Aptik.

A TECHNICAL WALKTHROUGH

Inside Aptik Assure

What Your $300 Per User Actually Delivers

Four enterprise-grade engines — productivity, security, resilience, and vulnerability management — unified into one flat unified into one flat rate, one accountable team, and zero surprises.

Aptik · AI-First Managed IT · aptik.ca · Prepared July 2026 · Confidential

WHAT WE'LL COVER

Seven Sections, One Flat Rate

01	**The Big Picture**	One flat rate, four enterprise engines, and why we built it this way.
02	**Complete Human Support**	Unlimited support, onboarding, offboarding, and workshops — all included.
03	**Microsoft 365 E7**	Your unified productivity, AI, identity, and compliance foundation.
04	**Managed Detection & Response**	24/7 human-led defense across endpoints and identities.
05	**Absolute Data Resilience**	Immutable backup and rapid recovery for everything you run.
06	**Vulnerability Management & Pen Testing**	Continuous visibility, automated remediation, provable compliance.
07	**Bringing It Together**	How it all combines into one predictable invoice.

THE BIG PICTURE

One Flat Rate. Four Enterprise Engines.

Every dollar of your $300-per-user rate funds four purpose-built engines working together — not four separate vendor bills.

Productivity & AI Foundation

Microsoft 365 E7 — apps, identity, identity, compliance, and Copilot AI Copilot AI in one governed platform. platform.

Threat Detection & Response

24/7 human-led monitoring across every endpoint and every identity, day and night.

Immutable Data Resilience Resilience

Ransomware-proof backup of your your mailboxes, files, Teams data, data, and identity infrastructure.

Vulnerability Management Management

Ongoing exposure scanning, automated remediation, and audit-ready compliance evidence.

THE BIG PICTURE

Not Just Consolidated — Integrated

TYPICAL FRAGMENTED STACK

- Separate vendors for productivity, security, backup, and vulnerability scanning
- Each tool sees only its own slice — a suspicious login in one system never informs the others
- Alerts pile up with no single team accountable for triage
- Support, licensing, and hardware billed by different companies, on different schedules

THE APTIK ASSURE STACK

- One identity fabric — a suspicious login anywhere instantly informs informs every other layer
- One 24/7 team triaging endpoint, identity, backup, and vulnerability signals together
- One accountable partner, one predictable invoice, one escalation path
- Enterprise-grade capability engineered for firms of 1–125 people, not Fortune 500 budgets

THE BIG PICTURE

The Defence-in-Depth Model

Four disciplines, working continuously, so no single point of failure decides the outcome.

1

Prevent

Harden identities, patch systems, and train people before an attacker ever gets a foothold.

2

Detect

24/7 human-led monitoring across endpoints, identities, and network exposure.

3

Recover

Immutable, tested backups mean ransomware never has real leverage.

4

Prove

Continuous evidence mapped to the compliance frameworks your clients and insurers expect.

4

engines working as one

24/7

human-led coverage

1

flat monthly rate

0

surprise invoices

SECTION ONE

Complete Human Support

The team behind the technology — because a platform alone was never the whole promise.

COMPLETE HUMAN SUPPORT

Unlimited Support, No Exceptions

Every one of the four engines is only as good as the team standing behind it. That team is unlimited — by design.

Unlimited Calls

Every employee can call and speak with a real technician as often as they need — not just designated IT contacts.

Unlimited Tickets

No ticket counted, no incident capped. Volume never triggers a surcharge or a conversation about overage.

No Hourly Billing, Ever

Support is not metered. There is no no clock running and no invoice at at the end of the month for time spent helping you.

Every Employee Covered Covered

Support extends to all 70 people, not a handful of named admins — because everyone eventually needs help.

