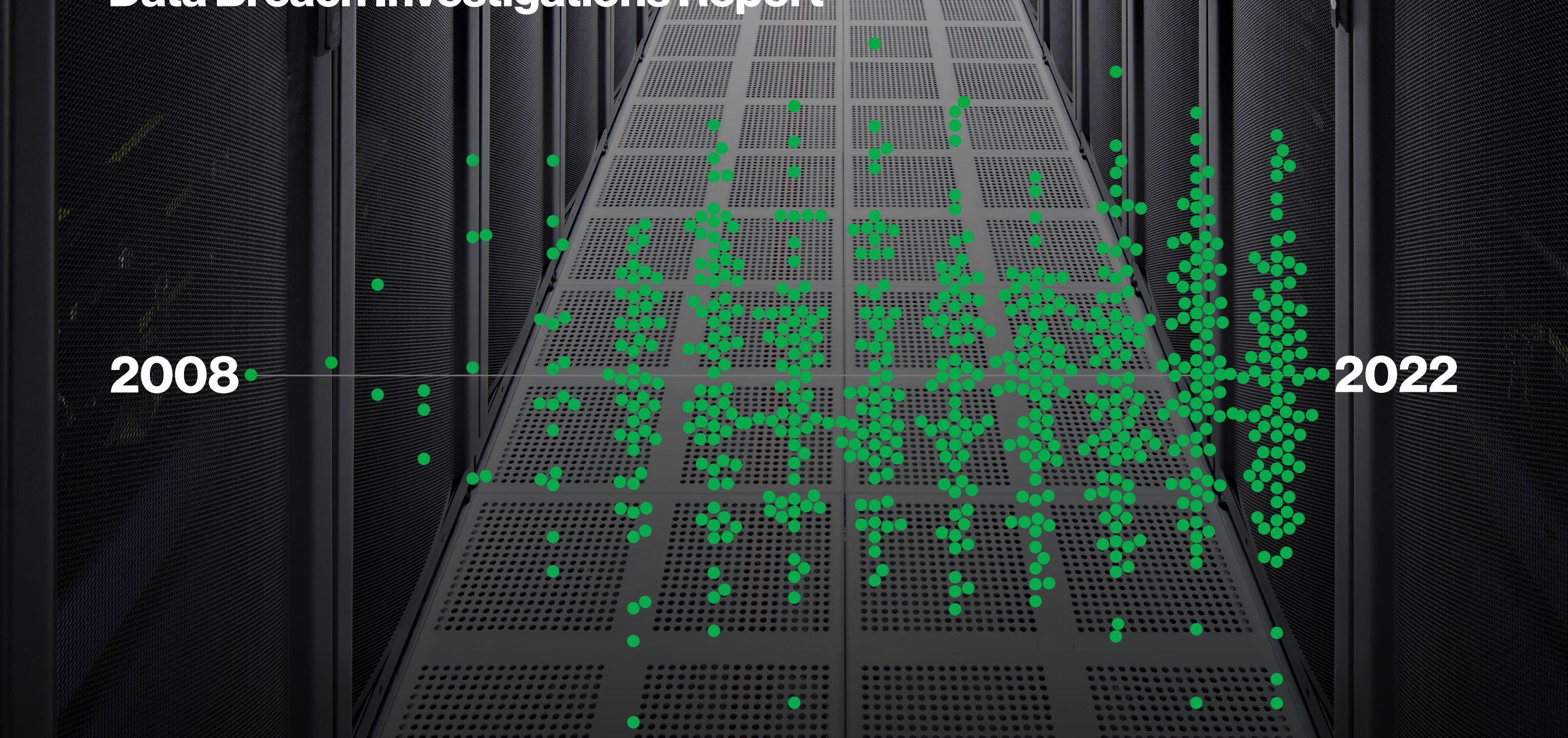
Arm yourself with information.

Key findings from the 2022 Verizon Data Breach Investigations Report



For 15 years, Verizon has been tracking data breach patterns. For the 2022 report:

5,212 breaches were analyzed.

23,896 security incidents were reviewed.

87 organizations contributed data.

What we found:

50%+ (0% 20% 40% 60% 80% 100%)
Over half of breaches involved the use of either remote access or web applications.

