASSETS AND APPLICATIONS ACROSS SECURITY AND IT

+

NO EASY WAY TO TRACK WHETHER VULNERABILITIES ARE BEING PATCHED

+

THINGS SLIP THROUGH THE CRACKS BECAUSE EMAILS AND SPREADSHEETS ARE USED TO MANAGE THE PATCHING PROCESS

=

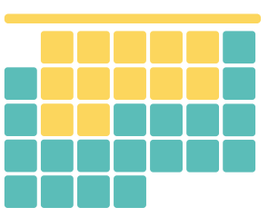
MANUAL PROCESSES AND SILOED TOOLS DELAY PATCHING

73%

62%

57%

12 DAYS



Time lost coordinating patching across teams

Learn how organizations avoid breaches.
Get the report: www.servicenow.com/lpayr/ponemon-vulnerability-survey.html

servicenow | Ponemon INSTITUTE