COMPLETE HUMAN SUPPORT

We Coordinate With Your Other Vendors

- **You keep one point of contact —** When a line-of-business app or an industry-specific tool has a problem, you call us — not a rotating cast of third-party vendors.
- **We make the calls on your behalf —** We open the ticket, sit on the call, and push the other vendor's support team, so your staff never has to manage that relationship.
- **Every vendor, not just the ones we sold you —** Coordination applies to software you already own and rely on, even if Aptik didn't originally provide it.
- **No extra line item —** This coordination is part of the flat rate — never a separate consulting fee for “third-party liaison” work.

The accountability void, closed

Your internet provider blames your firewall. Your software vendor blames your network. We sit in the middle and own getting it fixed, whoever's tool is actually at fault.

COMPLETE HUMAN SUPPORT

Onboarding & Offboarding, Handled

New Hire to Day-One Ready

A new employee's computer is configured, secured, and provisioned with every account and licence they need — ready before their first day, not scrambled together that morning.

Secure Offboarding, Within Minutes

Access is revoked across every system within minutes of your instruction. Mail and files are preserved and delegated, licences are licences are reclaimed, and the device is wiped and ready for its next its next user.

COMPLETE HUMAN SUPPORT

Workshops, Training & Standard Projects

Getting value from the platform is part of the service, not something you have to figure out alone.

AI & Adoption Workshops

Hands-on sessions that turn a new AI assistant into a habit your team actually uses, not a tool that sits unused.

Ongoing Training

As features roll out or your team grows, training is refreshed — never a one-time onboarding that's forgotten in a month.

Standard Projects Included Included

Everyday projects — a new office office move, a SharePoint site, a process automation — are part of of the rate, not a quoted extra.

Quarterly Business Reviews

A regular working session with your leadership to review what's working and plan what's next.

COMPLETE HUMAN SUPPORT

What “Unlimited” Actually Means

No asterisks, no fair-use throttling, no upsell waiting at the other end of a support call.

0
hourly billing on any support interaction

∞
calls and tickets, for every employee

100%
of staff covered, not just named admins
admins

1
point of contact for every vendor you use

Support, onboarding, offboarding, third-party coordination, workshops, and standard projects are not add-ons priced separately.
priced separately. They are the service — the reason a flat rate can exist at all.

SECTION TWO

Microsoft 365 E7

Your unified productivity, identity, and AI foundation — the platform every other engine plugs into.

MICROSOFT 365 E7

What Is Microsoft 365 E7?

E7 is Microsoft's newest and most complete enterprise suite — one licence that combines four previously separate purchases into a single governed platform.

Microsoft 365 E5

The full productivity suite plus advanced Defender, Purview, and Intune security and compliance capability.

Microsoft 365 Copilot

AI embedded directly in Word, Excel, PowerPoint, Outlook, and Teams — grounded in your own content.

Microsoft Entra Suite

Zero-Trust identity and access control extended beyond users to to apps, data, and AI agents.

Microsoft Agent 365

The governance control plane for every AI agent now working across your business.

MICROSOFT 365 E7

The Productivity Layer, Elevated

Every employee keeps working in the apps they already know — Word, Excel, PowerPoint, Outlook, Teams — now with an AI assistant built directly into the workflow, not bolted on as a separate app.

- **Drafting & summarizing —** Copilot writes first drafts, summarizes long email threads, and recaps meetings automatically.
- **Spreadsheets & analysis —** Plain-language questions turn into formulas, pivot tables, and charts inside Excel.
- **Presentations —** PowerPoint turns a document or outline into a fully designed deck in minutes.
- **Meetings —** Teams captures action items and decisions in real time, even for people who missed the call.

MICROSOFT 365 E7

Copilot & Work IQ

Work IQ is the intelligence layer behind Microsoft 365 Copilot — it understands your organization's own documents, emails, chats, and meetings, and answers accordingly.

- **Grounded, not generic —** Answers are built from your own content — proposals, proposals, standards, and prior correspondence.
- **Private by design —** Your data is never used to train public models and never leaves your governed tenant.
- **An assistant for everyone —** Every employee gets the same premium AI — not a shared seat or a rationed add-on.

