Security one-pager — Enterprise

Management-plane evidence and IdP integration

Trustholm Security One-Pager — Enterprise CISO

Headline: Management-plane evidence for privileged automation—beside your SIEM, not replacing it.

Why enterprise security teams care

- - Remote access tools correlated with 80% of ransomware incidents (At-Bay 2025)
- - RMM operational logs ≠ security audit for privileged actions
- - Third-party risk registers need reproducible vendor evidence

Three pillars

1. Integrity — Code signing policy before queue dispatch 2. Separation of duties — Submitter cannot self-approve (dual-custody) 3. Evidence — Security audit plane + Event Hub/DCR Sentinel sinks shipped

Identity & access

OIDC/SAML SSO, MFA, RBAC, JWT tenant binding (403 on mismatch)

SIEM handoff

- - Shipped: azure_eventhub / azure_dcr audit sinks, DCR template download
- - Backlog: Splunk/Datadog native sink templates

Honest gaps

- - Vendor SOC 2 Type II: observation in progress
- - WORM audit immutability: backlog

Links

Trust hub: https://www.trustholm.com/trust/for/enterprise SOC 2 framing: https://www.trustholm.com/compliance/soc-2-evidence