THREATNEXIS | SMALL BUSINESS CYBERSECURITY

The $500 Security Stack

That Covers 80% of Your Attack Surface

A curated, battle-tested set of tools any small business can deploy for under $500 — and why these specific tools stop the attacks that actually happen.

$200K+	400:1	80%
average cost of a small business data breach — per IBM 2024	return: $500 stack vs. average breach cost it prevents	of small business attack surface covered by this stack

FREE EDITION | threatnexis.com | 2025 Edition | For businesses with 1–250 employees

What's Inside This Guide

- Why $500 is enough for 80% coverage
- The 8 attack vectors this stack addresses
- The $500 stack: 7 specific tools with pricing
- Running budget tracker as you build your stack
- What the remaining 20% costs and covers
- Tools you already own (M365 free tier guide)
- 30-day deployment checklist
- The one thing to do in the next 60 minutes

1. The Math That Makes This Real

Let's be direct about something most cybersecurity vendors won't tell you: you do not need a $200,000 enterprise security platform to be meaningfully secure. The majority of small business cyberattacks succeed not because attackers are sophisticated — but because the victim had no basic controls in place at all.

The attacks that actually hit small businesses are almost entirely commoditized: phishing emails, credential stuffing from breached password lists, ransomware deployed via an unpatched system or stolen RDP credential, and business email compromise exploiting weak email authentication. These are not zero-day exploits. They are script-kiddie attacks that work because no one put up the basic fence.

This guide gives you the fence. Seven specific tools, one annual budget, one 30-day deployment plan. No fluff, no upsell trap, no enterprise complexity. Just the security controls that stop the attacks that actually happen to businesses like yours.

The Risk You're Carrying	The Investment You Need
$200,000+	**$500/year**
Average SMB data breach cost (IBM 2024). Does not include reputational damage, lost clients, or business closure.	The stack in this guide. Under $42/month. Covers the attack vectors responsible for 80% of small business incidents.

THE ROI CALCULATION

The question is not whether you can afford to spend $500 on security. The question is whether you can afford to lose $200,000. At 400:1 return on investment, this is the most efficient use of money available to any small business owner.

2. Why 80% — and What the Other 20% Costs

No security stack provides 100% protection. Anyone who claims otherwise is lying to you. But the 80/20 principle applies powerfully to cybersecurity: a relatively small set of controls addresses the overwhelming majority of the threats your business will actually face.

The 8 Attack Vectors This Stack Addresses

%	Attack Vector	How Common	What in the Stack Stops It
✓	**Phishing & Credential Theft**	#1 attack vector. 91% of breaches start with email.	MFA + Email security (Safe Links/DMARC)

© 2025 Threatnexis. All rights reserved. | threatnexis.com

✓	**Password Reuse / Stuffing**	Automated credential testing from breach databases.	Password manager (Bitwarden) + unique passwords
✓	**Ransomware via Email**	Malicious attachments deliver ransomware payload.	Email filtering + EDR detection
✓	**Ransomware Recovery Failure**	No clean backup = ransom payment or closure.	Backblaze immutable cloud backup
✓	**Malware on Endpoint**	Drive-by downloads, malicious USB, infected software.	Microsoft Defender EDR (free, already installed)
✓	**DNS Malware Delivery**	Malicious domains serve exploits at the DNS layer.	Cloudflare DNS filtering (free)
✓	**Unpatched Vulnerabilities**	Known CVEs exploited on unpatched Windows/apps.	Patch management discipline (process, not a tool)
✓	**BEC Wire Fraud Enablement**	Attackers spoof your domain to trick clients/banks.	DMARC email authentication (free DNS record)
⚠️	**Advanced Persistent Threats**	Nation-state / sophisticated targeted attacks.	Requires $3K–$10K+/year enterprise stack
⚠️	**Zero-Day Exploits**	Unknown vulnerabilities with no patch available.	Threat intel feeds + SOC (enterprise only)
⚠️	**Insider Threat Detection**	Behavioral analytics to detect rogue employees.	UEBA/SIEM platforms ($5K–$20K+/year)

THE REMAINING 20%

The vectors marked ⚠️ represent the 20% not covered by this stack. They require dedicated security staff, enterprise platforms, and budgets of $3,000–$20,000+ per year. For most small businesses, the risk of these scenarios is low relative to cost. Focus on the ✓ vectors first.