From questions to answers, instantly

“Summarize this client's last three emails and draft a reply.” — answered in seconds, using your own inbox as context.

MICROSOFT 365 E7

Defender: Unified Threat Protection

Defender is Microsoft's threat-protection engine inside E7 — four protection surfaces correlated into one signal, not four separate dashboards.

Endpoint

Behavioral protection for every laptop and desktop against malware and fileless attacks.

Email & Collaboration

Blocks phishing, malicious links, and attachments before they reach an inbox.

Identity

Flags impossible travel, stolen sessions, and anomalous sign-in behavior in real time.

Cloud Apps

Visibility and control over the SaaS apps your team connects to their Microsoft 365 identity.

MICROSOFT 365 E7

Phishing & Attack Simulation Training

Your people are trained against realistic attacks captured from real-world phishing — not generic, easy-to-spot test emails.

- **Realistic, automated simulations —** Campaigns run on a schedule using payloads modeled on modeled on real captured attacks, including QR-code phishing.
- **Personalized training on the spot —** Anyone who clicks is immediately routed to a short, relevant lesson — not a generic annual course.
- **Organization-wide risk tracking —** Leadership sees a predicted compromise rate and watches it improve, department by department.
- **30+ languages —** Every employee trains in the language they're most comfortable in.

Why it matters

The overwhelming majority of breaches still start with start with one click on a convincing email. Training that Training that mirrors real attacks — and coaches in the coaches in the moment of failure — is the single single highest-leverage defense you can put in front of front of a workforce.

MICROSOFT 365 E7

Entra Suite — Identity Beyond the Login

The office firewall is gone. Identity is the new perimeter — and Entra Suite extends Zero Trust to everything an identity can touch, including AI agents.

Conditional Access

Every sign-in is evaluated for device health, location, and risk before access is granted.

Identity Governance

Access reviews and lifecycle automation ensure people only hold the permissions they still need.

Identity Protection

Machine-learning risk detection flags flags compromised credentials before they're used.

Extends to AI Agents

The same Zero-Trust controls now govern the agents acting on your data, not just your people.

MICROSOFT 365 E7

Purview — Governing Your Data

As AI reads more of your company's content, governing that content matters more than ever. Purview is the control layer that keeps sensitive data classified, contained, and auditable.

- **Data loss prevention —** Outbound files and emails are scanned and classified automatically; sending a protected file to a personal address is personal address is blocked before it happens.
- **eDiscovery —** Legal and compliance teams can search across mailboxes, files, and Teams conversations from one place when it matters.
- **Information protection —** Sensitivity labels travel with a document wherever it goes, inside or outside the organization.
- **Insider risk management —** Unusual data-handling patterns are surfaced early, before they become a real incident.

MICROSOFT 365 E7

Agent 365 — Governing the AI Workforce

As AI agents start doing real work — drafting, researching, filing, automating — someone has to answer for what they touch. Agent 365 is that control plane.

Agent Registry

Every AI agent operating in your environment is inventoried — nothing runs unaccounted for.

Least-Privilege Access

Agents are granted only the specific data and permissions their task requires, nothing more.

Full Audit Logging

Every action an agent takes is logged, logged, so activity can always be be reviewed and explained.

Shadow AI Detection

Unsanctioned or unmanaged AI tools running on company devices are surfaced and can be blocked.

MICROSOFT 365 E7

Security Copilot — An AI Analyst on Every Team

- **Included, not an add-on —** Every E7 tenant is automatically provisioned with Security Copilot capacity at no extra cost.
- **Faster phishing triage —** Reported phishing emails are automatically classified and prioritized for the security team.
- **Automated access reviews —** Routine identity and permission reviews are drafted for a human to approve, not built from scratch.
- **Guided vulnerability remediation —** When a weakness is found, Security Copilot recommends the exact fix in plain language.

A force multiplier, not a replacement

Security Copilot drafts the analysis; your accountable team — and ours — still makes the call. It removes the busywork, not the judgment.

