# Our Products: **Security and Professional Services**

Security
Risk Assessment & Compliance

verizon business

# Security Overview

## Security Professional Services

### Security risk assessment and compliance

- Cyber Risk Programs
- Penetration testing
- Governance, risk and compliance
- PCI DSS
- Ransomware attack assessment

### Security strategy and implementation

- Operational technology security Assessment
- Data discover identification and security classification
- Attack detection assessment
- Incident analytics

### Mobile Security

- Mobility mgmt. and security
- Verizon Business Internet Security

## Security Monitoring and Operations

### Device health monitoring and management

- MSS-Premises
- Managed Detection and Response

### Advanced Threat Detection

- Managed Security Services-Analytics
- Advanced Security Operations Center

## Network and Gateway Security

### Security Gateway solutions

- Unified Security Solutions
- Virtual Networks Services - Security
- Managed Trusted Internet Protocol Services (Federal)

### Network defense

- DDoS Shield
- DDoS Shield for IDS

## Incident Response

### Incident Response planning

- Executive Breach Simulation
- Security Health Check
- Espionage Health Check
- Red Team Operations

### Cyber breach and IT investigations

- Computer Emergency Response Team services
- Threat Intel and Response Service
- Verizon Fraud Management Service
- Rapid Response Retainer

### E-discovery and litigation support

- eDiscovery Professional Services

# A comprehensive look at data breaches

18

years of the Data Breach Investigations Report

22,052

incidents reviewed in our 2025 report

139

victim countries identified

12,195

data breaches analyzed in our 2025 report

# Learn the hackers' playbook

Our 2025 Data Breach Investigations Report decoded more than 12,000 data breaches. Here's a snapshot of some of our most critical findings.

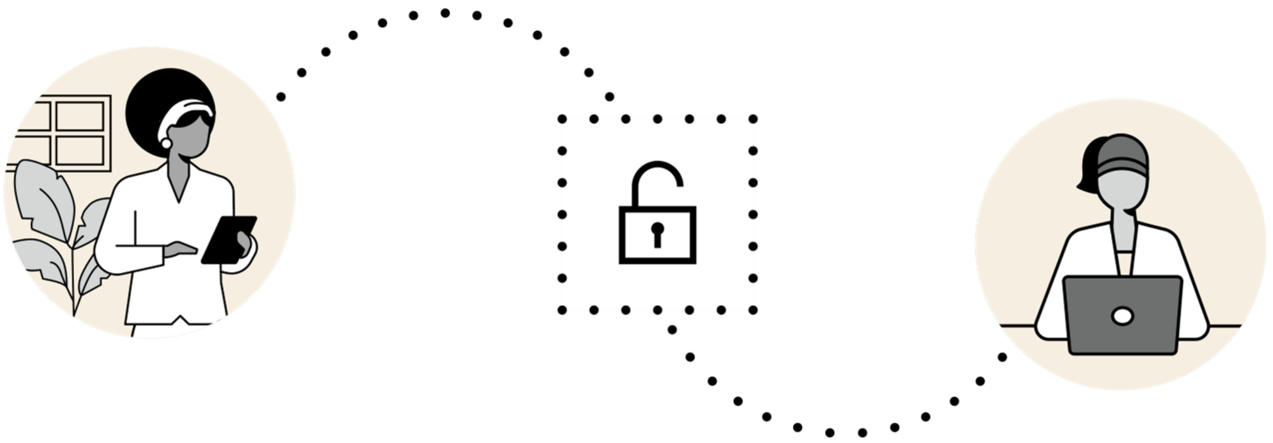
## Stack your cybersecurity knowledge.

34% ↑ **Exploitation of vulnerabilities as an initial access step for a data breach grew by 34%, now accounting for 20% of breaches.**

54% **Only about 54% of perimeter device vulnerabilities were fully remediated, and it took a median of 32 days to do so.**

60% **Human involvement in security breaches remained about the same as last year – 60%.**

15% **15% of employees routinely accessed generative AI platforms on their corporate devices – increasing the potential risk for data leaks.**



## Are you vendor vulnerable?

The percentage of breaches where a third party was involved doubled in the past year, from 15% to 30%.

Developing a unified cybersecurity posture with partners can help reduce vulnerability.

## Ransomware is on the rise.

44% of cybersecurity breaches involved ransomware, up 37% from last year.

## But ransom payments are down.

The median amount paid to ransomware groups was $115,000, down from $150,000 in last year's report. However, our 2025 report shows that most victim organizations – 64% – did not pay the ransoms.

# Our security insights are complemented by our expertise and experience.

## Global Visibility

- **9 security operations** centers around the globe
- **Insight** into a considerable amount of the world's IP traffic
- **61B security events** processed each year (average) to improve our threat library

## Deep Expertise

- **25+ years** of industry experience
- **12 years** of forensic investigations and security incident data
- **One of the world's largest teams** of PCI Qualified Security Assessors

## Security Intelligence

- **18 years** publishing the Data Breach Investigations Report (DBIR)
- **296K+** incidents and **10K+** confirmed data breaches analyzed by our RISK team
- World-class, global threat intelligence center

## First Hand Experience

- **2000+** retail stores in the US
- **116M+** wireless connections (pre- and post paid)
- Global IP network spanning **2700+** cities in over **150** countries across **6** continents
- **1.3B+** digital media users (Oath subsidiary)

verizon business