Security in Your Pocket: AI Risk Assessment for Cloud-Native SMBs

CONF42 CLOUD NATIVE 2026

VAISHALI MAHAVRATAYAJULA · AI SECURITY ARCHITECT, WELLS FARGO

The Challenge

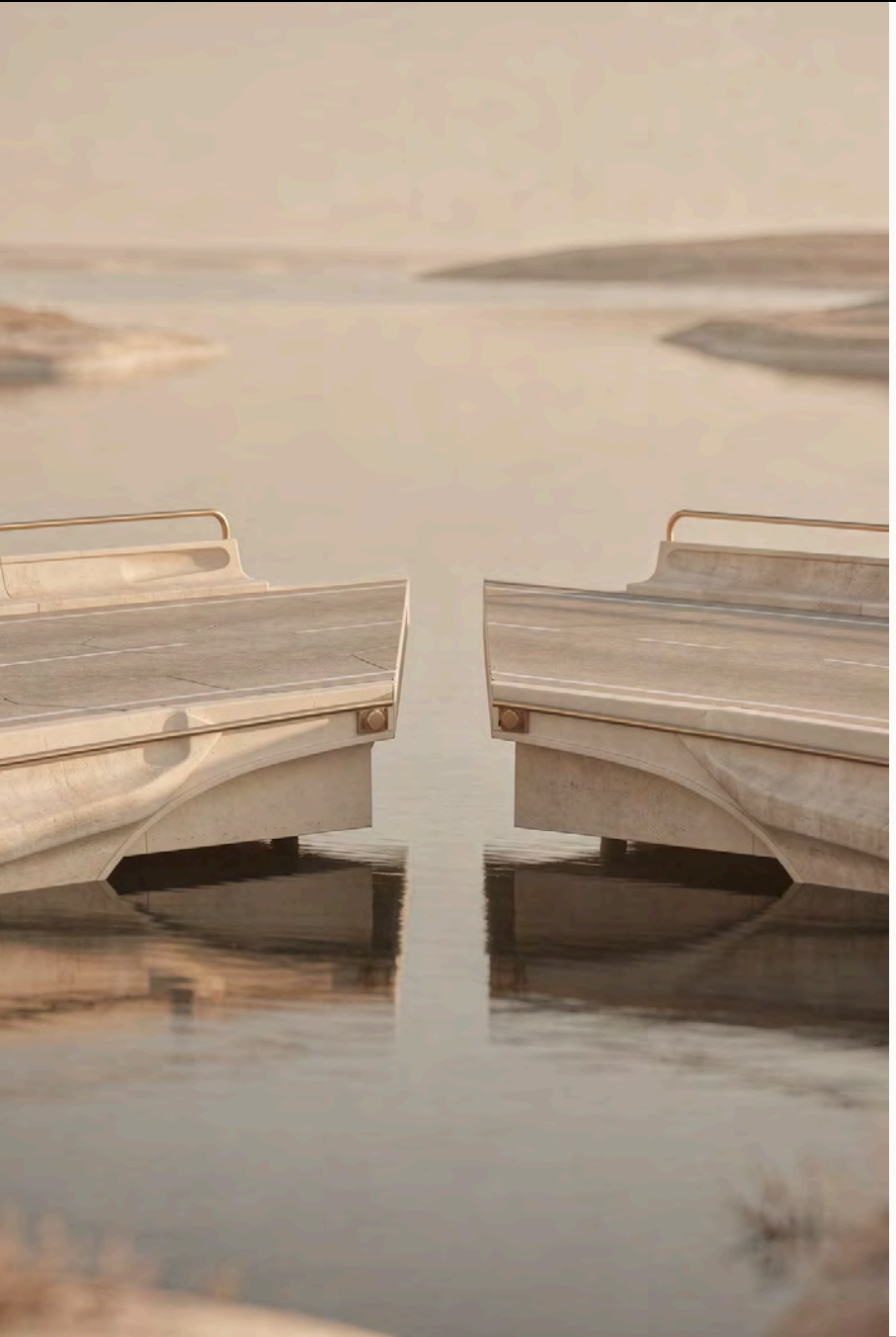
Small Businesses Are Going Cloud-Native — Fast

Today's small and home-based businesses run on a complex, distributed web of digital infrastructure. E-commerce SaaS platforms, serverless backends, third-party APIs, cloud storage services, and social media integrations have replaced the simple website of a decade ago.

This shift creates a **digital footprint that is distributed, dynamic, and inherently difficult to secure** especially without a dedicated IT team. The attack surface grows with every new tool adopted, and most owners don't even know what they're exposed to.