3. The $500 Stack: Every Tool, Every Dollar

Here is the complete stack. Every tool below has been selected for maximum security value per dollar, ease of deployment by non-technical teams, and compatibility with the most common small business environment: Microsoft 365 on Windows.

The total annual cost is based on a 10-person business. Adjust the per-user tools proportionally for your headcount. Every free tool listed is genuinely free — no credit card required, no feature-crippled trial.

01 **Microsoft Authenticator + Security Defaults** — **$0 / year** — Already in your M365 subscription

© 2025 Threatnexis. All rights reserved. | threatnexis.com

Category: Identity & MFA

The single highest-ROI security action available. Enable Security Defaults in your M365 Admin Center and every user will be prompted to enroll in MFA at next login. This blocks 99.9% of automated credential attacks. The Microsoft Authenticator app is free on iOS and Android. There is no reason this is not already enabled at your company.

02

Bitwarden Teams

Category: Password Management

$36/year

$3/user/month × 10 users × 12 months

The #1 cause of credential breaches is password reuse. Bitwarden Teams is open-source, zero-knowledge, and costs $3/user/month — less than a cup of coffee. Employees get a browser extension that auto-fills unique 20-character passwords for every site. Admins get a dashboard showing password health across the team. This ends password reuse overnight.

03

Backblaze Business Backup

Category: Backup & Recovery

$84/year

$7/device/month × 10 devices annually

Ransomware only wins if you have no backup. Backblaze Business backs up every file on every endpoint to the cloud, continuously, for $7 per device per month. It is immutable, meaning ransomware cannot encrypt or delete it. Restoring is a web browser away. This is the single tool that turns a ransomware event from “business closure” to “bad Tuesday.”

04

Microsoft Defender Antivirus / EDR

Category: Endpoint Detection & Response

$0 / year

Built into Windows 10/11 — zero additional cost

Most small businesses run Windows. Microsoft Defender Antivirus is built into every Windows 10/11 machine and is, by independent testing labs, one of the top-performing AV/EDR solutions available — including paid alternatives. It scans in real time, detects behavioral threats, and integrates with Microsoft 365 Defender. The only action required: verify it is turned on. Go to Settings → Windows Security → Virus & threat protection. Confirm it shows green.

05

Microsoft 365 Defender: Safe Links + Safe Attachments

Category: Email Security

$0 / year

Included in M365 Business Premium ($22/user/mo)

If you have M365 Business Premium, Safe Links rewrites every URL in every email and checks it against threat intelligence at the moment of click. Safe Attachments detonates every attachment in a sandbox before delivering it to your inbox. Combined, these two controls stop the majority of phishing and malware delivery via email. If you don’t have Business Premium, this is the strongest argument to upgrade. The incremental cost over Business Standard is approximately $10/user/month.

© 2025 Threatnexis. All rights reserved. | threatnexis.com

06

Cloudflare Gateway DNS Filtering

Category: DNS & Web Filtering

$0 / year
Free for businesses via Cloudflare Zero Trust (up to 50 users)

DNS filtering blocks your entire network from reaching known malicious domains before a connection is ever established. Cloudflare Gateway is free for up to 50 users, requires no software installation (just a DNS settings change on your router), and blocks malware, phishing, and command-and-control infrastructure. Setup takes 15 minutes. Point your router's DNS to 1.1.1.2 for immediate basic protection, or create a free Cloudflare Zero Trust account for full category-based filtering and reporting.

07

DMARC + SPF + DKIM Email Authentication

Category: Email Domain Protection

$0 / year
Free DNS records — implemented via your DNS provider

DMARC prevents attackers from spoofing your email domain to impersonate your business. Without it, anyone can send an email that appears to come from you@yourcompany.com. With DMARC at p=reject, that becomes impossible. SPF and DKIM are the foundation records. Combined, they protect your clients from receiving fraudulent emails that appear to be from you, and improve your email deliverability. Check your current status at mxtoolbox.com/dmarc. Most small businesses are missing at least one record.

