

Unified Security Intelligence That Prevents Breaches and Wins Deals

Preventative cybersecurity for MSPs and lean IT teams. Correlating endpoint, identity, cloud, SaaS, and compliance signals.



The dashboard provides a comprehensive overview of system health and security. Key sections include:

- EXECUTIVE OVERVIEW:** Shows 4316 suspected breaches detected, including 4106 signals from Microsoft 365 and 210 signals from Google Workspace.
- Device Overview:** Displays 532 total devices, with 279 online now, 3857 patches needed, and 294 needing restart. Platform distribution includes 406 Windows, 46 macOS, and 35 Linux devices.
- Issues Requiring Attention:** Lists 41 AV issues, 46 low disk space warnings, 6 high CPU usage alerts, 125 high memory warnings, 88 configuration issues (23 critical, 65 high), 44 overheating alerts, 294 restarts needed, 365 residential connections, 78 bad batteries, 202 aging computers (3+ years), 89 aging computers (5+ years), and 1 low printer supply.
- Cloud Security:** Details Microsoft 365 and Google Workspace security, including 296 users without MFA, 17 users without 2SV, 3 risky OAuth apps, 0 risky OAuth apps, 173 AI apps, 94 new apps (30 days), 690 external users, and 1589/2083 license usage.
- Top Missing Patches:** Lists critical updates for Microsoft Edge (2400 devices), Google Chrome (475 devices), Zoom Workplace (67 devices), Cisco Webex (53 devices), LibreOffice (45 devices), Mozilla Firefox (42 devices), Git (35 devices), ScreenConnect CL... (20 devices), Wireshark (18 devices), OpenSSL (17 devices), Firefox (14 devices), and Postman x86_64 (14 devices).
- Recent Alerts:** Shows critical alerts for login compromise followed by data theft at Calgary Foothills Primary Care Network.
- Internet Vulnerability:** Features a radar chart for faceskinandbody.ca with scores for Admin (44), Web (104), Domain (2), and Encrypt (21).
- Compliance:** Shows progress for CFPCN (0%), SGB (80%), TEST ONLY (4%), and ThreeShield (6%).
- Device Locations:** A world map showing 454 devices with location data.
- Replacement Priorities:** A table listing hardware items like SHIPPING-3, SHIPPING-4, DNA, TS-RA-M700-2, GUSTAVO-PC, CFCN-MS02, Megan, and DESKTOP-PH8R4IE with their respective years, reasons, and scores.
- Low Consumables:** A table for printer status, showing NPID72AC5 with 99% toner and 18% drum levels.

THE PROBLEM

The Security Stack Is Fragmented—and Failing

Siloed Tools

Security tools operate in silos across endpoint, cloud, identity, and network.

Alert Noise

Alerts lack context, creating noise instead of clarity for teams.

Manual Burden

Lean IT teams and MSPs lack time for manual correlation.

Reactive Compliance

Compliance visibility is reactive and incomplete.

Result: Breaches go undetected, incidents escalate, and trust is lost.