What a Typical SMB Runs Today

- E-commerce platform (Shopify, WooCommerce)
- Payment processor APIs
- Cloud storage (AWS S3, Google Drive)
- SaaS marketing & CRM tools
- Social media integrations
- Serverless functions & webhooks
- AI-powered plugins & chatbots



The Cloud-Native Security Gap

A widening divide exists between where small businesses operate and what security tools are designed to protect.

Enterprise Platforms

Built for complex ownership models, DevSecOps pipelines, and dedicated security teams. **Far too complex** for a 5-person business.

Consumer Tools

Designed for personal use antivirus, password managers. They **overlook business-level risk** entirely: APIs, SaaS configs, cloud exposure.

The SMB Reality

No security team. No DevSecOps. No budget for consultants. Yet **real business risk** exists and grows with every cloud tool adopted.

Four Systemic Gaps Facing Cloud-Native SMBs

The **securemystore.ai** framework was designed by identifying and directly addressing four root-cause security failures specific to small businesses operating in cloud-native environments.

1

Limited Cloud Asset Visibility

Owners don't have a complete picture of their own digital footprint. Forgotten APIs, shadow SaaS, and unmonitored cloud buckets create invisible exposure.

2

No Clear Security Ownership

In small businesses, no one "owns" security. Responsibility falls between the business owner, a web developer, and a hosting provider with critical gaps in between.

3

Uncontrolled Third-Party & AI Tool Exposure

Plugins, integrations, and AI-powered tools are adopted without vetting. Each one introduces data flows and permissions that may never be reviewed.