The Complete Budget Tracker

Tool	Annual Cost (10 users)
01 Microsoft Authenticator + M365 Security Defaults	$0
02 Bitwarden Teams Password Manager	$36
03 Backblaze Business Backup (10 devices)	$84
04 Microsoft Defender AV / EDR (built-in)	$0
05 M365 Defender: Safe Links + Safe Attachments	$0*
06 Cloudflare Gateway DNS Filtering	$0
07 DMARC + SPF + DKIM Email Authentication	$0

TOTAL ANNUAL COST (all 7 tools, 10 users)

*Safe Links/Attachments require M365 Business Premium ($22/user/mo). If on Business Standard, upgrade cost = ~$100/mo for 10 users, or $1,200/yr. Use Proofpoint Essentials ($4/user/mo = $480/yr) as an alternative.

$120–$500
per year

BUDGET NOTE FOR M365 BUSINESS STANDARD USERS

If you only have M365 Business Standard (not Premium), substitute Cloudflare Area 1 Email Security ($1.50/user/mo) or Proofpoint Essentials ($4/user/mo) for the email filtering gap. Either brings your total to approximately $380–$500/year. Still well under budget.

© 2025 Threatnexis. All rights reserved. | threatnexis.com

4. Tools You Already Own (If You Use Microsoft 365)

Before you spend a single dollar, check what you already have. Microsoft 365 subscribers are sitting on a significant security capability that most businesses have never turned on. Here is what is available at each plan level:

Security Capability	Business Basic / Standard	Business Premium	Action Required
Microsoft Authenticator MFA	✔️ Included	✔️ Included	Enable Security Defaults in M365 Admin
Microsoft Defender AV (Windows)	✔️ Included	✔️ Included	Verify active in Windows Security
Exchange Online Protection (spam filter)	✔️ Included	✔️ Included	Already active — no action needed
Microsoft Secure Score Dashboard	✔️ Included	✔️ Included	Visit security.microsoft.com
Safe Links (email URL scanning)	❌ Not included	✔️ Included	Enable in M365 Defender portal
Safe Attachments (sandbox detonation)	❌ Not included	✔️ Included	Enable in M365 Defender portal
Microsoft Defender for Business (EDR)	❌ Not included	✔️ Included	Deploy via security.microsoft.com
Conditional Access (MFA policies)	❌ Not included	✔️ Included	Configure in Entra ID Admin Center
Intune Device Management (MDM)	❌ Not included	✔️ Included	Enroll devices via Intune portal
Azure AD Identity Protection	❌ Not included	✔️ Included	Enable in Entra ID → Security

THE BUSINESS PREMIUM UPGRADE ARGUMENT

Microsoft 365 Business Premium costs approximately $22/user/month. If you are on Business Standard ($12.50/user/month), the upgrade costs $9.50/user/month. For 10 users, that is $114/month or $1,368/year. You gain: EDR, Safe Links, Safe Attachments, Conditional Access, Intune, and Azure AD P1. For many businesses, this single upgrade replaces $3,000–$8,000 worth of third-party security tools.

5. The 30-Day Deployment Plan

© 2025 Threatnexis. All rights reserved. | threatnexis.com

You can have this entire stack deployed in 30 days with roughly 4–6 hours of total effort. Here is a week-by-week plan:

