CSACyber | G-Cloud

CSA AppGuard ZeroTrust

CSA AppGuard ZeroTrust hardens endpoints and servers using application control, isolation and least-privilege policies to block untrusted execution, macro/script abuse and lateral movement. The service includes design, deployment, policy tuning and ongoing management, with telemetry integrated into your SIEM/SOAR for centralised monitoring and response.

Key features

- Zero-trust application control and process isolation
- Least-privilege enforcement; macro/script containment
- Policy design, baselining and continuous tuning
- Integration to SIEM/SOAR (e.g., Microsoft Sentinel) for alerting and correlation
- Health monitoring and exception management
- Rollout assistance, change control and governance
- Hardening aligned to NCSC/CIS benchmarks
- Operational runbooks and knowledge transfer

AppGuard gives your organisation proactive, kernel-level protection that stops malware at the source, eliminates alert fatigue, and enhances the performance and effectiveness of your SOC and endpoint estate. It's prevention-focused Zero-Trust model is simpler, lighter, and more reliable than traditional detection-based approaches.

References and case studies can be provided on request.

BENEFITS

- ✓ **Zero-Trust Endpoint Protection (Prevents Attacks Before They Execute)**
- ✓ **"Prevention Without Detection" (No Signatures, No Alert Fatigue)**
- ✓ **Strong Application Containment & Isolation**
- ✓ **Highly Effective Against Zero-Day, Fileless, and Advanced Attacks**
- ✓ **Ultra-Lightweight & Minimal Operational Overhead**
- ✓ **Complements Existing Security Stack (AV, EDR, XDR)**
- ✓ **Proven in High-Stakes Environments**

CREST Security Operations — Security Operations Centre
CREST Incident Management — Incident Response
CREST Security Testing — Penetration Testing
CREST Red Teaming — Intelligence-led Pen Test
CREST Security Testing — Vulnerability Assessment

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

Assured Service Provider
in association with National Cyber Security Centre
Cyber Incident Response: Standard Level

Cyber Essentials
Cyber Essentials Plus

hello@csacyber.com
csacyber.com
0300 303 4691