

WHY IT MATTERS

Most businesses discover their ransomware exposure after an attack. A few discover it before. The difference usually comes down to whether your defences were tested against how ransomware actually spreads, or just assumed to be sufficient.

WHAT RANSOMWARE ACTUALLY COSTS

01 Operational Downtime

Systems locked, files inaccessible, and staff unable to work, often for weeks, not days, while systems are rebuilt from scratch.

02 Financial Impact

Beyond any ransom demand, the real cost comes from lost revenue, incident response fees, and regulatory exposure if client data was involved.

03 Reputational Damage

Clients and partners remember how an incident was handled, long after the systems are back online.

HOW WE SUPPORT YOU

Design We assess your current defences against how ransomware actually spreads, and design a plan to close what's missing.	Operate We keep backups, monitoring, and response plans tested and current, so you're never improvising during an active incident.	Mature We extend coverage as your firm grows, adding continuous testing and monitoring only when the business is ready to sustain them.
--	--	---

READY BEFORE THE ATTACK

Recovering from a ransomware attack costs far more than preventing one. We assess your defences against how these attacks actually happen, and close the gaps while it's still your choice to do so.