Week	Actions	Est. Time	Cost
WEEK 1 Identity	• Enable M365 Security Defaults (admin.microsoft.com → Identity → Properties → Manage Security Defaults) • Notify team: “You will be prompted to set up Microsoft Authenticator at next login” • Sign up for Bitwarden Teams at bitwarden.com/products/business • Send all employees an invite to the Bitwarden organization • Walk team through installing the Bitwarden browser extension	2–3 hours	$0
WEEK 2 Backup	• Sign up for Backblaze Business at backblaze.com/business-backup.html • Deploy the Backblaze agent to all employee computers (takes 5 min per machine) • Wait 24–48 hours for initial backup to complete • Test a file restore from the Backblaze web console • Log the restore test date and result — you’ll need this for cyber insurance	1–2 hours	$7/ device
WEEK 3 Network	• Log into your office router admin panel (typically 192.168.1.1 or 192.168.0.1) • Change primary DNS to 1.1.1.2 and secondary DNS to 1.0.0.2 (Cloudflare for Families) • Save and reboot router — all devices now have DNS-layer malware filtering • Verify Defender AV is active on all Windows devices: Settings → Windows Security • Go to mxtoolbox.com and check your domain’s SPF, DKIM, and DMARC records	1 hour	$0
WEEK 4 Email & Finish	• If SPF/DKIM/DMARC are missing: contact your IT provider or DNS registrar to add them • If on M365 Business Premium: enable Safe Links and Safe Attachments in M365 Defender • If not on Business Premium: evaluate upgrade or add Cloudflare Area 1 / Proofpoint Essentials • Run all employee emails through haveibeenpwned.com — change any compromised passwords • Send team a 5-bullet “Security Basics” reminder	2 hours	$0

© 2025 Threatnexis. All rights reserved. | threatnexis.com

	email with what you've deployed		

6. What Changes at $1,000 and $5,000 Per Year

Once your $500 foundation is deployed, here is what the next tier of investment buys you. These are meaningful upgrades — not upsells. But they are not necessary until the basics are solid.

Budget Level	Additional Tools	Coverage Added
$500/year (This guide)	MFA, Password Manager, Backblaze, Defender, DNS Filtering, DMARC	80% coverage: credential attacks, ransomware, malware, email fraud, DNS malware
$1,000–$2,000/ year	+ M365 Business Premium upgrade or Proofpoint + Dark web monitoring (SpyCloud, $1/user/mo) + KnowBe4 phishing simulation ($3/user/mo)	88% coverage: adds advanced email security, credential exposure monitoring, human behavior defense
$2,000–$5,000/ year	+ Huntress Managed EDR ($6/device/mo) + Cisco Umbrella DNS ($2/user/mo) + DMARC monitoring (Dmarcian, $20/mo)	93% coverage: adds managed threat detection, enhanced network security, domain abuse visibility
$5,000+/year	+ Full SOC/MDR service + SIEM/log management + Zero Trust architecture + Penetration testing	95%+ coverage: enterprise-grade detection, compliance readiness, proactive threat hunting

7. Objections We Hear — and the Real Answers

Q **"We're too small to be targeted."**

This is the most dangerous belief in small business security. Attackers use automated tools that scan millions of IP addresses per day looking for unpatched systems, open RDP ports, and weak credentials. They are not targeting you specifically — they are targeting everyone, all the time, at scale. Small businesses are attacked more frequently than large ones because they are easier targets.

Q **"We already have antivirus."**

Antivirus alone addresses perhaps 25% of your attack surface. It does nothing to stop phishing, credential stuffing, ransomware that uses legitimate tools (like PowerShell), or email domain spoofing. Antivirus is necessary but nowhere near sufficient.

Q **"I don't have time to manage security tools."**

© 2025 Threatnexis. All rights reserved. | threatnexis.com

The tools in this stack require approximately 4–6 hours to deploy and roughly 30 minutes per month to maintain. Recovering from a ransomware attack requires 40–300 hours and costs $50,000–$500,000. The time objection does not survive this comparison.

Q

“We trust our employees.”

Employee trust is irrelevant. Even the most conscientious employee can be tricked by a sophisticated phishing email. The controls in this stack are not about distrust — they are about removing the conditions that let human errors become catastrophic events.

Q

“Our IT guy handles this.”

Ask your IT provider to show you: (1) a screenshot of your MFA enrollment report, (2) your last backup restoration test log, and (3) your DMARC DNS record at mxtoolbox.com. If they cannot produce all three, security is not being actively managed.

