CISILION

PILLAR 01 • TRUST

Cyber Security

Reduce cyber risk. Strengthen Digital Resilience. Earn trust.

We protect the identities, data, AI and infrastructure your business depends on – before, during and after an incident.

WHY THIS MATTERS

Cyber security is a business resilience issue: AI expands exposure, identity is the control plane and regulation raises the bar.

79% of security leaders report increased executive scrutiny of AI risk

Source: 1H 2026 State of AI and API Security Report

62% of breaches involve people, making identity and access controls more critical

Source: Verizon 2026 DBIR

WHERE THINGS GO WRONG

Risk without ownership

Security is fragmented across tools, vendors, teams and suppliers.

Identity and data exposed

Identity is the control plane for people, workloads and AI agents. Inconsistent, and ungoverned access controls amplify risk & exposure

Alerts without response

Too many alerts across disconnected tools overwhelm teams; skills gaps slow investigation and response.

Compliance without assurance

Point-in-time audits, testing and training do not demonstrate sustained digital resilience.

WHAT WE DELIVER

Protect the enterprise

Identity, endpoints, networks, cloud, data and AI secured as one estate.

Govern and assure

Risk-led strategy, architecture and controls aligned to ZTA and NIST CSF 2.0 Frameworks

Detect and respond

AI-assisted XDR, automation and 24/7 co-managed security operations.

Improve continuously

Posture, compliance and recovery measured and optimised over time with managed XDR.

WHAT GOOD LOOKS LIKE

- ✓ Clear ownership and outcome based cyber metrics
- ✓ Secure by design and secure by default
- ✓ AI agents, identities and data continuously governed
- ✓ Recovery plans tested; posture continuously evaluated
- ✓ Faster detection, containment and recovery with managed XDR

WHY CISILION

Risk-led resilience
Align investment to business risk, regulatory priorities and recovery outcomes.

Integrated security platforms
Unify Microsoft, Cisco and ecosystem controls while reducing tool sprawl.

One accountable partner
Strategy, delivery and 24/7 co-managed operations through one team.

Secure AI by design
Protect Copilot, agents, data and AI workloads from adoption onward.

Proven at scale
Security delivered across complex, regulated and hybrid estates.

CLIENT PROOF

INTERSOFT · WD-40 COMPANY · WARBURG PINCUS

Our 5-step approach

We reduce cyber risk across the full lifecycle — from strategy and controls to continuous detection and response.

STEP 01 **ASSESS** Identity, data, cloud and AI-agent risk assessment.	Cyber maturity, CE+ and regulatory readiness · Identity, data, cloud and AI-agent risk assessment · Penetration testing and control validation · 3rd-party, cryptographic, threat exposure review	**Outcome:** Board-ready view of material risk, resilience gaps and investment priorities.
STEP 02 **DESIGN** Define the target security architecture and roadmap.	Zero Trust architecture aligned to NIST CSF 2.0 · Control gaps, consolidation and target platforms · GRC operating model and recovery plans · Managed/co-managed runbooks	**Outcome:** Defensible target state with clear accountability, recovery objectives and an executable roadmap.
STEP 03 **DELIVER** Implement governance and controls. Simplify the estate.	Entra, Defender, Sentinel and Purview · Cisco XDR, Secure Access and AI Defence · Identity, endpoint, network, cloud and data controls · Platform integration, remediation and consolidation	**Outcome:** Reduced attack surface and tool sprawl, with secure-by-default controls across the estate.
STEP 04 **ADOPT** Secure, governance, accountability and responsible AI usage.	Executive risk reporting and communication · Role-based phishing and attack simulations · Responsible AI governance and guardrails · Security champions and response exercises	**Outcome:** A cyber-aware workforce with tested playbooks and clear accountability.
STEP 05 **MANAGE** Monitor, respond and improve resilience continuously.	24/7 co-managed SOC, SIEM and XDR · AI-assisted investigation and automated response · Continuous exposure and posture management · Platform, compliance and service optimisation	**Outcome:** Lower detection and recovery times, continuous assurance and predictable service resilience.

CLIENT PROOF

"Cisilion quickly understood the challenge, designed a solution that met our security requirements and delivered it within demanding timescales. The outcome has given us a secure platform we can confidently build on."

Mike Brown, IT Director
QA
Learn. To Change.

Start with a Cyber Resilience assessment

Prioritise risk, compliance and your route to Zero Trust

Book now