Ransomware and the Cost of Downtime

By 2023, a business will fall victim to a **ransomware attack every 11 seconds.**

The Rise of Ransomware

2019 — **187 million** ransomware attacks

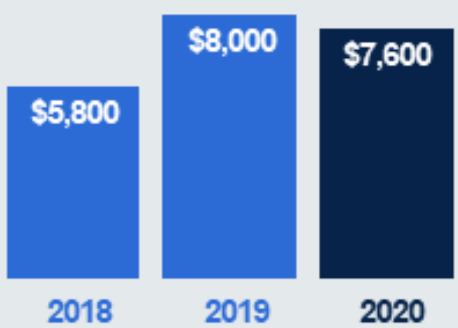
2020 — **188 million** ransomware attacks

In the first half of 2020, **ransomware attacks grew by 715%** as cybercriminals began exploiting the COVID-19 pandemic

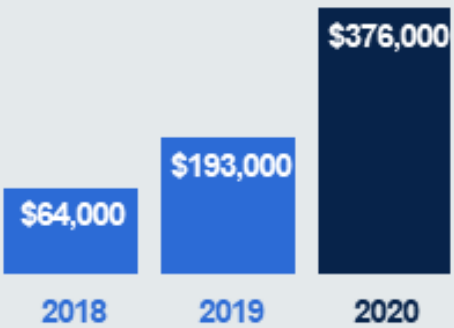
About **half of businesses worldwide** are hit by ransomware each year

Ransomware attacks are 2.5X more damaging than other cyber security incidents

Average global ransom demand



Average downtime cost as a result of an attack



Attacks are Getting More Sophisticated

Attackers **target and encrypt backup solutions** to increase the likelihood the victim will pay the ransom

New ransomware **exploits Wake-on-LAN** to power up more networked devices and increase its spread

Hackers target managed service providers (MSPs) to gain access to **multiple businesses in a single attack**

Downtime after an attack **can cost nearly 50X** more than the ransom itself

The True Cost of Downtime

After an attack, businesses must spend valuable time restoring their systems

Repairing networks

Restoring backups

Replacing lost devices

Downtime from ransomware is costly at up to $376,000

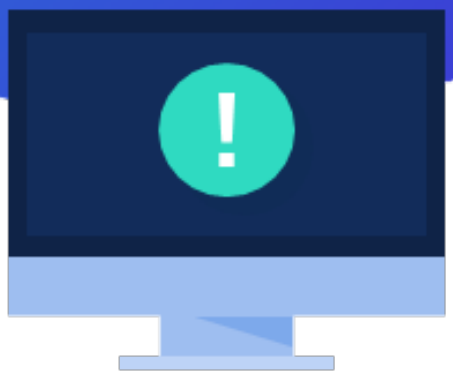
To Pay or Not to Pay - Either Means Downtime

of those who pay the ransom receive a decryption tool from the hackers

That means they still face costly downtime while decrypting their data - **4% never successfully recover the encrypted data**

of businesses take more than a week to recover from ransomware

For some, full recovery could take months



91% of MSPs say

clients with a business continuity and disaster recovery plan **(BCDR)** are **less likely to experience significant downtime from ransomware**

Business Continuity and Disaster Recovery (BCDR)

Why BCDR?
Comprehensive BCDR will:

- Reduce downtime during a security incident or emergency
- Quickly restore key information for minimal disruption
- Help maintain regulatory compliance
- Help you determine lessons learned after an incident

Key Features for Maximum Resiliency

Fast Failback
Uses a "Rescue Agent" for disaster recovery while performing a continuously-mirrored bare metal restore

Ransomware Detection
Automated post-backup ransomware scans and data and boot verification ensures you know as soon as ransomware is detected

Rapid Rollback
Allows incremental reversion to a previously-backed-up state without reformatting or re-partitioning

Two-factor Authentication
Secures a backup solution to prevent ransomware attacks from compromising data

Instant Virtualisation
Minimises downtime after an attack or outage, with virtualisation in the cloud or locally

Secure Cloud Backup
Offsite, secure, SOC2 compliant, geo-replicated cloud infrastructure enables fast and secure disaster recovery