8. Your Next 60 Minutes

You do not need to deploy the entire stack today. But you can start the most important piece right now. Here is what to do in the next 60 minutes:

#	Action	Time	Cost
01	Open admin.microsoft.com. Navigate to Identity → Properties → Manage Security Defaults. Toggle MFA to Enabled. Save. Done. 99.9% of automated attacks on your accounts are now blocked.	15 min	**$0**
02	Go to mxtoolbox.com/dmarc. Enter your email domain. Screenshot the result. If DMARC is missing or set to p=none, email your IT provider today: “We need to publish a DMARC record at p=quarantine.”	5 min	**$0**
03	Open Settings → Windows Security on your computer. Confirm Virus & threat protection shows green. If not, re-enable Microsoft Defender immediately.	5 min	**$0**
04	Go to backblaze.com/business-backup.html. Click Start Free Trial. Sign up. You have 15 days free to verify it works before any charge.	10 min	**Free trial**
05	Go to bitwarden.com. Click Get Started. Create a free individual account. Install the browser extension. Start saving passwords for new logins this week.	10 min	**$0**

9. Resources & Direct Links

© 2025 Threatnexis. All rights reserved. | threatnexis.com

Tool	Where to Sign Up	Documentation
M365 Security Defaults	admin.microsoft.com → Identity → Properties	learn.microsoft.com/security-defaults
Bitwarden Teams	bitwarden.com/products/business	bitwarden.com/help
Backblaze Business	backblaze.com/business-backup.html	help.backblaze.com
Cloudflare Gateway DNS	1.1.1.2 (router) or cloudflare.com/zero-trust	developers.cloudflare.com/cloudflare-one
DMARC Check / Setup	mxtoolbox.com/dmarc	dmarc.org/overview
Have I Been Pwned	haveibeenpwned.com	haveibeenpwned.com/API
Microsoft Secure Score	security.microsoft.com	learn.microsoft.com/secure-score

MAINTAINANCE REALITY CHECK

Security is not a product you buy once and forget. It is a practice. The $500 stack you build this month will need a quarterly 30-minute check-in: verify backups are running, confirm MFA is on all accounts, check that no former employees still have access. That's it. Less than two hours per year of maintenance to protect everything you've built.

SEO & Content Strategy Reference

Primary Keyword:

- $500 cybersecurity stack small business

Secondary Keywords:

- affordable security tools small business 2025
- cheapest way to secure small business
- small business security on a budget
- cybersecurity for under $500 small business
- best free security tools small business

SEO Title:

- The $500 Security Stack: Cover 80% of Your Attack Surface [2025 Guide]

Meta Description:

- 7 specific tools, one $500 annual budget, 30-day deployment plan. Cover 80% of your small business attack surface with MFA, password manager, backup, EDR, DNS filtering, and email authentication.

SEO Slug:

- /500-dollar-security-stack-small-business

© 2025 Threatnexis. All rights reserved. | threatnexis.com

People Also Ask:

- What is the minimum cybersecurity a small business needs?
- Can I protect my small business from hackers for free?
- What security tools are included in Microsoft 365?
- Is Backblaze a good backup solution for small business?
- How do I set up DMARC for my business email domain?

Monetization Opportunities:

- Premium $500 Stack Deployment Guide with evidence templates
- Security Stack Assessment & Gap Analysis Service
- $500 Stack Deployment Package (done-for-you service)
- Virtual CISO Retainer for ongoing stack management

Want the Complete Small Business Security Toolkit?

The Threatnexis Premium Toolkit includes per-industry stack configurations, deployment evidence templates, and premium vendor scorecards:

✓ $500 Stack Deployment Evidence Package
✓ 7 Industry-Specific Stack Configurations
✓ Vendor Comparison Scorecards (all categories)
✓ 30-Day Deployment Tracking Worksheet
✓ Budget Scaling Guide ($500 to $10,000)
✓ MSP / IT Provider Briefing Templates
✓ Cyber Insurance Readiness Tracker
✓ Board-Ready Security Investment Report

➤ [Unlock the Premium Small Business Security Toolkit at threatnexis.com]

Want Us to Deploy This For You?

Threatnexis Consulting will deploy the entire $500 stack for your business in 5 hours. We handle the configuration, verification, and documentation.

➤ [Book a Free Consultation]

Join the Threatnexis Insider Community

Monthly checklists, tool reviews, security tips, and new downloads — always free.

➤ [Subscribe Free]

© 2025 Threatnexis. All rights reserved. | threatnexis.com