Guardian Fundamentals for Small and Medium Business

Enterprise-grade IT, security, and strategic planning for businesses without an IT department. Flat-rate, sub-1-hour critical response, one standard, set high.

The business problem: Small and medium businesses face the same cyber threats as large enterprises with a fraction of the resources. 43% of cyberattacks target small business. 60% of SMBs that suffer a breach go out of business within six months. Most owners are not IT people, but every IT decision lands on their desk: the security risk, the downtime cost, the budget, the call from the cyber insurance broker, the strategic roadmap. Outsourced break-fix and hourly billing leave gaps. Enterprise providers are not built for a business your size.

The PTS answer: Guardian Fundamentals is our flat-rate, all-inclusive managed-services plan: 24/7 monitoring, enterprise-grade security, real help desk, and strategic IT planning, all for one predictable monthly fee. We have one standard, and it is high. A 10-person company gets the same response times, security, and engineering attention as our largest clients. **Enterprise-level protection, SMB pricing, no corners cut.**

THE SOLUTION

Why Guardian Fundamentals

Fundamentals is the Guardian tier built for SMBs that need real protection, real response, and a real partner. Six capabilities define the difference:

- **Flat-rate monthly fee with everything included.** One predictable invoice covering monitoring, security, support, and strategic planning. No hourly billing, no surprise invoices, no scope debates. Budget with confidence from day one.
- **Sub-1-hour acknowledge on critical issues, guaranteed.** When something breaks, the clock starts the moment you call. Real engineers who already know your environment, not a call center reading a ticket queue. On-site under 8 business hours.
- **Enterprise-grade security sized for your business.** Advanced endpoint detection, 24/7 managed detection and response, phishing-resistant MFA, email security, encrypted file storage, and security awareness training. The same caliber large companies rely on, priced for SMBs.
- **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 an existential crisis for the business.
- **Strategic IT planning through annual vCIO reviews.** Annual technology business review with a real strategic conversation: roadmap, budget, growth plan, security posture, and where to invest next. Quarterly cadence on Compliance tier.
- **A local partner who knows your name and your network.** Indiana-based, serving Michiana and surrounding markets. We treat a 10-person business the same way we treat a 200-person business. One standard, set high.

WHAT YOU GET

Inside the Fundamentals tier

A single managed-service bundle that delivers everything an SMB needs from an IT department: monitoring, support, security, backup, M365, and strategic planning. Flat monthly fee. No hourly billing.

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-resistant MFA, email security, phishing simulations and training, DNS filtering, full-disk endpoint encryption, basic SIEM monitoring.
Backup	Image-based cloud backup (workstations and servers), monthly restore testing performed and logged by PTS, ransomware recovery runbook. 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, email and file backup, DNS and domain management.
IT Leadership (vCIO)	Annual technology business review, technology roadmap, budget planning, vendor and SaaS inventory, PTS firewall and network standards, AUP and IR Plan scaffold, cyber insurance renewal evidence package.

Why one flat-rate bundle, not piecemeal

Most SMBs accumulate a stack: a break-fix IT guy who shows up when things break, an antivirus subscription, a backup tool no one tests, and a friend-of-a-friend who set up email five years ago. 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.

What it takes	Piecemeal	Phantom Bundle
Pricing	Hourly break-fix, per-incident, surprise invoices every month	One flat monthly fee. Budget with confidence
Response time	Best-effort when the IT guy gets to it, often next-day	Sub-1-hour acknowledge on critical issues, guaranteed
Who answers the phone	Call center, ticket number, generic script	Real engineer who knows your environment and network
Security posture	Antivirus, maybe MFA on email, fingers crossed on the rest	EDR, 24/7 MDR, MFA, encryption, training, all included
Restore testing	Backup tool exists, but no one has actually restored from it	Monthly restore testing performed and logged by PTS
Strategic planning	Reactive break-fix, no roadmap, no budget conversation	Annual vCIO review with real strategic conversation

One standard. Set high. No small-business tier. A 10-person company gets the same response times, the same security, and the same engineering attention as our largest clients.

THE PROOF

The cost of getting it wrong

SMBs do not show up in the headline breach lists. They go out of business quietly. The figures below come from the FBI, ITIC, Eftsure, and industry research. They are not enterprise numbers, they are SMB numbers, and they hit hardest where there is no internal IT department to absorb the shock.

