SERVICE OVERVIEW

ProtectPro

Layered security with EDR, 24/7 SOC monitoring, and a stack no point-product matches.

KATALYST

Most organizations own security tools but never staff the security operations to watch what those tools generate. ProtectPro consolidates the sprawl — separate EDR, app-control and awareness-training subscriptions become one managed stack with a 24/7 SOC behind it.

Who it's for

- Organizations where security is on the table — compliance pressure (HIPAA, PCI, CMMC), an industry that's a target, or a recent incident or near-miss.
- Teams with no EDR or built-in antivirus only, or whose compliance and cyber-insurance requirements mandate SIEM and log monitoring, zero-trust controls, and access reviews.

What's included

- ✓ **Identity & access** — Entra ID hardening, Conditional Access, MFA, SSO/SAML
- ✓ **M365 governance** — Exchange Online, SharePoint, Teams, Intune, Purview DLP, Power Platform
- ✓ **User lifecycle** — onboarding/offboarding, licensing, password and MFA support, guest access, quarterly access and license reviews
- ✓ **Endpoint operations** — Autopilot/Intune provisioning, patching, software deployment with unapproved-software alerting, MDM for iOS and Android with remote wipe
- ✓ **Layered detection** — EDR, ITDR, Defender hardening with Safe Links and Safe Attachments, BitLocker, awareness training, and mandatory zero-trust application control on every endpoint
- ✓ **SIEM with weekly rule tuning** and 24/7 SOC oversight (our team + Huntress)
- ✓ **Full M365 backup** — mailbox, OneDrive, SharePoint, Teams — with point-in-time recovery
- ✓ **Network & server essentials** — firewall, switch, wireless and server OS patching and monitoring

What sets it apart

Blocked before it runs, not caught after. EDR responds once a process has executed; default-deny application control stops it running at all.

A SOC that is actually awake. A true SIEM correlates endpoint, identity and M365 signal with weekly rule tuning, and a 24/7/365 SOC contains confirmed threats whenever they fire — including the after-hours intrusion a business-hours model leaves until morning.

SERVICE LEVELS

Critical (P1)	**15 min · 4h fix**
High (P2)	**30 min · 8h fix**
Medium (P3)	**2 h · 16h fix**
Low (P4)	**8 h · 40h fix**

24/7/365. Fully-managed tier with a 24/7 SOC and on-call for production-down and active-incident events, with immediate escalation to a senior engineer.

TOOLS WE DEPLOY

Huntress EDR, ITDR, SAT and SIEM — detection, identity, training, log correlation

ThreatLocker — zero-trust application control

Microsoft Defender — endpoint AV

NinjaOne — monitoring, patching, inventory, remote support

HaloPSA — ticketing, SLAs, asset and change control

Auvik, Rewst and CIPP — network monitoring, operations automation, M365 management at scale

WHAT WE NEED FROM YOU

Microsoft 365 Business Premium at minimum. We integrate and manage the security stack — Defender for Office 365 P1, Defender for Endpoint P1, and Intune — and can't deliver without it.

Google Workspace customers keep Workspace but must add Microsoft 365 security & mobility licensing so we can run those components.

30-Day Satisfaction Guarantee

If the first thirty days don't meet what we committed to, you are not locked in.

WHERE PROTECTPRO SITS

CloudStart › SafeStart › **ProtectPro** · everything in SafeStart, plus a real security stack

Find out what your current tools would miss tonight.
Book a call: katalystng.com/schedule-a-call/

katalystng.com · 704-790-4440
Your Digital Operations Partner