SECTION THREE

24/7 Managed Detection & Response

Human-led monitoring across every endpoint and every identity — watching while you sleep.

MANAGED DETECTION & RESPONSE

Endpoint Protection, Watched by Humans

Artificial intelligence filters millions of signals down to what matters. Human threat hunters make the final call on every one of them, 24 hours a day. hours a day.

- **Every alert reviewed by a person —** Nothing reaches your team without a human analyst confirming it's real first.
- **Decisive response actions —** Confirmed threats trigger endpoint isolation, process termination, and file quarantine automatically.
- **Extremely low noise —** A sub-1% false-positive rate means your team only hears about what actually matters.
- **Managed antivirus included —** Built-in protection is centrally managed and kept current, with no separate licence to track.

~8 min

median time to isolate a confirmed threat

<1%

false-positive rate across all alerts

24/7

human analyst coverage, every day

MANAGED DETECTION & RESPONSE

Identity Threat Detection & Response

Identity is now the most common way into a business. This layer watches Microsoft 365 sign-ins and account activity around the clock for the patterns that precede a breach.

Session Hijacking

Automatically catches stolen session tokens being used to bypass multi-factor authentication.

Rogue Applications

Detects malicious third-party apps quietly granted access to a mailbox or files.

Foreign Logins

Flags sign-ins from unexpected countries or impossible-travel patterns instantly.

Business Email Compromise

Catches hidden forwarding rules and mailbox rules used to intercept wire transfers.

MANAGED DETECTION & RESPONSE

Detect → Isolate → Eradicate

The same disciplined process runs for every confirmed threat, whether it starts on an endpoint or inside an identity.

1

Detect

Behavioral patterns that bypass traditional defenses defenses are surfaced by AI and confirmed by human human analysts.

2

Isolate

The moment a threat is verified, the affected device or account is instantly and autonomously cut off.

3

Eradicate

The threat is completely removed and a clean incident report is delivered — operations never stop unnecessarily.

~3 min

median response to a confirmed identity threat

24/7

coverage across endpoints and identities alike

MANAGED DETECTION & RESPONSE

Continuous Security Posture Hardening

Prevention is always cheaper than recovery. This layer continuously audits configurations and closes the doors attackers look for, before they ever try the handle.

- **Endpoint posture management —** Devices are continuously checked against strict security baselines and snapped back when they drift. when they drift.
- **Identity posture management —** Microsoft 365 identity configurations are hardened continuously — fewer chances for attackers to abuse a misconfiguration.
- **Shrinking the attack surface —** Risky default settings are identified and corrected before they become the entry point of an incident.

MANAGED DETECTION & RESPONSE

Human-Risk Training & Phishing Coaching

A second, complementary layer of people-focused defense — beyond the platform-native simulation covered under Microsoft 365 E7.

Story-Driven Training

Short, engaging training episodes built by professional animators — content people actually finish.

Real-Attack Simulations Simulations

Phishing scenarios modeled on tradecraft observed across millions of real, active threats.

Behavior-Based Coaching Coaching

Repeat-risk users get targeted, individual coaching rather than a a one-size-fits-all course.

Gamified Engagement

Recognition and friendly competition keep participation and completion rates high.

MANAGED DETECTION & RESPONSE

24/7, Every Endpoint, Every Identity

The numbers behind a defense posture most 70-person firms could never staff on their own.

<1%	~8 min	~3 min	24/7
false-positive rate on endpoint alerts	median endpoint threat response	median identity threat response	human threat hunters, every day of the year

Artificial intelligence is powerful — but it takes an elite, global team of human threat hunters to outsmart a human attacker. That's attacker. That's the combination behind every alert you never had to see.

SECTION FOUR

Absolute Data Resilience

Immutable, ransomware-proof backup for everything your business runs on — including identity itself.