82% (0% 20% 40% 60% 80% 100%)
Most breaches, 82%, involved a human element.

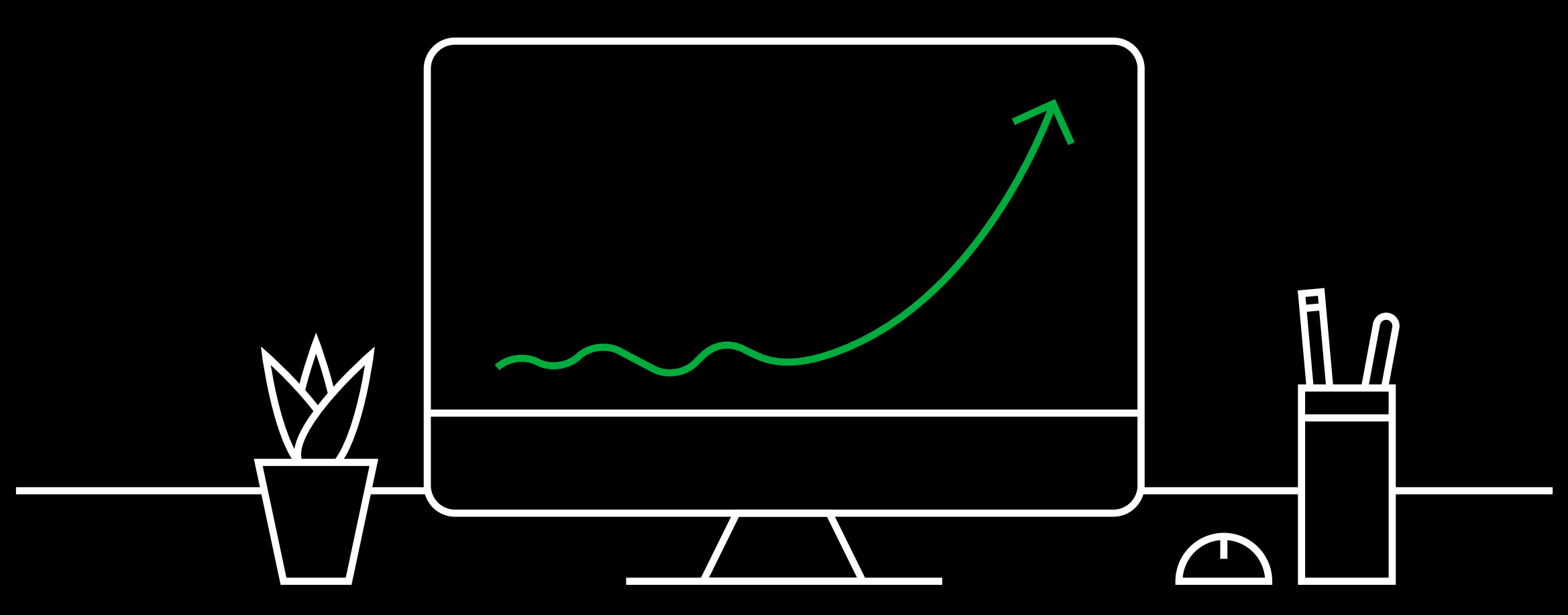
20% (0% 20% 40% 60% 80% 100%)
Social engineering was implicated in 20% of breaches.

62% (0% 20% 40% 60% 80% 100%)
Partners accounted for 62% of System Intrusion incidents, although this was mostly due to single supply chain breaches.

66% (0% 20% 40% 60% 80% 100%)
About two-thirds of breaches involved Phishing, Stolen credentials and/or Ransomware.

95% (0% 20% 40% 60% 80% 100%)
The vast majority of breaches had five or fewer steps.

Ransomware increased 13% over the previous year—a jump greater than the last five years combined.



