WILLAMETTE VALLEY IDENTITY & SECURITY ASSURANCE

See what is exposed. Prove what is protected. Choose the right level of assurance.

Willamette Valley Identity & Security Assurance gives customers a clear answer to three urgent questions: what is on the network, what is exposed to risk, and what should be fixed first. This guide shows exactly what each run type includes, how deep the visibility goes, and where the limits are.

What the customer walks away with

- A clear customer-ready security report
- Prioritized findings with practical remediation guidance
- A visible explanation of what was reviewed, what was discovered, and what still needs deeper validation

Run Types At A Glance

Proof of Concept is the low-friction entry. Starter Scan is the main seller for most homes and small businesses. Standard Review adds router, DNS, and exposure insight. Premium Deep Review adds the strongest fix-first roadmap and business-grade report delivery.

Commercial tiers: **Proof of Concept $29** — **Starter Scan $69** — **Standard Review $149** — **Premium Deep Review $299** — **Small Business Security Review $499**. Add monthly local rescans for $20/month.

WVISA PROOF OF CONCEPT

$29

WVISA Proof of Concept - score, top issues, and light report

Low-friction entry tier with a security score, top issues, and lightweight local network awareness from the assessed device.

Included

- Local device security review
- Backup readiness review
- Local network exposure and visibility analysis
- Light endpoint-observed local discovery with no router login and a smaller probe footprint.

Best For

- Lead generation and first-touch customer conversations
- Customers who want a score and a few issues before committing to a deeper review
- Low-noise assessment with a small probe footprint

Not Meant For

- Prioritizes only the top issues instead of the full finding set
- No router login or router-backed inventory
- No open-port sampling or full remediation plan

Run Depth

- Light endpoint-observed local discovery with no router login and a smaller probe footprint.

WVISA STARTER SCAN

$69

WVISA Starter Scan - full device and network baseline

Mainline scan for homes and smaller environments: full report, risk breakdown, remediation steps, and stronger local network visibility without router credentials.

Included

- Local device security review
- Backup readiness review
- Account security review
- Identity risk review
- Local network exposure and visibility analysis
- Application security review
- Expanded endpoint-observed discovery with bounded active checks, open-port sampling, and device naming enrichment on the reachable local segment.

Best For

- Most customer assessments when router credentials are not available
- Homes and small businesses that want the mainline WVISA report package
- Customers who want device, account, identity,

Not Meant For

- Router-backed guest and IoT visibility is not included
- No authenticated router ingestion or device trust map
- Guest and isolated IoT networks may not be fully visible

- Bounded local discovery budget: up to 64 candidate targets and about 45 seconds of discovery time.

application, and local network coverage in one run

Run Depth

- Expanded endpoint-observed discovery with bounded active checks, open-port sampling, and device naming enrichment on the reachable local segment.
- Bounded active discovery: up to 254 candidate targets, about 120 seconds of discovery time, TCP confirmation on up to 24 devices, and port sampling on up to 20 devices.

WVISA STANDARD REVIEW

$149

WVISA Standard Review - deeper exposure and router insight

Everything in Starter Scan plus network exposure checks, router and DNS insight, configuration context, and stronger visibility across segmented Wi-Fi environments.

Included

- Local device security review
- Backup readiness review
- Account security review
- Identity risk review
- Router posture and supported-router evidence review
- External attack surface review
- Local network exposure and visibility analysis
- Family safety review
- OS hardening and remote-access review
- Application security review
- Expanded local discovery plus supported-router ingestion, which can improve coverage across main, guest, and IoT segments.

Best For

- Customers who want stronger visibility into what attackers can see
- Homes and small businesses with guest networks,

Not Meant For

- May request router IP and admin login on supported routers
- If router credentials are

WVISA PREMIUM DEEP REVIEW

$299

WVISA Premium Deep Review - priority roadmap and deepest customer review

Everything in Standard Review plus priority risk scoring, what-to-fix-first guidance, and the strongest customer-facing deep review package.

Included

- Local device security review
- Backup readiness review
- Account security review
- Identity risk review
- Router posture and supported-router evidence review
- External attack surface review
- Local network exposure and visibility analysis
- Family safety review
- OS hardening and remote-access review
- Application security review
- Widest local probe budget plus supported-router ingestion for the strongest visibility WVISA currently offers.

Best For

- Customers who want the clearest fix-first roadmap
- Larger households, denser Wi-Fi environments,

Not Meant For

- May request router IP and admin login on supported routers
- Still bounded for safety and

IoT segments, or DNS concerns
- Assessments where router-assisted context materially improves trust

not supplied, guest/IoT visibility may be partial
- Does not include the strongest priority-ranked fix roadmap

Run Depth

- Expanded local discovery plus supported-router ingestion, which can improve coverage across main, guest, and IoT segments.
- Bounded active discovery: up to 510 candidate targets, about 210 seconds of discovery time, TCP confirmation on up to 48 devices, and port sampling on up to 32 devices.

and premium technical reviews
- Situations where prioritized remediation matters more than raw detail alone

endpoint tolerance
- Small Business scope adds recurring local rescans, consultation, and multi-device service on top of this engine

Run Depth

- Widest local probe budget plus supported-router ingestion for the strongest visibility WVISA currently offers.
- Bounded active discovery: up to 1022 candidate targets, about 300 seconds of discovery time, TCP confirmation on up to 72 devices, and port sampling on up to 40 devices.

