

# Small and Medium Businesses are Under Siege From Unprecedented Ransomware Attacks



**88%** Ransomware Targeted SMBs Dominantly



compared to

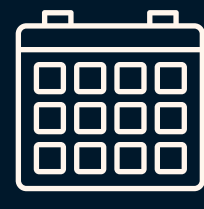


**39%** of attacks on large enterprises involved ransomware



**4X** Greater Risk

Small and Medium Businesses experience breaches at four times the rate of larger organizations.



**21** Days of Downtime

Average days of operational downtime following a successful ransomware attack.

## Primary Attack Vectors and Patterns



**96%** of all SMB Breaches Involve Three Primary Attack Methods:

These three attack methods account for 96% of all SMB breaches, combined.



**Compromised Credentials**

#1 - Dominant Method

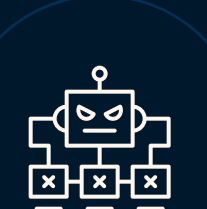
Stolen creds enable unauthorized access and long-term persistence



**Social Engineering**

#2 - Distant Second

Phishing and manipulation tactics are highly effective against SMBs



**Web Application Attacks**

#3 - Third Most Common

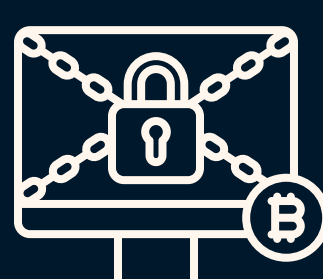
Vulnerabilities primarily exploited for initial access via weak or stolen creds

## SMB Industry Spotlight: Manufacturing Sector Hit Hardest



Manufacturing Security Incidents Up

**66%** ⬆️



Confirmed Ransomware Attack

**47%** ⬆️

Nearly half of all security incidents in Manufacturing involved ransomware

Key Tactics Used:

**34%**



USE OF STOLEN CREDENTIALS

**23%**



VULNERABILITY EXPLOITATION

**19%**



PHISHING ATTACKS

## Financial and Operational Impact



**99%**

**Profit-Driven Attacks**

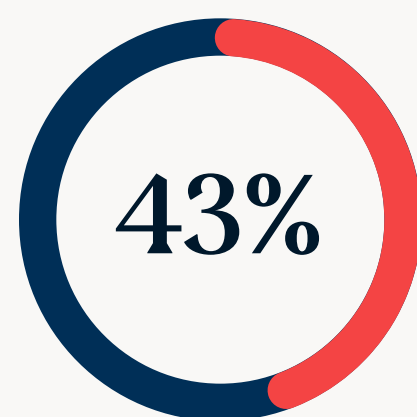
Nearly all breaches against SMBs are financially motivated by organized criminal groups.



**98%**

**External Threat Actors**

External threats dominate SMB breaches versus internal threats from employees.



SURGE IN INCIDENTS

**Supply Chain Risk**

Threat actors increasingly target large organizations through their SMB partners, making small business security critical to supply chains integrity.



BREACH RISK RISING

**Scale of Impact**

The majority of breaches impact SMBs with fewer than 1,000 employees, confirming no business is too small to be targeted.

**Most Targeted Data**



**Credentials**

User's login credentials and access tokens



**Personal Data**

Customer and employee information



**Internal Information**

Sensitive plans, reports, and emails

**The Human Element**



**60%**

OVERALL HUMAN ERROR



**18%**

SOCIAL ENGINEERING

VS

Social engineering remains one of the most effective ways attackers get through the door at SMBs.



**Don't Become Another Statistic**



**Get the Halcyon Advantage**

Get a demo of the Halcyon Platform and see how it is built for resource-constrained businesses, looking to eliminate the impacts of ransomware. Lightweight, effective, and affordable.

With ransomware attacks continuing to evolve, it is wise to invest and upgrade your cybersecurity solutions sooner rather than later. Get a demo of the Halcyon Platform and see how we can help you eliminate ransomware risk.

[Get a Demo](#)

[See Risk vs. Value](#)