ABSOLUTE DATA RESILIENCE

Everything Backed Up, Including Identity

Most backup conversations stop at files and email. True resilience means protecting the identity infrastructure that controls access to everything else.

Exchange Online

Every mailbox, every folder, backed up on a continuous, automated schedule.

SharePoint & OneDrive

Document libraries and personal files protected against deletion, corruption, or attack.

Microsoft Teams

Chats, channels, and files inside Teams are captured, not just the files files people remember to save.

Entra ID (Identity)

Users, groups, applications, and access logs — the part of recovery most providers forget entirely.

ABSOLUTE DATA RESILIENCE

The Immutable Vault

- **Write-once, read-many storage —** Once a backup is written, it cannot be altered, encrypted, or deleted by anyone — including an administrator.
- **Virtually air-gapped —** Backup data lives isolated and decoupled from your production Microsoft 365 environment.
- **256-bit encryption —** Every backup is encrypted in transit and at rest, to the same standard used by regulated industries.
- **Built to survive an attacker with admin access —** Even a fully compromised administrator account cannot touch what's already in the vault.

Why immutability matters

Modern ransomware is engineered to find and destroy backups first, before encrypting production systems. A backup that can be deleted is not a backup — it's a second target.

ABSOLUTE DATA RESILIENCE

Ransomware Detection Inside the Backup Itself

Rather than waiting to discover an attack after the damage is done, a behavioral detection engine watches the backup data continuously for the earliest for the earliest signs of ransomware.

- **Behavioral anomaly detection —** Individualized behavioral profiles flag ransomware activity at the earliest possible stage, not after encryption completes.
- **Broad strain coverage —** Detection is tuned for accuracy across a wide range of ransomware families, not a narrow signature list.
- **One centralized threat view —** Ransomware alerts and native Microsoft malware alerts appear together in a single threat center.
- **Real-time alerting —** Your team is notified the moment suspicious activity is confirmed — not during a routine weekly check.

ABSOLUTE DATA RESILIENCE

Two Speeds of Recovery

Granular Recovery

One deleted email, one overwritten file, one Teams message — — restored in minutes without touching anything else. Most recoveries are this simple.

Large-Scale Recovery

When the incident is bigger — ransomware, a destructive mistake, a compromised tenant — high-throughput recovery restores users, sites, or entire workloads at the speed a real crisis demands.

ABSOLUTE DATA RESILIENCE

The Gold Standard: 3-2-1-1-0

We architect every backup to an uncompromising, industry-leading methodology — not the bare minimum.

3	2	1	1	0
Copies of your critical data	Different types of storage media	Copy safely stored offsite	Completely air-gapped, immutable copy	Errors upon recovery, guaranteed

Canadian data stays in Canada — all cloud backups are stored in top-tier Canadian data centres.

SECTION FIVE

Vulnerability Management & Penetration Testing

Continuous visibility into every exposure, automated remediation, and evidence ready for any audit.

VULNERABILITY MANAGEMENT

Seeing What Attackers See

Before an attacker can exploit a weakness, they scan for it. This engine runs the exact same reconnaissance daily — from the outside in.

- **Every exposed IP, port, and website —** A continuous external scan identifies every internet-facing asset across the business, not a one-time snapshot.
- **Known vulnerabilities (CVEs) —** Exposed systems are checked against the full published catalog of known software vulnerabilities.
- **Daily automated reports —** Results land automatically every day, with critical risks prioritized so nothing meaningful gets buried.
- **Zero added technician workload —** Continuous value delivered without anyone having to manually run or chase a scan.

VULNERABILITY MANAGEMENT

Mapping the Internal Network

External scanning shows the front door. Internal scanning shows everything an attacker would find after they're already inside.

Shadow Devices

Vulnerable IoT and unmanaged devices your team doesn't even know are connected.

Flat Networks

Poorly segmented networks that let one compromised device reach everything else.

Exploitable Hardware

Routers, switches, and endpoints endpoints with weaknesses found found before an attacker finds them them first.