The Cost of Blind Spots Is Rising

85%

SMB Reliance

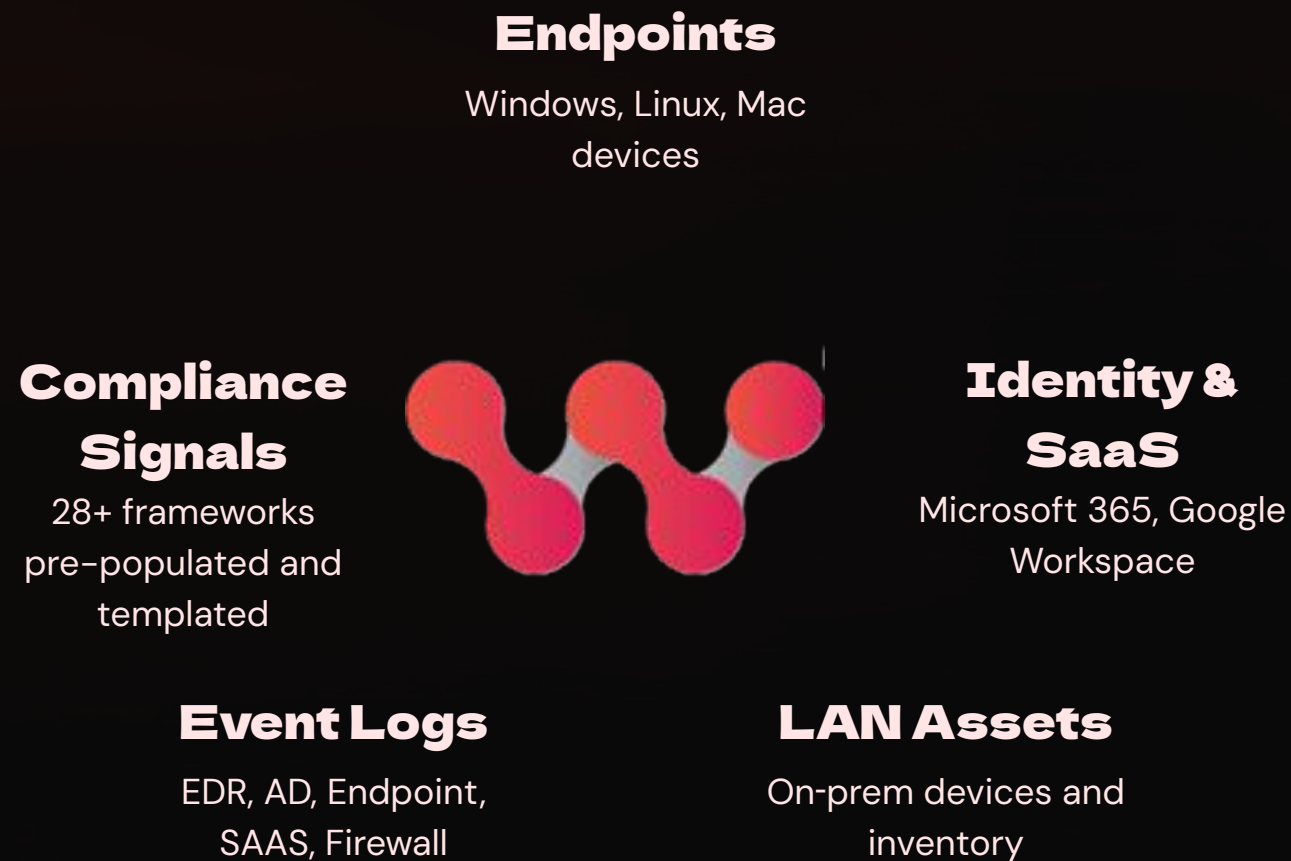
SMBs rely on MSPs or small IT teams for security

- Cloud-first attacks bypass traditional perimeter tools
- Compliance expectations increase without added staff
- Customers expect answers, not alerts

Security must move from reactive tooling to preventative intelligence.



A Preventative Security Intelligence Layer



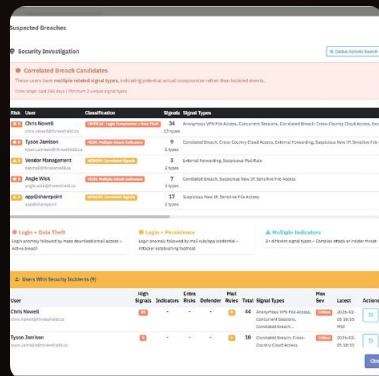
Lavawall consolidates and correlates signals across your entire security stack:

- Endpoints (Windows, Linux, Mac)
- Identity & SaaS (Microsoft 365/Entra, Google Workspace)
- LAN assets and network visibility
- OS and application event logs
- Configuration, patching, and GRC compliance

Lavawall explains *why* issues occur and *where* to act.