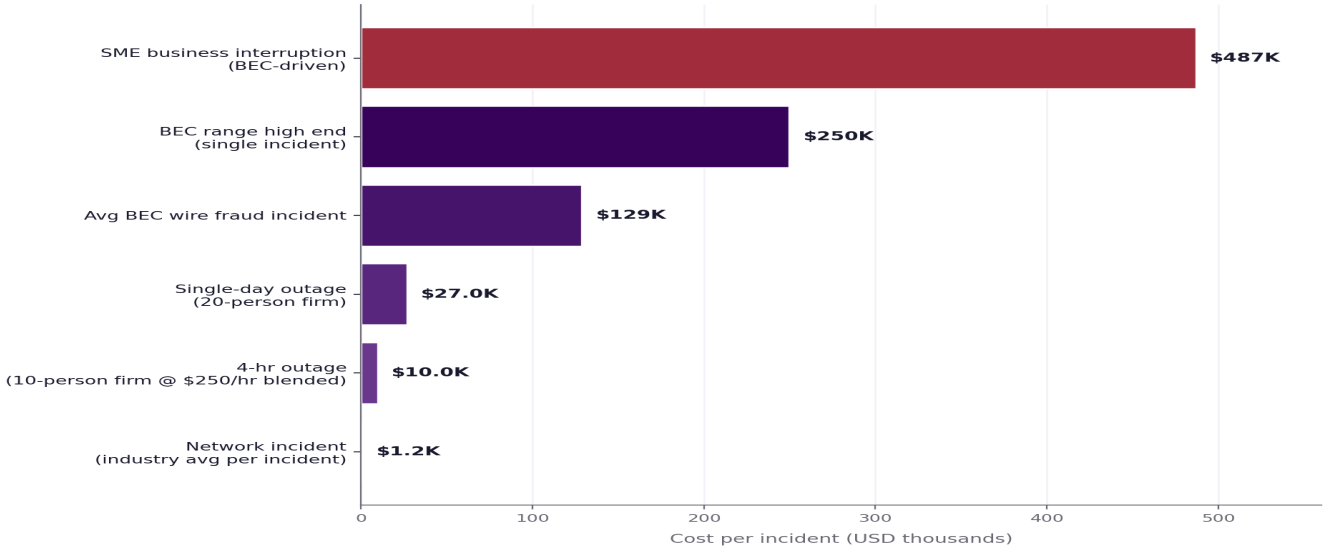
43%
Of cyberattacks target small business

60%
Of SMBs out of business within 6 months of a breach

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

Sub-1hr
Guaranteed PTS acknowledge on P1 issues

SMB 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. SME business-interruption average includes downtime, recovery, legal, and customer churn estimates.

Three patterns we keep finding in SMBs

PATTERN 01

The IT guy is a person, not a system

One IT person (internal or break-fix) who knows everything. When they are on vacation, sick, or move on, the business is blind. Documentation, runbooks, and monitoring fill the gap. Guardian provides all three from day one.

PATTERN 02

Backups exist, but no one has tested a restore

A backup tool was installed years ago. The monthly invoice keeps coming. No one has actually restored from it. The first time it gets tested is during a ransomware event, which is exactly the wrong time.

PATTERN 03

Strategic planning is whatever broke last week

Most SMBs have no IT roadmap, no budget plan, no security posture review. Decisions happen reactively, often under pressure. A real vCIO conversation, even once a year, changes the trajectory of the business.

THE DETAIL

Inside Guardian Fundamentals

What you actually get for the monthly fee. Five layers, every one included, all delivered by real PTS engineers. This is the answer to 'what does my money buy?'

DAILY OPERATIONS - Help desk, monitoring, M365 management

Component	What it does	What it prevents
Help desk	Remote and on-site support. Sub-1-hour acknowledge on critical issues. Real engineers who know your environment.	Lost productivity from waiting hours or days for IT support, call-center frustration, repeated explanations.
24/7 monitoring	Endpoints, servers, network, and M365 watched around the clock. Issues caught and resolved before they impact staff.	Finding out about an outage from a frustrated employee. Silent failures that compound into outages.
M365 management	M365 Business Premium administration, mailbox and user provisioning, conditional access, license optimization.	Stale accounts retaining access, license waste, unmanaged guest access, no audit trail of admin changes.

SECURITY AND PROTECTION - EDR, MDR, MFA, training

Endpoint detection	Advanced endpoint detection and response on every staff device. Threat behavior analysis, not just signature antivirus.	Modern ransomware and credential-theft malware that signature-only antivirus misses entirely.
24/7 MDR	Partner Security Operations Center monitors detections around the clock. Triage, response, and escalation handled.	Detection alerts firing into a void overnight or on weekends. Initial breach turning into a full ransomware event.
MFA and SSO	Phishing-resistant MFA on email, VPN, file storage, and admin. Single sign-on through Entra ID where supported.	Credential theft from phishing, password reuse compromise, and the most common BEC entry path.
Awareness training	Monthly phishing simulations, annual training, BEC-aware playbook for finance and admin staff.	Staff clicking phishing links, finance approving fraudulent wire transfers, lateral spread from one compromised account.

