Guardian Fundamentals for Professional Services Firms

Flat-rate IT, sub-1-hour critical response, and a documented security posture that lets you bill clients, answer questionnaires, and renew cyber insurance without scrambling.

The business problem: Your firm sells expertise and trust, billed by the hour. Every minute your team fights with technology is unbilled time. Every outage hits a deadline. Every client questionnaire arriving in your inbox asks security questions you have not documented. Cyber insurance renewals get harder each year. And the firms that scramble through all of that are the ones quietly losing engagements to peers who can answer those questions in writing.

The PTS answer: Guardian Fundamentals is our flat-rate managed-services tier built for billable-hour businesses. One monthly fee, sub-1-hour response on critical issues, a documented security baseline aligned to CIS Controls v8.1 IG1 and IG2, and the answer set your team needs when a client sends a vendor security questionnaire or a cyber insurance renewal lands on the managing partner's desk. **Predictable cost, sub-hour response, and a security posture you can put in writing.**

THE SOLUTION

Why Guardian Fundamentals

Fundamentals is the Guardian tier built for the firms where every minute matters and every client wants their data handled with documented care. Six capabilities make the difference:

- **Sub-1-hour acknowledge, sub-8-hour on-site, flat monthly fee.** When email goes down before a client presentation or the file server crashes during a project deadline, the clock starts the moment you call. Predictable cost, no hourly billing debates.
- **Microsoft 365 Business Premium with MFA and SSO baseline.** Phishing-resistant MFA across email, VPN, file storage, and client portal access. Single sign-on through Entra ID. The control set cyber insurers now require for any renewal.
- **Encrypted file storage and secure client document workflows.** BitLocker on every endpoint, M365 file encryption, secure external sharing, audit log of who accessed which client file and when. The answer to half of every client questionnaire.
- **Image-based cloud backup with PTS-tested monthly restore.** Cloud backup is table stakes. Restore testing is not. We perform and log a restore every month so a ransomware event is a recovery exercise, not a firm-survival crisis.
- **Documented WISP and Incident Response Plan.** Written Information Security Program tuned to professional services. Named partner-level IR liaison. Decision tree for breach notification, client communication, and cyber insurance activation. The document a client questionnaire actually asks for.
- **Annual phishing training, simulation, and BEC-aware staff drills.** Business Email Compromise (BEC) wire fraud is the single largest loss category in the FBI IC3 report. Monthly phishing simulations, annual training, BEC red-flag playbook for finance and admin staff.

WHAT YOU GET

Inside the Fundamentals tier

A single managed-service bundle that delivers the help desk, security, backup, M365 cloud, and IT leadership your billable-hour business depends on. Flat monthly fee. No hourly billing. No scope debates.

Service Layer	What you get
Help Desk	Remote, on-site, and emergency support within monthly limits. Acknowledge under 1 business hour, on-site under 8 business hours. 25% discount on after-hours emergency. Real engineers who know your environment, not a call center.
Cybersecurity	Advanced endpoint detection and response, 24/7 managed detection and response, phishing simulations and training, DNS filtering, full-disk endpoint encryption, BEC-aware finance and admin training, basic SIEM monitoring.
Backup	Image-based cloud backup (workstations and servers), monthly restore testing performed and logged by PTS, ransomware recovery runbook. Optional air-gapped server backups available on Co-Mgd and Compliance tiers.
Cloud (M365 Business Premium)	M365 Business Premium licensing, Entra ID conditional access, phishing-resistant MFA, encrypted email and file storage, Message Encryption for client communication, DNS and domain management.
IT Leadership	Quarterly business review, PTS firewall and network standards, vendor and SaaS inventory, AUP and WISP policy templates, IR Plan scaffold, client questionnaire response support, cyber insurance renewal evidence package.

Why one flat-rate bundle, not piecemeal

Most professional services firms accumulate a stack: a break-fix IT guy, an antivirus subscription, a backup tool no one tests, a free MFA app on the email and nothing else, and a WISP someone downloaded once and never finished. Guardian Fundamentals replaces that with one flat-rate provider whose monthly fee is predictable, sub-1-hour response is guaranteed, and security posture is documented and ready to answer a client questionnaire.