The four key paths to data breaches are:

- Credentials
- Phishing
- Exploiting vulnerabilities
- Botnets

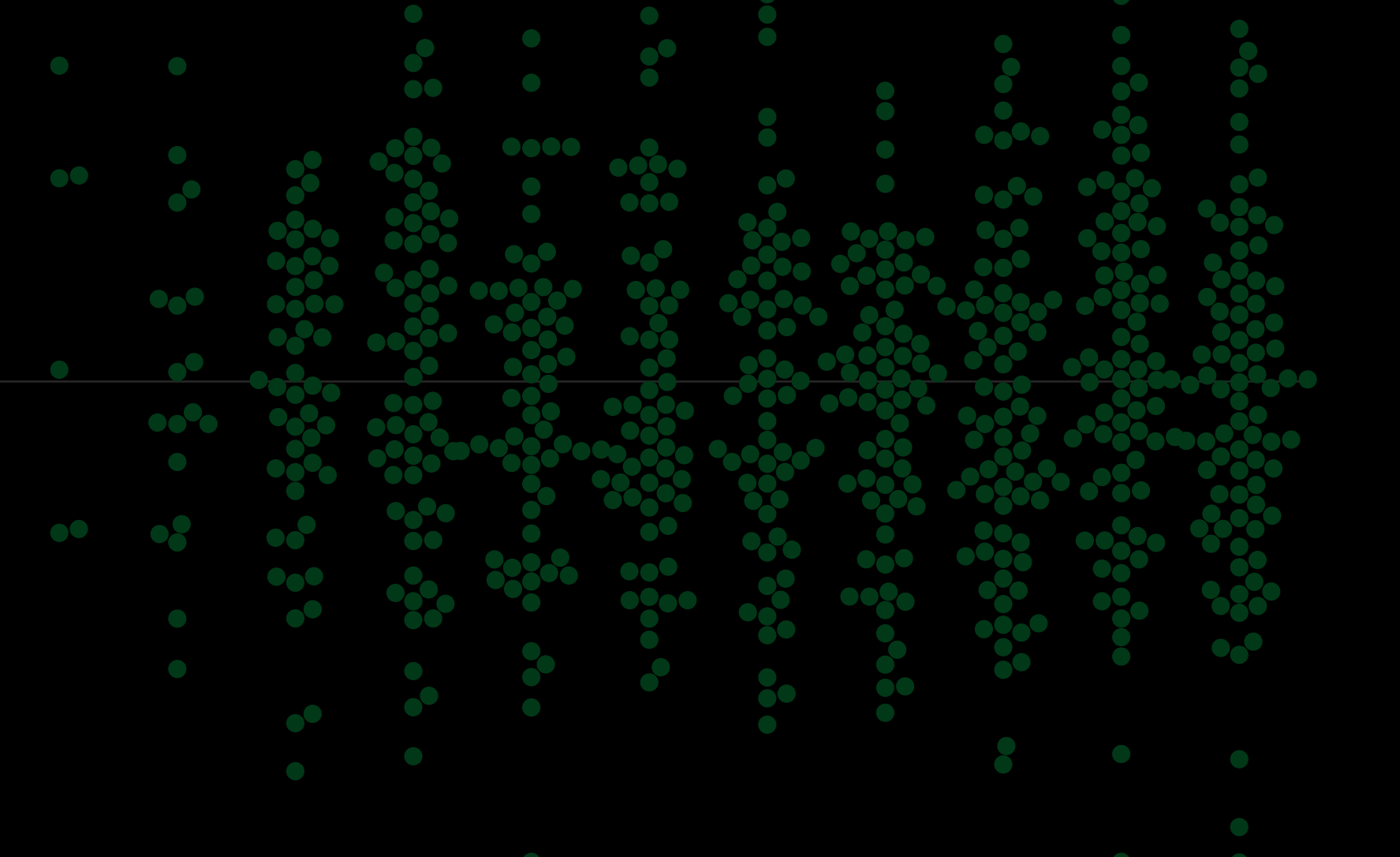
No organization is safe without a way to handle them all.

Who are the culprits?

4/5 — Almost four out of five breaches were attributable to Organized crime.

#1 — The number-one motive was Financial gain.

#2 — The number-two motive was Espionage.



Securing your organization is essential. The Data Breach Investigations Report is the right place to start.

For detailed analysis of the latest trends in data breaches, including spotlights on 12 industry sectors and four regions of the world, read the full 2022 Verizon Data Breach Investigations Report.

Read the report

verizon

Network details & coverage maps at vzw.com. © 2022 Verizon. INF2400522