WVISA SMALL BUSINESS SECURITY REVIEW

$499

WVISA Small Business Security Review - premium recurring local rescan coverage

Premium scope for multi-device environments, recurring local rescans, consultation-led delivery, VLAN and multi-network visibility, and operator review on top of the Pro engine.

Included

- Local device security review
- Backup readiness review
- Account security review
- Identity risk review
- Router posture and supported-router evidence review
- External attack surface review
- Local network exposure and visibility analysis
- Family safety review
- OS hardening and remote-access review
- Application security review
- Widest local probe budget plus supported-router ingestion for the strongest visibility WVISA currently offers.

Best For

- Small-business and premium guided engagements
- Customers who want recurring

Not Meant For

- Quoted scope instead of fixed self-service pricing
- Timing and deliverables may

local rescans instead of one-time delivery

- Multi-device environments that benefit from operator-led follow-through, white-hat validation, VLAN visibility, and fuller routed-network inventory

include operator review and consultation

- Underlying technical engine follows the Pro assessment depth, carries forward router-backed segmented and VLAN networks, and can add external-vantage white-hat evidence when provided

Run Depth

- Widest local probe budget plus supported-router ingestion for the strongest visibility WVISA currently offers.
- Bounded active discovery: up to 1530 candidate targets, about 420 seconds of discovery time, TCP confirmation on up to 96 devices, and port sampling on up to 56 devices.

Feature Comparison

This matrix is tied directly to the current product logic, so it reflects what WVISA actually does today rather than sales-only wording.

Feature	WVISA Proof of Concept $29	WVISA Starter Scan $69	WVISA Standard Review $149	WVISA Premium Deep Review $299	WVISA Small Business Security Review $499
Customer-facing report	Included	Included	Included	Included	Included
Remediation checklist + admin-approved commands	Limited guidance	Included	Included	Included	Included
Device security review	Included	Included	Included	Included	Included
Backup readiness review	Included	Included	Included	Included	Included
Account security review	No	Included	Included	Included	Included
Identity risk review	No	Included	Included	Included	Included
Application security review	No	Included	Included	Included	Included
Family safety review	No	No	Included	Included	Included
OS hardening / remote access review	No	No	Included	Included	Included
Router security review	No	No	Included	Included	Included
External attack surface review	No	No	Included	Included	Included
Local network visibility depth	Light	Expanded	Router-assisted	Maximum	Maximum
TCP confirmation of discovered devices	No	Included	Included	Included	Included
Open-port sampling on observed hosts	No	Included	Included	Included	Included
Reverse DNS / device naming enrichment	Included	Included	Included	Included	Included

Feature	WVISA Proof of Concept $29	WVISA Starter Scan $69	WVISA Standard Review $149	WVISA Premium Deep Review $299	WVISA Small Business Security Review $499
Router login request	No	No	Requested when available	Requested when available	Requested when available
Guest / IoT visibility via supported router login	No	No	Supported router only	Supported router only	Supported router only
Trust / communication view	Basic local view	Local-segment view	Router-informed	Router-informed	Router-informed

Important Visibility Notes

Routerless tiers are honest, not magic

Proof of Concept and Starter Scan can do useful local-segment discovery without logging into the router, but they only see what the assessed device can observe on the reachable LAN. Isolated guest and IoT networks may remain partially hidden.

Standard Review and Premium Deep Review may ask for router access

On supported routers, Standard Review and Premium Deep Review may request the router IP and admin login so WVISA can ingest the router's client table and improve coverage across main, guest, and IoT segments. Coverage still depends on router support and network design.

Note: Actual visibility varies based on endpoint permissions, security software, network segmentation, sleeping devices, and whether supported router credentials are available during the run.

Monthly Monitoring Add-On — $20/month

Available as an add-on to any paid tier. Run a monthly local re-scan, track your score over time, and review change notes in the generated report. This is not a 24/7 monitoring agent or emergency response service.

What is included

- Monthly local re-scan using the same profile as the original paid scan
- Score tracking across runs — see if you are improving, stable, or declining
- New risk detection and change notes when findings differ from the prior run
- New-device notes when a monthly run sees devices that were not present in the prior baseline
- Side-by-side comparison against the prior run

How it works

The add-on attaches to any Proof of Concept, Starter Scan, Standard Review, or Premium Deep Review engagement. The report for each monthly run follows the same content-gating rules as the original tier, and Small Business Security Review can layer recurring service, operator review, and routed-network follow-through on top when needed.