What it takes	Piecemeal	Phantom Bundle
Pricing	Hourly break-fix or per-incident, surprise invoices each month	One flat monthly fee. No hourly billing, no scope debates
Response time	Best-effort when the IT guy gets to it, often next-day	Sub-1-hour acknowledge, sub-8-hour on-site, guaranteed in SLA
Client questionnaires	Partner scrambles to answer every vendor security survey	Pre-built answer set and evidence binder maintained by PTS
Cyber insurance renewal	Each annual questionnaire is a research project, premiums rise	Annual evidence package, MFA / EDR / backup posture documented
Restore testing	Backup tool exists, but no one has actually restored from it	Monthly restore testing performed and logged by PTS
WISP / IR Plan	Downloaded template, never customized, never reviewed	Documented WISP and IR Plan, reviewed annually with vCIO

One contract. One flat rate. One accountable provider. That is the difference between fighting your IT stack and running a firm where security is documented and downtime is rare.

THE PROOF

The cost of getting it wrong

Professional services firms do not show up in the headline breach lists, but they bleed quietly. A 4-hour outage at a 10-person firm is $10K of lost billable revenue. A single BEC wire fraud event averages $129K. The full business-interruption hit for an SME BEC incident now averages $487K including downtime and recovery.

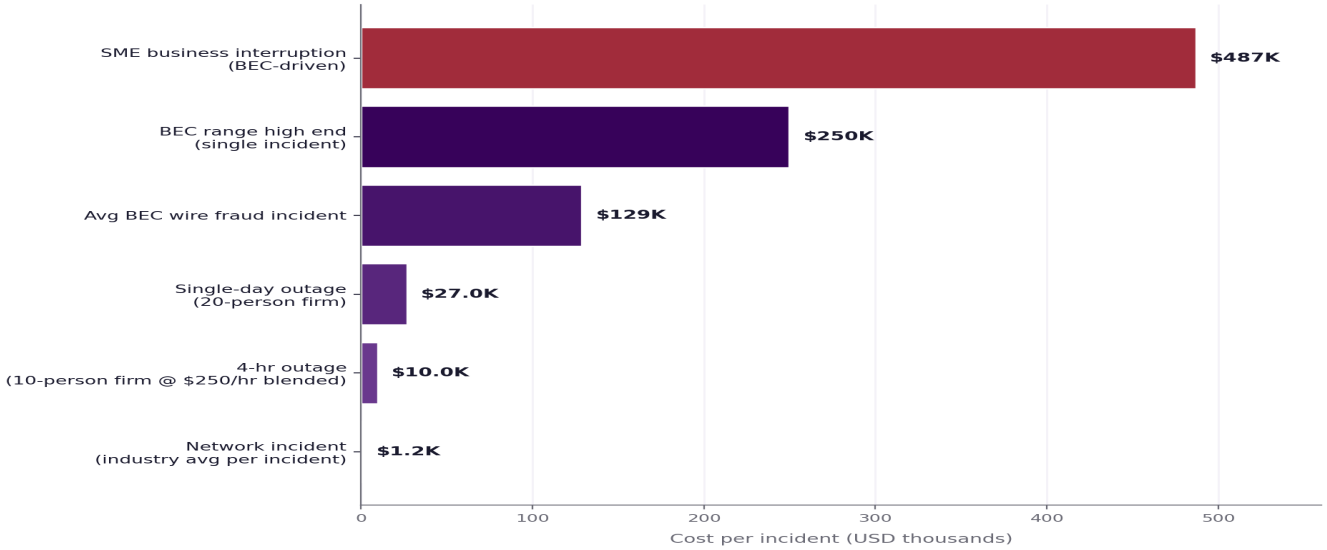
$129K
Average loss per BEC wire fraud incident (FBI IC3 2024)

$487K
Average business-interruption cost for an SME BEC event

15-20%
Forecast cyber insurance premium increase for 2026

40%+
Cyber insurance claims denied for missing controls

Professional services IT and security cost per incident.



Downtime costs based on ITIC SMB benchmarks and EMA Research 2024 figures, applied to a $250 blended hourly rate. BEC figures from FBI IC3 2024 and Eftsure 2025 reporting. SME business-interruption average includes downtime, recovery, legal, and client churn estimates.

Three patterns we keep finding in professional services firms

PATTERN 01

MFA on email, but only sometimes on the file store

Email has MFA. The client file storage, the time-tracking system, the CRM, and the project tool do not. Cyber insurers now require MFA across the board, and BEC actors target the gap.

