



AI-Powered Network Security

The Role of Managed Firewalls in Proactive
Threat Defence

White Paper

PROACTIVE[™]
Enhancing Digital Experience

Executive Summary

Boards now expect security teams to prove prevention, not just respond. Encrypted traffic, SaaS sprawl, remote work, and AI-driven attacks make manual firewall operations brittle. The path forward is an AI-powered operating model where a managed firewall run, delivered as a Cisco Powered service, becomes the control plane for prevention, detection, and audit evidence.

This paper sets out the business case, target architecture, operating cadence, and a 90-day plan to move from device ownership to outcome ownership. You leave with a 90-day plan and the five metrics that prove progress.

Industry signal: recent studies such as Cisco's Cybersecurity Readiness Index and the Verizon Data Breach Investigations Report highlight growth in webapp attacks and credential misuse, reinforcing the need for selective decrypt and outcome metrics.

Table of Contents

- Why AI Changes Network Security
- What "AI-Powered" Means In Practice
- Target Architecture For AI-Powered Managed Firewall
- Operating Model, From Devices To Outcomes
- Outcome Metrics That Matter
- Economics And Risk: The Business Case
- Outcomes At A Glance
- 90-Day Roadmap
- Buyer Due Diligence For Private Procurement
- Risks, Controls, And Mitigations
- Governance And Reporting
- What Good Looks Like After One Year

Glossary

Why AI Changes Network Security

Attacker economics have shifted

Commodity models generate convincing phishing at scale, mutate payloads, and probe misconfigurations faster than humans can review rules. Attackers chain identity, endpoint, and network signals. You need a policy and inspection that adapts hour by hour.

Defender data has exploded

Firewalls, proxies, identity providers, EDR, and SaaS audit logs produce rich telemetry. The value lies in correlation at speed, not in more dashboards. AI models that score risk on flows, users, and assets let you act before incidents spread.

Encrypted by default

TLS, QUIC, and HTTP/2 dominate. Blind spots grow if you decrypt everywhere or nowhere. The right answer is selective decryption backed by breakrate monitoring and error budgets. A managed run can hold that line every week.

Regulatory pressure

Regulators ask for timely reporting, clear timelines, and auditable controls. You need evidence on tap, not adhoc exports.

What “AI-Powered” Means In Practice

AI should live inside the run, not sit on a slide. In practice that means models that learn what normal looks like for your egress, east–west traffic, and SaaS use, then flag and rank the oddities that matter. It means hygiene tasks that humans avoid, rules without hits, objects without owners, duplicate entries, are queued for retirement with a clear owner and an approval path.

Change requests carry a risk score based on blast radius and conflict history, so high-risk items demand pre-checks or smaller windows. When alerts pile up, naturallanguage summaries stitch events into an incident timeline and propose next actions. Most importantly, every resolved event updates the playbook, so the run improves rather than resets. AI augments expert operators. Humans still decide policy intent and approvals.

Target Architecture For AI-Powered Managed Firewall

The architecture starts with control points at the edge, branch, cloud entry, and datacentre gateways. Identity, endpoint, and asset sources provide context so policy can align to people and devices, not just IPs. A central policy service holds templates, exceptions, and drift signals so changes land the same way every time.

Traffic treatment follows simple rules. Decrypt where it is lawful and useful, typically browser and API traffic, and keep industrial or clinical device portals outside the decrypt. Use application-aware controls and DNS security to reduce blind spots without adding latency.

Data fuels the system. Flow logs, DNS logs, change logs, and identity events feed a feature store. Models score anomalies close to real time, then run hygiene jobs each week to find stale rules and unused objects. Outcomes flow back into policy, closing the loop.

Evidence stays ready. Reports map to ISO 27001 and local reporting rules. Dashboards surface outcome metrics leaders care about, not device counters.

Operating Model, From Devices To Outcomes

A managed run moves value from owning devices to proving outcomes. Clients retain policy intent and full visibility. The provider operates to an agreed runbook with named owners.

Roles stay clear. The client policy owner defines intent, approves change, and owns exceptions. The run team executes change, tunes inspection, manages incidents, and reports metrics. A platform lead ensures capacity, clustering, and automation fit the load.