RECOVERY AND STRATEGY - Backup, vCIO, planning

Backup and restore	Image-based cloud backup of workstations and servers. PTS performs and logs a restore every month.	A backup tool that exists on paper but cannot actually restore your business after a ransomware event.
vCIO planning	Annual technology business review: roadmap, budget, security posture, where to invest. Quarterly on Compliance tier.	Reactive IT spending, no roadmap, surprise renewals, no answer when a board or banker asks about the IT plan.
Evidence package	Cyber insurance renewal evidence, vendor inventory, AUP, IR Plan scaffold, MFA / EDR / backup posture documented.	A renewal questionnaire that takes weeks to answer, premium hikes from missing controls, or coverage denials.

THE PATH FORWARD

When to step up, and where to go next

Most SMBs start on Fundamentals. Some have triggers that push them up. And some operate in a regulated vertical that deserves its own dedicated document. Below is the simple decision map.

Tier	You are here when	What changes
Stay on Fundamentals	5-50 employees. No internal IT. No specific regulatory framework. Standard SMB security and operations needs.	One flat fee. Sub-1-hr response. EDR / MDR / MFA / backup / vCIO.
Step up to Co-Managed	Internal IT person or team. Want PTS to extend or augment, not replace. Growing past 50 employees. SIEM and ticketing maturity.	PTS layers on top of internal IT. Co-owned escalation runbooks. SIEM, advanced monitoring, vCISO touchpoints.
Step up to Compliance	Specific regulatory obligation (see list below). Client questionnaires arriving regularly. Cyber insurance asking for documented WISP and tabletop. Board cyber inquiry.	Full WISP, air-gapped backups, audit-ready evidence binder, annual tabletop, quarterly vCIO.

Operating in a regulated vertical? Ask for the dedicated sheet

Each Guardian tier described above applies to the verticals below, but every regulated audience deserves a sheet written in its own language. If your business fits one of these, ask us for the dedicated document.

Vertical	Regulatory anchor	Dedicated sheet
Healthcare and dental practices	HIPAA, 45 CFR Part 164. Patient PHI handling, OCR breach reporting, BAA management.	**PTS HIPAA / Medical sheet**
DoD subcontractors and federal manufacturing	NIST 800-171, CMMC Level 2, DFARS 252.204-7012, CUI handling, SSP, POA&M.	**PTS Manufacturing CMMC sheet**
RIAs, wealth, broker-dealers, CPAs	FTC Safeguards Rule (16 CFR Part 314), SEC Reg S-P, Reg S-ID, IRS Pub 4557.	**PTS Financial Services sheet**
Law firms (5 to 50 attorneys)	ABA Model Rule 1.6(c), Formal Opinions 477R / 483 / 498, client confidentiality.	**PTS Legal / Professional Services sheet**
Nonprofits and associations	IRS Form 990 governance, state charitable solicitation, PCI DSS v4.0 for donations, grantor security.	**PTS Nonprofit / Association sheet**
K-12 districts and small schools	FERPA, PPRA, CIPA, COPPA, state student data privacy laws, FCC E-rate and Cyber Pilot.	**PTS K-12 Education sheet**
Consulting, AEC, marketing, HR, real estate, insurance	Client questionnaires, cyber insurance renewals, billable-hour pricing pressure. Generic CIS baseline.	**PTS Professional Services sheet**

GETTING STARTED

What working with PTS looks like

Four stages, no surprises. Most SMBs go from first call to a deployed Fundamentals posture in 30-60 days.

1
Discovery
30-min business and IT environment walkthrough. No cost.

2
Assessment
Security and infrastructure snapshot, prioritized findings, roadmap proposal.

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

4
Ongoing
Real help desk, monthly restore testing, annual vCIO business review.

Businesses we serve

We serve SMBs across **professional services, retail and e-commerce, construction and trades, real estate and property management, marketing and creative agencies, distribution and logistics, healthcare and dental practices, and nonprofits**. Indiana-based, serving Indiana and Michigan from South Bend, Mishawaka, Elkhart, Granger, La Porte, Michigan City, Valparaiso, and Niles, MI.

Common gaps we find in SMBs

- One IT person knows everything, no documentation
- Antivirus, but no EDR or 24/7 MDR coverage
- MFA on email, missing on file storage and admin
- Backups exist but never tested
- No IT roadmap or budget conversation
- Off-boarded staff still have SaaS access

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

Next step: Free IT Assessment

Schedule a free, no-obligation IT assessment. We review your current environment, identify security gaps, and show you how Guardian Fundamentals supports your firm's growth.

Talk to PTS

hello@phantomts.com
phantomts.com/guardian

Why SMBs choose Phantom

Since 2010
OPERATING
Indiana-based MSP serving SMBs across Indiana and Michigan.

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 surprise invoices. No scope debates.