PATTERN 02

Client questionnaires arriving with no answer set

Large enterprise clients now send vendor security questionnaires before signing the next SOW. Firms with no documented WISP, MFA evidence, or IR Plan lose engagements quietly to peers who can answer in 48 hours.

PATTERN 03

Cyber insurance renewal turning into a research project

Renewal questionnaires now ask about MFA scope, EDR coverage, backup posture, training, and IR planning. Firms without documented answers see premium hikes, coverage exclusions, or outright non-renewal.

THE DIFFERENTIATOR

Client Questionnaire Crosswalk

Every quarter, more of our professional-services clients receive vendor security questionnaires from their own clients before signing the next SOW. Below is the question set we see most often, mapped to the Guardian capability that answers it. Skim the Fundamentals column, every YES is documented and ready to share. Co-Mgd and Compliance tiers add deeper controls for firms facing more rigorous third-party reviews.

ACCESS, IDENTITY, AND AUTHENTICATION

Topic	Question / Requirement	How Guardian Answers	Fund.	Co-Mgd	Compl.
MFA	Do all staff use phishing-resistant MFA on email and any system handling client data?	Entra ID conditional access, phishing-resistant MFA on email, VPN, file storage, M365 admin, finance, and SSO-integrated SaaS.	YES	YES	YES
SSO	Is access to client-data systems consolidated under single sign-on with central account control?	Entra ID single sign-on for supported SaaS, joiner-mover-leaver workflow, quarterly access reviews.	PART	YES	YES
Admin	Are administrative and privileged accounts separated from daily-use accounts?	Designated admin accounts, enterprise password vault, just-in-time elevation, documented privileged access policy.	YES	YES	YES

DATA PROTECTION AND CONFIDENTIALITY

Encryption	Is client data encrypted at rest on staff devices and in transit when shared externally?	BitLocker full-disk encryption on every endpoint, M365 encrypted email and file storage, TLS in transit on all supported services.	YES	YES	YES
Access log	Can the firm produce an audit log of who accessed which client file and when?	M365 Purview audit logs (extended retention on Co-Mgd and Compliance tiers), SharePoint and OneDrive activity logs.	PART	PART	YES
Data DLP	Are controls in place to prevent client data from being sent to personal email or unmanaged cloud storage?	M365 DLP rules tuned to client-PII patterns on Compliance tier, conditional access blocks on Fundamentals and Co-Mgd.	PART	PART	YES

OPERATIONAL SECURITY AND INCIDENT RESPONSE

EDR / MDR	Does the firm have endpoint detection and 24/7 managed detection and response coverage?	Advanced EDR on every endpoint, 24/7 partner SOC monitoring, documented escalation runbooks, monthly threat report.	YES	YES	YES
Backup	Are backups tested? When was the most recent successful restore?	Image-based cloud backup with monthly PTS-performed restore testing, log retained, ransomware recovery runbook on file.	YES	YES	YES
IR Plan	Does the firm have a documented Incident Response Plan with named contacts and notification timelines?	Documented IR Plan with P1-P4 playbooks, named partner-level liaison, breach notification scaffold, annual tabletop exercise.	PART	YES	YES
Training	Are staff trained on phishing, BEC, and acceptable use, and is completion documented?	Monthly phishing simulations, annual training, BEC-aware finance and admin playbook, documented completion records.	YES	YES	YES

CIS 01-05 - Inventory, data, configuration, accounts

CIS Control	Question / Requirement	How Guardian Answers	Fund.	Co-Mgd	Compl.
CIS 01-02	Inventory and control of enterprise assets and software; only authorized software installed.	Asset inventory in a secure documentation portal, RMM-managed endpoints, application allow-listing on Co-Mgd and Compliance.	YES	YES	YES
CIS 03	Data protection: identify, classify, securely handle, retain, and dispose of client data.	BitLocker encryption, M365 file encryption, encrypted email, documented client-data classification, secure media disposal.	YES	YES	YES
CIS 04	Secure configuration of enterprise assets and software; patch and update systems.	Documented hardening baselines via Intune, patch management on supported endpoints, monthly compliance reporting.	YES	YES	YES
CIS 05	Account management: assign and manage credentials for staff, contractor, and service accounts.	M365 identity governance, designated admin accounts, enterprise password vault, joiner-mover-leaver workflow.	YES	YES	YES