Cadence creates trust. Each day starts with an anomaly review, tidy-ups for stale rules, and a scan of queued changes. Each week closes with published metrics and actions. Each month, reviews exceptions and the noisiest rules. Each quarter proves readiness with an audit drill and evidence in forty-eight hours.

Guardrails keep discipline. A shared console provides role-based write so you always see who changed what, when, and why. Standard templates shape branches, factories, and cloud edges. Vendor access stays time-bound, with auto-expiry and a full audit trail.

Outcome Metrics That Matter

Senior leaders want trend lines, not counters. The policy-to-incident ratio shows whether hygiene keeps pace with change. Ruleage distribution reveals neglect before it becomes a risk. Changesuccess rate tells you whether windows hold and rollbacks are rare. Mean time to detect and mean time to respond track how fast the run sees and resolves issues. Decrypt break rate confirms that selective policies protect users without collateral outages. Each metric needs an owner and a weekly target. Miss a target, assign an action and a date.

Economics And Risk, The Business Case

Boards ask cost first, risk second, and delivery impact third. A mature managed run often costs less than a full-time security engineer when you factor nights, weekends, and specialist cover, and the model scales across sites from day one.



Directional total cost of run (illustrative)

Run coverage 24x7, weekend and holiday cover, specialist time, platform ops, planned change windows, and audit support versus 1 FTE salary, oncall, backfill, and churn risk. The aim is not to undercut a salary; it is to start now with full coverage and predictable outcomes.

Track risk reduction with baselines. Measure fewer incidents, shorter outages, and fewer

audit findings against prerun levels, then link gains to revenue or customer experience, for example smoother checkouts, more stable live classes, or higher plant uptime.

Contract strength matters in private procurement. Time-bound access and evidence on tap reduce client audit risk for IT and ITes providers and help win work in regulated sectors.

Outcomes At A Glance

We measure outcomes, not promises. Here is what buyers care about most:



PACS without dropouts, healthcare

Selective decrypt for browsers, clinical portals exempt. Incidents down, audit prep time cut from weeks to days.

Lines and cells, not flat networks, manufacturing

Zones and conduits isolate lines and cells. Industrial DPI enforces function allow lists. Egress pinned to known regions. Unplanned downtime from network events near zero.

Lines and cells, not flat networks, manufacturing

Zones and conduits isolate lines and cells. Industrial DPI enforces function allow lists. Egress pinned to known regions. Unplanned downtime from network events near zero.

Checkout stays fast, retail

Store and DC segmentation keep POS away from the guest WiFi and cameras. Egress is pinned to CDNs and payment regions. Flashsale latency stable, fewer cart errors.

Projects without drift, ITes

Project segments connect to client VPCs with tagged owners. Time-bound contractor access expires by default. Weekly metrics show drift early.

Sector Outcomes, Before And After

Sector	Before	After	Time to result
Healthcare	TLS breaks during uploads, weeks to prepare audit	Stable uploads, evidence in days	4–8 weeks
Manufacturing	Flat network, linewide impact	Zones and conduits, incidents halved	6–8 weeks
Retail	Checkout latency spikes in promos	Stable latency, fewer cart errors	4–6 weeks
ITes	Rule sprawl, afterhours rollbacks	Tagged rules, 98% change success	6–8 weeks

90-Day Roadmap

First month, establish the baseline. Remove duplicate and shadow rules, tag owners, and switch on selective decrypt for browser flows while pinning exemptions for sensitive apps. Publish the outcome metrics so everyone sees the starting point.

Second month, the segment where it moves risk. Pick two plants, two stores, or two key projects. Add east–west inspection and allow lists for the protocols and APIs that matter most. Introduce time-bound vendor access with auto-expiry and make it the default.

Third month, tighten the edges. Constrain SaaS egress and Altool access by region. Run an audit drill and produce evidence within forty-eight hours. Close the quarter by agreeing nextquarter targets based on the trend lines you now have.