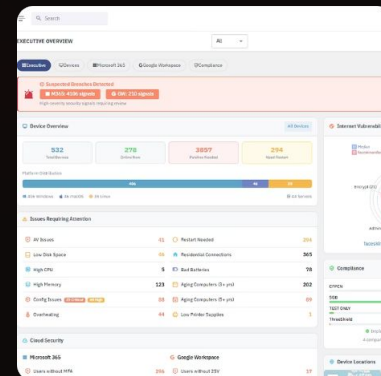
What Makes Lavawall Different

Correlation, Context, and Explanation



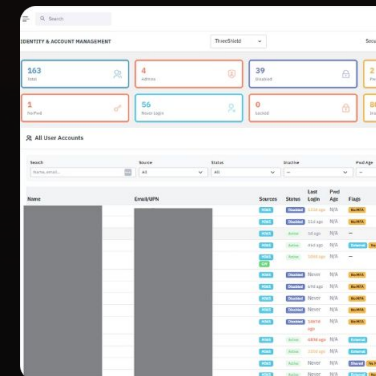
Signal Correlation

Cloud alerts correlated with device and user behavior



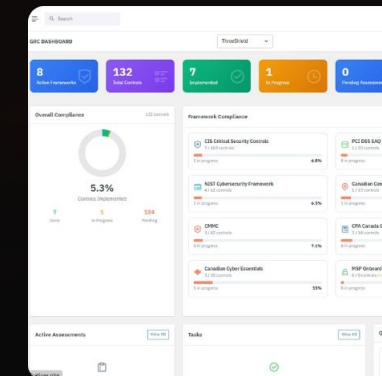
Multi-Platform Analysis

Event logs analyzed across OS platforms



Identity Integration

Identity risks tied to endpoint and network state



Continuous Compliance

Compliance gaps surfaced continuously, not during audits

This depth exposes issues other tools miss—and reduces false positives.

Legacy competitors

Vulnerability Scanners
Lavawall: Full domain coverage,
but less deep

RMM Tools
300x patching
30% efficiency gain
Integrated sales



Patch and Config
Lavawall: 300x coverage

SIEM & Alerts
Lavawall: Automated correlation with
lower data storage; fewer false
positives by correlating with endpoint
data

M365 tools like SaaS Alerts and Petra
have false positives without device
correlation

Lavawall is the MSP sales engine with that correlates cloud, endpoint, endpoint, network, patches, configurations, and events for world-class security

Fewer Fires, Faster Resolution



Earlier Detection

Breach detection through cross-signal correlation



Reduced Fatigue

Less alert fatigue for lean teams



Faster Analysis

Quick root-cause identification



Proactive Fix

Remediation before users complain

Customers resolve issues faster and avoid costly escalations.



Security Insight That Wins Deals



Insight-driven outreach achieves 20% meeting rates (10× industry-average)

- Demonstrated risk visibility drives near-100% conversion in early pilots
- Clear findings expand managed security attach rates
- Providers differentiate by showing risks competitors miss

Lavawall turns security depth into sales leverage.

Built for MSPs and Lean Internal IT



Managed Service Providers

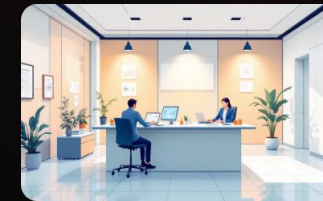
MSPs managing
50–5,000+ endpoints
across multiple clients