CIS 06-08-14 - Access control, audit logging, awareness

CIS Control	Question / Requirement	How Guardian Answers	Fund.	Co-Mgd	Compl.
CIS 06	Access control: phishing-resistant MFA on all remote access, role-based access, quarterly reviews.	Entra ID conditional access, phishing-resistant MFA on email, VPN, file storage, and SSO-integrated SaaS, quarterly access reviews.	YES	YES	YES
CIS 08	Audit log management: collect, alert, review, and retain audit logs.	M365 Purview audit log retention, basic SIEM monitoring on Fundamentals, full compliance SIEM on Compliance tier.	PART	YES	YES
CIS 14	Security awareness and skills training: phishing-resistant culture, BEC-aware finance and admin staff.	Monthly phishing simulations, annual training, BEC-aware playbook for finance and admin, documented completion records.	YES	YES	YES

CIS 11 / 17 - Recovery and incident response

CIS Control	Question / Requirement	How Guardian Answers	Fund.	Co-Mgd	Compl.
CIS 11	Data recovery: tested practices sufficient to restore in-scope assets to a pre-incident state.	Image-based cloud backup, monthly restore testing performed by PTS with documented log, ransomware recovery runbook.	YES	YES	YES
CIS 17	Incident response: documented program to prepare, detect, and respond to attacks, including client notification.	Documented IR Plan, P1-P4 playbooks, partner SOC threat response, named partner liaison, annual tabletop on Compliance.	PART	YES	YES

Firms with a regulated overlay: see the dedicated sheet

Some professional services firms also carry a specific regulatory obligation. If that is your firm, ask us for the dedicated sheet: **accounting and CPA** (FTC Safeguards Rule, see the Financial Services sheet), **law firms** (ABA Model Rule 1.6, see the Legal sheet), **healthcare-adjacent or medical** (HIPAA, see the HIPAA sheet), **DoD subcontractors** (NIST 800-171 / CMMC, see the Manufacturing CMMC sheet). All overlays use the same Guardian tier structure described in this sheet.

THE PATH FORWARD

What working with PTS looks like

Four stages, no surprises. Deployed Fundamentals posture in 30-60 days, with a client questionnaire answer set and cyber insurance evidence package in hand.

1
Discovery
30-min firm assessment and IT environment walkthrough.

2
Assessment
CIS gap snapshot, MFA and backup posture review, questionnaire-gap report.

3
Implementation
Fundamentals tier deployed in 30-60 days. M365 Business Premium, MFA, EDR, backup, IR Plan.

4
Ongoing
Quarterly business review, monthly restore testing, annual renewal evidence package.

When to step up from Fundamentals

Firms growing beyond 25 employees, hitting recurring client questionnaires, or facing a cyber insurance renewal with stricter controls typically step up from Fundamentals to **Co-Managed** (add internal IT collaboration, SIEM, vCISO touchpoints) or to **Compliance** (full WISP, air-gapped backups, audit-ready evidence binder). All tiers share the same flat-rate predictability.

Common gaps we find in pro services firms

- MFA on email but missing on file storage or CRM
- Backup tool exists but never restored from
- Vendor security questionnaires answered ad-hoc
- Cyber insurance renewal turning into a research project
- Personal cloud storage in use for client files
- Off-boarded contractors retain SaaS access

Important. Cybersecurity and IT outcomes depend on the specific environment, staff behavior, and threat landscape facing each firm. PTS provides the technology, documentation, and program rigor that demonstrably reduce risk. Cyber insurance coverage, client contractual obligations, and any sector-specific regulatory requirements remain the responsibility of the firm and its principals. PTS is not a law firm and does not provide legal advice.

Next step: 30-minute Pro Services IT Review

We walk your firm's environment against this exact crosswalk and leave you with a one-page questionnaire-readiness snapshot. No obligation.

Talk to PTS

hello@phantomts.com
phantomts.com/guardian

Why firms choose Phantom

Since 2010
OPERATING
Indiana-based MSP serving Indiana and Michigan professional services firms.

Sub-1-hr
CRITICAL RESPONSE
Guaranteed acknowledge on P1 issues. Real engineers, not a call center.

Flat-rate
PREDICTABLE COST
One monthly fee. No hourly billing. No scope debates. No surprise invoices.