

Endace Consultancy from 2T Security

2T Security is a UK-based, NCSC-assured, independent security consultancy company with 10+ years of experience in deploying network visibility solutions across UK government.

Service description

2T Security delivers UK public sector-specific consultancy to design, deploy, and optimise Endace-based network visibility. We enable your SOC/DFIR team to pivot from alerts to packet evidence in <30 seconds at OFFICIAL and ABOVE classifications.

Capabilities

- Endace Deployment Architecture: Lossless capture at internet gateways, data centres, and cloud (AWS/Azure), without impacting performance.
- Data handling: Deployable in high risk environments and aligned to UK government data classification rules (OFFICIAL and above).
- Corelight & SIEM Integration: Seamless pivot-to-evidence workflows with one-click access, e.g., Splunk alerts to full packet history. Validated deployments in UK public sector.
- SOC/DFIR Enablement: Custom playbooks for UK use cases for threat-hunting, regulatory evidence, and NOC performance analysis.
- Compliance-Ready Design: Architecture documented to NCSC's Security Principles and UK public sector data handling standards.

Engagement Process

- Discovery & Scope: We deliver workshop(s) to understand your threat landscape, identify your critical networks to optimise the data acquisition strategy for maximum visibility.
- Design & Integration:
 - Design Endace placement
 - Integrate with your SIEM
 - Optimisation & Handover: Tune filters/retention to meet UK data retention rules
 - Co-create SOC playbooks with your Incident Response team
 - Formal handover with suitable documentation and a Knowledge Transfer workshop

Service benefits

- Eliminate "evidence gaps" in audits: accurate, lossless packet capture for evidence preservation
- Cut incident response time: Pivot to packet workflows with one click integrations from SIEM to PCAP, without having to download massive amounts of sensitive data
- Hardware precision and security: Tamper-Resistant Records with Nanosecond Time-stamping
- Appliance installation, configuration, and tuning done by experts

Security, data protection and compliance

All work is conducted in line with relevant UK public sector security policies and data protection requirements.