Readiness checklist

- Named client policy owner and approvers
- Source of identity and device posture confirmed
- Inventory of sensitive portals exempt from decrypt
- Initial zone and conduit map for two pilot sites or projects
- Logging pipeline validated for flow, DNS, and change logs

Buyer Due Diligence For Private Procurement

Private buyers still need structure, even without an RFP. Replace forms with evidence. Ask vendors to walk you through their daily, weekly, monthly, and quarterly cadence. See a live demo of anomaly detection on flows and policy hygiene, not a slide. Review a selectivedecrypt policy with breakrate monitoring and show how exemptions stay time-bound.

Inspect a real exception registry and an audit trail with requester, approver, scope, start and end time. Open a sample evidence pack mapped to ISO 27001 and local reporting rules. Finally, agree on the outcome metrics you will see every week, with named owners and actions. If they cannot show it live in ten minutes, treat it as unproven.

Risks, Controls, And Mitigations

Models drift and can create false positives. Keep human approval for policy changes, run models in shadow mode before enforcement, and backtest against recent incidents. Privacy and lawfulintercept needs vary by jurisdiction. Keep sensitive portals out of decrypt, apply selective policies with documented exemptions, and involve legal and compliance in reviews.

Throughput and latency can suffer if the inspection is mismatched to the load. Validate at target traffic, use hardware crypto, and cluster where needed. Skills are scarce. Use a named run team with crosscoverage, publish runbooks, and practise handovers.

Governance And Reporting

Governance should make control visible without slowing work. Keep a shared console with role-based write so every change carries a requester, approver, scope, start time, and end time. Hold a weekly review for metrics and actions and a monthly session for exception hygiene. Align quarterly reports to audit windows and keep evidence packs ready to export. The provider prepares evidence, you approve and submit within the regulatory window. Record playbook updates and lessons learned so improvements persist after people rotate.

What Good Looks Like After One Year

One year in, the policytoincident ratio trends down even as the rate of change rises. Rule age is under control, with most rules reviewed within ninety days. Change success sits above ninety-eight per cent, and rollbacks are rare and fast. Mean time to detect stays under fifteen minutes for highconfidence events, and mean time to respond under sixty minutes. Audit packs are produced within forty-eight hours, and findings drop across cycles. A trend table appears in the appendix.

Glossary

AI model

A program that learns from data to score risk on flows, users, or assets.

Anomaly detection

A method that baselines normal use and flags meaningful deviations for review.

Selective decrypt

TLS inspection applied where lawful and useful. Keep sensitive portals out. Track break rate.

Zones and conduits

A way to group assets and control the paths between them. Common in ISA or IEC 62443.

Eastwest inspection

Checks traffic inside the network to stop lateral movement and data leaks.

Outcome metrics

Weekly measures that show risk and operations, policy to incident, rule age, change success, MTTD, MTTR.

Feature store

A data store that holds processed fields used by models.

Break rate

The share of sessions that fail after decrypt. Watch it to protect users.

Time-bound access

Vendor or contractor access that has an owner, scope, start and end time, and auto expiry.

Policy hygiene

The practice of keeping rules and objects current, with owners and expiry.

Conclusion: Do Less, Achieve More

Cloud-managed networking doesn't just shrink your hardware footprint. It reduces decision fatigue, support load, and compliance risks. It lets your team focus on business, not troubleshooting. And it makes every new hire, location, or client just another tab on a dashboard.

Stop firefighting. Start scaling. Partner with Proactive Data Systems to simplify your IT, secure your network, and grow your business.

Write to us at pro@proactive.co.in or

Visit proactive.co.in/firewall to learn how we can help.



Proactive Data Systems is an IT infrastructure and services company that designs, deploys, and supports secure, high-performance technology environments for organisations that cannot afford downtime. With over 35 years of experience, we have enabled more than 1,500 enterprises across India to modernise their networks, strengthen security, and scale with confidence.

Recognised as a Cisco Preferred Partner across Networking, Security, Cloud & AI, and Collaboration, Proactive combines deep systems integration capability with disciplined delivery and managed services. Our expertise spans enterprise networking, cybersecurity, data centres, collaboration platforms, and structured cabling. We build and run infrastructure that performs reliably every day, not just at go-live.

To learn more about our solutions, write to us
at pro@proactive.co.in

 www.proactive.co.in

PROACTIVE™
Enhancing Digital Experience