Security one-pager — MSPs

Supply-chain risk and customer audit resale

Trustholm Security One-Pager — MSPs & vCISOs

Headline: Govern privileged automation beside your RMM—prove script runs to insurers and end-customers.

Why MSPs care

- - 69% of MSP leaders reported 2+ breaches in 12 months (CyberSmart MSP Survey 2025)
- - Supply-chain attacks target RMM and remote access paths
- - End-customers and insurers ask for attributable script execution evidence

Three pillars

1. Integrity — Signed PowerShell policy; unsigned blocked when required 2. Separation of duties — Dual-custody (four-eyes) on by default 3. Evidence — Exportable audit; per-customer Sentinel routing for resale

Stack fit

Keep NinjaOne / ConnectWise / PDQ for endpoint management. Add Trustholm for script governance and audit export.

30-minute pilot

```
Install one agent → run one signed script → export audit CSV.
```

Honest gaps

- - Vendor SOC 2 Type II: observation in progress, not certified
- - WORM audit immutability: backlog

Links

Trust hub: https://www.trustholm.com/trust/for/msps Trial: https://www.trustholm.com/trial