Primary focus: U.S. and North American expansion



Internal IT Teams

Teams without
dedicated SOC
resources needing
unified visibility



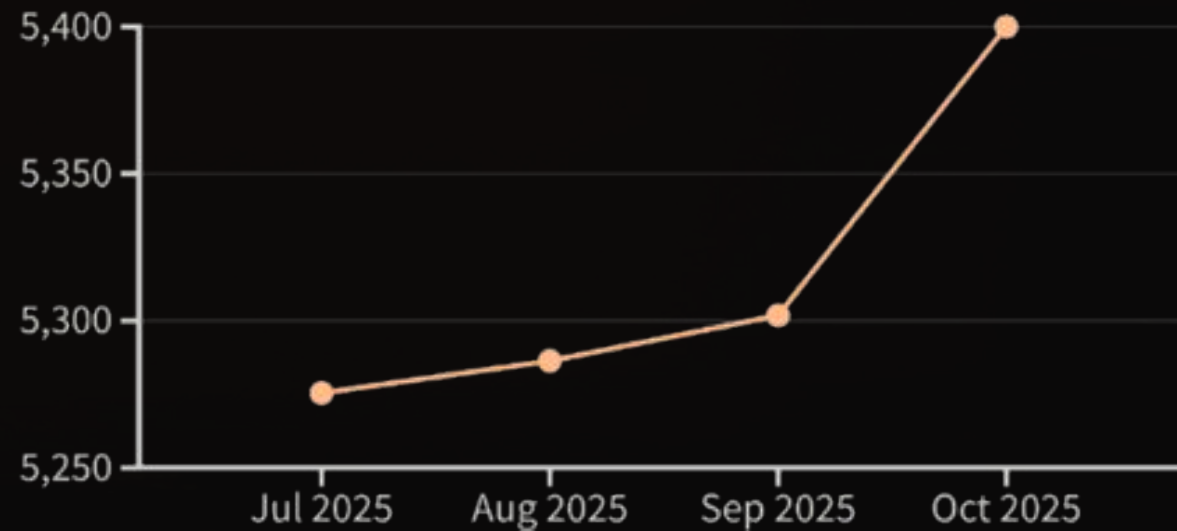
Compliance-Sensitive Industries

Accounting,
professional services,
and regulated SMBs

Early Validation & Traction

50+

Active Companies
ICP + Non-ICP



Domains scanned with Lavawall

Full Per Computer

C\$1.75/device/mo

No-brainer add on vs. \$1.25M average breach Cost

Marketing Only

C\$100 monthly



Risks & Mitigations

Adoption: change resistance

- Low-friction entry tier
- Agentless option
- Proven conference conversion

Competitive Risk

- Application approach and stagnation at 25 vs 7,533
- Focus on operations vs. prospecting & retention

Security & Privacy

- Canadian hosting
- Minimal data retention
- Zero-trust encryption
- SOC2 roadmap
- Developed by auditors

Scaling

- RDS optimized
- Multi-host platform

Distribution

- Conference strategy
- Partner pull-through

Price sensitivity

- Proven sales benefit
- Tiered pricing

Dependencies

- API Change monitoring
- Cache & batch approach

Execution

- IRAP enabling hiring
- Modular codebase

Compliance

- Founder with 25 years of compliance experience

Initial Market Focus

41 Priority MSPs in Calgary & Edmonton



C\$3.5M ARR

Potential ARR from initial target group

\$5.3M ARR of 3-year North America serviceable market including early adopting internal IT teams

65,000 North American MSPs



C\$5.5B ARR

Total ARR North American Opportunity

The Team Behind Lavawall



Chris Nowell

- 25 years of cybersecurity
- Space Shuttle to fintech
- CISSP, CISA, MBA



Saad Alkafir

- Transformed Lavawall to a scalable, cross platform powerhouse
- Security degree and certifications



Tyson Jamison

- DevOps & MSP experience
- Application hunter
- Cybersecurity diploma and certs



Angie Wisk

- High-growth startup experience
- Efficiency, relationships
- MBA with MSSP experience

Seeking Customers, Partners, and Investors

Our Goal

Make preventative security intelligence the new standard

01

U.S. MSPs & Lean IT Teams

Adopt and validate Lavawall

02

Strategic Partners

Accelerate distribution and market reach

03

Investors

Scale marketing, sales, and channel execution