

The True Cost of a Data Breach for Business

A breach will drain your data. But the devastation doesn't end there, it sinks leadership, reputation, and revenue.

Legacy security solutions (firewalls, endpoint tools, perimeter defenses) create a sense of protection, but they don't protect data itself. Attackers no longer need to break in to sink your business. With stolen credentials, they simply log in. But there is a way to stop them from exfiltrating your data and using it against you.

The obvious risks CXOs expect... but ignore

- Regulatory fines (GDPR, DORA, NIS2: up to 4% global revenue)
- Ransomware payouts
- Service downtime losses
- Customer churn

Below the Waterline The Hidden Costs

£1.9 billion

Did you know?

The recent cyber attack on Jaguar Land Rover is the most economically damaging cyber event in UK history, estimated to cost £1.9bn

Source: Cyber Monitoring Centre, 2025

Executive Liability

CEOs and CISOs face fines, lawsuits, even prosecution. Uber, Equifax, SolarWinds are proof.

Regulatory Enforcement

Audits, sanctions, and binding remediation orders that drag on for years.

Brand Reputation Collapse

Media backlash, stock price collapse, investor distrust.

Contractual Fallout

Breach of SLAs, lawsuits, and lost eligibility for government or critical contracts.

Compromised Backups

Corrupted data in transit infects recovery systems, crippling resilience.

Legacy Security Exposed

Firewalls and passwords delay, but don't stop attackers who simply log in with stolen credentials.

Quantum-Safe Security

Data stolen today will be exposed tomorrow. Without post-quantum readiness, your breach never really ends.

Did you know?

TikTok was fined €530 million by the Irish Data Protection Commission for breaching GDPR via unlawful data transfers

€530 million

Where Legacy Security Fails, Certes Protects

- Certes Data Protection & Risk Mitigation (DPRM) protects data in transit, not just the perimeter.
- Quantum-safe today, ensuring stolen data never becomes exploitable.
- Full key ownership ensures compliance with DORA, GDPR, NIS2, and CJIS.
- Certes makes stolen data worthless, even when attackers get inside.

88%

Did you know?

88% of breaches result from misused (stolen, weak, or compromised) credentials

Source: Verizon, 2025



Legacy security defends walls. Certes protects what matters – your data.