



Ransomware Protection Plus

Product Overview





About

Ransomware Protection Plus is an ML-based solution that detects anomalous behaviour indicative of ransomware activity. It identifies and mitigates ransomware while ensuring seamless data recovery in the event of an attack.

The solution continuously monitors system behaviour even when it's offline to identify and neutralize sophisticated and emerging ransomware strains to maintain strict compliance and operational continuity.

The Problem

- **72% of businesses** hit by ransomware in 2023.
- Average ransom payment is around **\$1.5 Million**.
- **60% of SMBs** shut down within 6 months of an attack.
- **40% increase** in ransomware attacks in SMEs.
- Ransomware will cause its victims around **\$265 Billion** annually by 2031.





Consequences of a ransomware attack

- **Financial Loss:** Ransom payments, recovery costs, legal fees.
- **Operational Chaos:** Downtime, data loss, supply chain disruption.
- **Reputational Damage:** Loss of customer trust, compliance/regulatory fines.

Problem with traditional security

- **Signature-based tools miss sophisticated ransomware:** Signature-based tools rely on predefined patterns to identify known threats. By focusing on what ransomware does rather than what it looks like, behavioural detection offers proactive, adaptive protection against evolving threats.
- **Over-reliance on back ups:** Backup-deleting ransomware or anti-recovery ransomware employ tactics to hinder restoration efforts, ensuring victims cannot easily recover without paying the ransom. Traditional security tools lack the mechanism to counter this.



Overview

Proactive defense

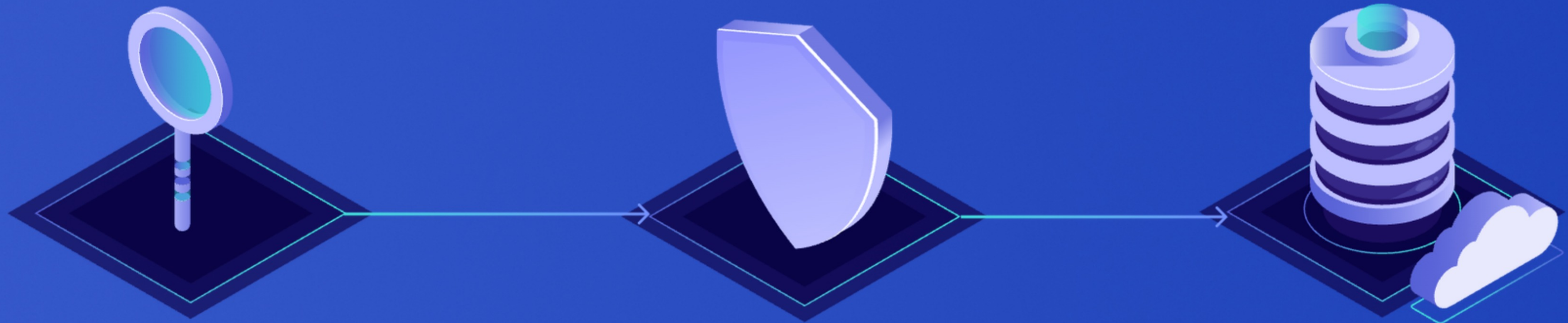
- AI-powered ransomware detection
- Memory-based ransomware protection
- Offline ransomware mitigation
- Exploit mitigation

Active protection

- Attack lifecycle analysis
- Pre-emptive incident mitigation
- Real-time device isolation Dynamic
- Encryption blocking

Rapid response and recovery

- Forensic investigations
- Instant endpoint recovery
- Repeat offender defense
- Adaptive kill-switch



Features of Ransomware Protection Plus



Ransomware detection

Behavioural detection:

Spot ransomware through abnormal system activity (like mass file encryption) in real-time, even for zero-day threats.

Fileless Malware

Protection: Block memory-based attacks that exploit trusted tools (PowerShell, WMI) to evade traditional scanners

Edge based detection:

Localized detection engine monitors endpoints to catch ransomware at the first sign of intrusion.

Attack Analysis and Forensics

Discover your attack chain: Visualize the ransomware's path—from initial breach to data recovery.

MITRE ATT&CK Mapping: Map attacks to frameworks like MITRE and VirusTotal to decode attacker tactics.

Indicators of Compromise (IoC): Flag known ransomware fingerprints (malicious IPs, hashes) to stop repeat attacks.

Response and Recovery

Tamper-proof backups:

Immutable backups ensure ransomware can't erase your recovery data.

Quick rollback and

recovery: Restore encrypted files/systems to pre-attack states in minutes.

Switch between Audit and

Kill mode: Test defenses in Audit mode, then activate Kill mode to neutralize live threats.

Withstand repeat attacks:

Auto-harden systems post-recovery to prevent attackers from striking twice

Why Ransomware Protection Plus?



Detect behaviour anomalies with ML

Identify ransomware by analyzing suspicious activity in real time.

Intercept ransomware mid-attack

Neutralize ransomware in its tracks, preventing encryption and minimizing damage.

Recover ransomware-encrypted files

Restore encrypted files instantly —no downtime, no ransom paid.

Protect from zero-day ransomware

Defend against never-before-seen ransomware attacks and emerging strains.

Unique differentiators

- **Your silent guardian:** Operates invisibly without slowing users or workflows with zero performance drag, even during full-system scans.
- **Learns and grows with you:** Centralized management scales effortlessly from startups to enterprises, adapting to growing IT ecosystems and evolving threats.
- **Effortless deployment:** Deploy enterprise-wide protection in minutes—no reboots, no downtime, no complex setups.
- **Cyber insurance and ROI advantage:** Ransomware risk reduction lowers premiums while being light on your security budget.
- **Adaptive defense:** Customize enforcement with modes—automated kill-switch or forensic audit—to match your cybersecurity posture.

Pricing

Free upto

25

Endpoints

Starts at

\$6.99

**per endpoint
annually**

**Available
On-premise**

Learn and Explore

[Home](#)

[Avail a free 30-day trial](#)

[Get quote](#)

[Free personalized demo](#)

[Getting started](#)

[Help documents](#)