Full Visibility

A complete, continuously updated map of every device on every network you operate.

VULNERABILITY MANAGEMENT

AI-Assisted Penetration Testing

- **A pen test that never goes stale —** Traditional penetration tests happen once a year at best. This runs continuously, all year round.
- **Meaningful coverage at a fraction of the cost —** Delivers roughly 70% of the insight of a traditional external penetration test — the kind that typically costs $10,000–$20,000 on its own.
- **AI-generated reporting —** Findings are compiled automatically into a clear, structured penetration-test-style report.
- **Prioritized by real exploitability —** Only vulnerabilities that are actually exploitable rise to the top, so effort goes where it matters.

Continuous beats annual

A once-a-year test only tells you about the day it ran. New exposures appear every week — continuous testing means you're never working from a stale picture.

VULNERABILITY MANAGEMENT

Automated Remediation, Not Just Alerts

Finding a problem is only half the job. This is the layer that actually closes it — automatically, and at scale.

7,000+ Applications Patched

Software across the estate is kept current automatically, without manual intervention per title.

Risky Software Removed

Unwanted or unsecure applications are identified and uninstalled automatically.

Firewall & AV Configuration

Security settings are enforced and and corrected to match a defined defined benchmark.

Ticketing Kept in Sync

Every automated fix updates your support system automatically, so nothing happens in the dark.

VULNERABILITY MANAGEMENT

Proving Compliance, On Demand

Regulators, insurers, and clients increasingly want evidence, not assurances. This engine turns continuous scanning into audit-ready proof.

Cyber Essentials	ISO 27001	SOC 2	NIST	Essential 8	HIPAA

- **Evidence, not opinions —** Every control is mapped directly to the framework language auditors and insurers actually ask for.
- **Hours, not days —** Audit preparation that used to take days of manual document-gathering now takes hours.
- **Always current —** Because scanning is continuous, your evidence reflects today's environment, not last year's snapshot.

VULNERABILITY MANAGEMENT

Closing the Identity Gaps

Multi-factor authentication is the lowest-hanging fruit for an attacker to target — which is exactly why it's audited continuously, not assumed. assumed.

- **MFA non-conformance reporting —** Every account without proper multi-factor authentication is surfaced automatically, including guest including guest users.
- **Guest and external account hygiene —** Third-party accounts with lingering access are flagged before they become the forgotten way in.
- **Estate-wide, not sample-based —** Every identity across the environment is checked — not a spot check of a handful of accounts.

BRINGING IT TOGETHER

How It All Works Together

1

Support

One team, unlimited calls, tickets, onboarding, and vendor coordination.

2

Foundation

Microsoft 365 E7 — productivity, AI, identity, and and compliance, unified.

3

Detect & Respond

24/7 human-led monitoring across every endpoint and identity.

4

Recover

Immutable backup of everything, including identity, tested and ready.

5

Prove

Continuous vulnerability management and audit-ready compliance evidence.

Five layers, one signal, one accountable team — that's the platform underneath every seat.

BRINGING IT TOGETHER

Everything Inside Your $300 Per User

- Microsoft 365 E7 — full productivity suite, Copilot AI, Entra Suite, Agent Suite, Agent 365
- Phishing & attack simulation training in 30+ languages
- 24/7 human-led endpoint detection & response
- 24/7 identity threat detection & response
- Continuous security posture hardening
- Human-risk security awareness training
- Immutable backup of mail, files, Teams & identity
- Built-in ransomware & malware detection
- Granular and large-scale disaster recovery
- Continuous external & internal vulnerability scanning
- AI-assisted penetration testing
- Automated remediation & compliance evidence

Unlimited calls & tickets, third-party vendor coordination, onboarding & offboarding, workshops, and standard projects — also included, always. always.

Questions?

All Your IT. One Flat Price. Zero Surprises.

Aptik · AI-First Managed IT · Edmonton & Saskatoon, serving Canada-wide

aptik.ca · **hello@aptik.ca**