4

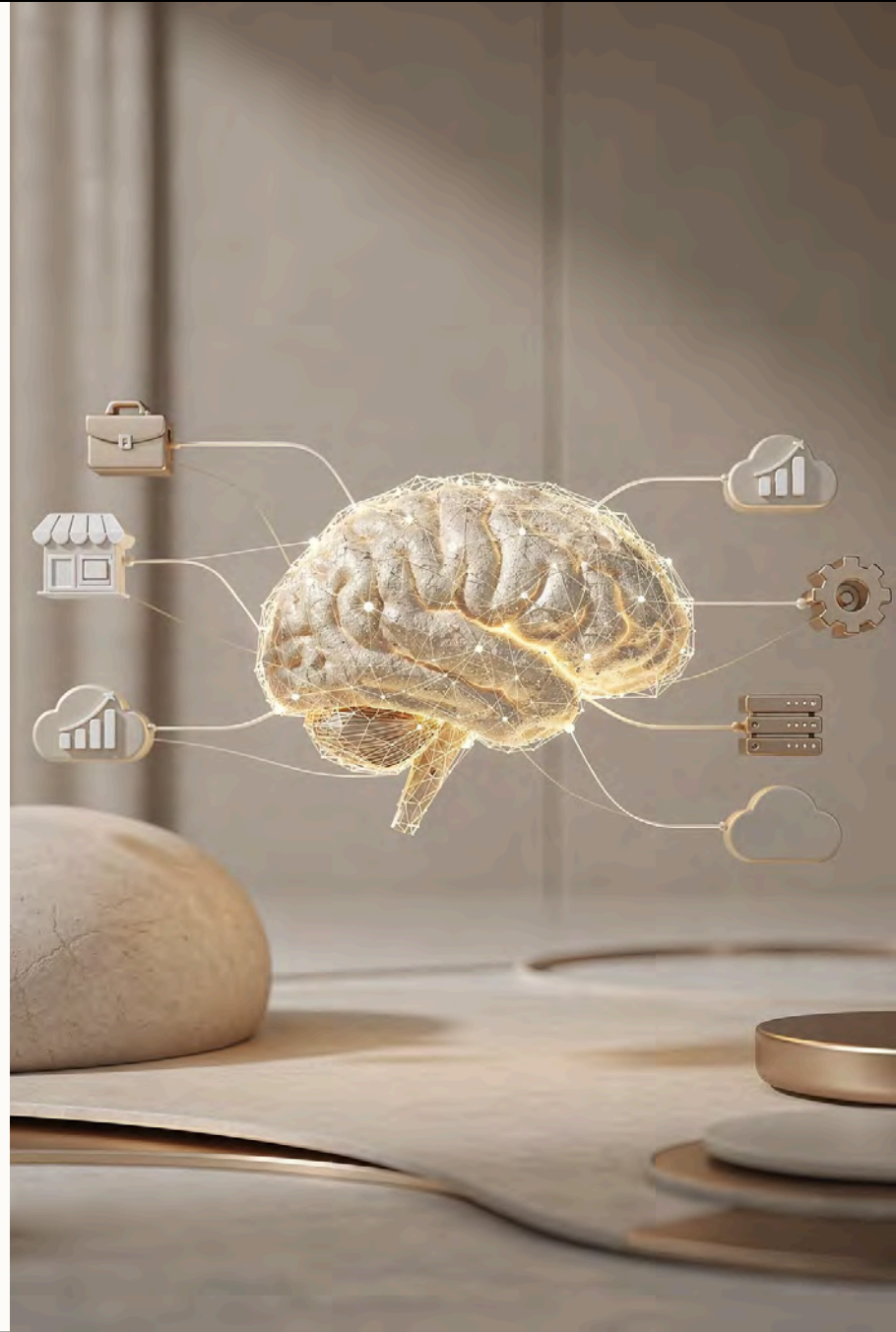
Misaligned Security Solutions

Available tools speak in CVEs and CVSS scores. Small business owners need plain-language guidance that maps to their actual risk not security jargon.

Introducing the Solution

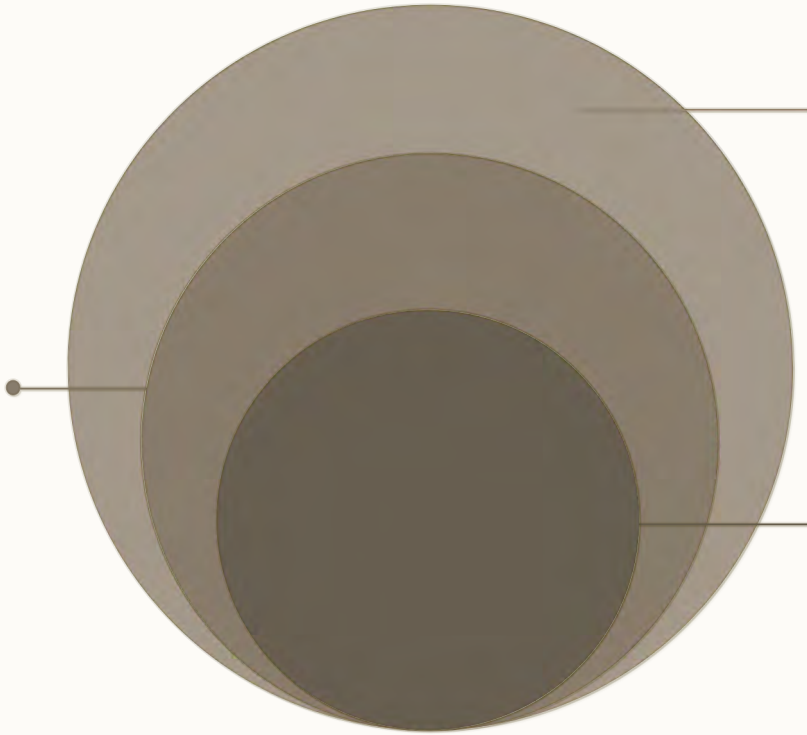
Security in Your Pocket: The securemystore.ai Framework

Developed for SKRM Technologies, **securemystore.ai** is an AI-driven, self-service cybersecurity platform purpose-built for small and home-based businesses. It operationalizes continuous, cloud-native security without requiring any dedicated security expertise bringing enterprise-grade risk intelligence into an accessible, actionable service.



A Six-Layer Security Architecture

The framework stacks six integrated capabilities into a coherent, automated security pipeline — from discovering what you own to continuously proving it's protected.



Outer: Asset Discovery & Detection

Discover assets, detect vulnerabilities, monitor

Mid: Business Risk Scoring

Translate findings into business-aligned risk

Core: Continuous Attestation

Prove systems remain secure and compliant

Each layer feeds the next. Asset discovery informs vulnerability detection; AI correlation transforms raw findings into prioritized, plain-language guidance; and attestation closes the loop with ongoing proof of protection.

Layer 1

Asset Discovery Know What You Own

You cannot protect what you cannot see. The first layer of the framework automatically maps every digital asset associated with a small business including assets the owner may have forgotten about or never knew existed.

Continuous discovery ensures the inventory stays current as the business grows, changes platforms, or adds new integrations.

→ Websites & Subdomains

All web properties, staging environments, and forgotten microsites.

→ APIs & Endpoints

Public and private APIs, webhooks, and third-party integrations.

→ Cloud Services & Storage

Buckets, functions, databases, and hosted services across providers.

→ SaaS Tools & Plugins

All connected software including e-commerce plugins and AI tools.

Layer 2

Vulnerability Detection Find What's Broken

Misconfigurations

Open S3 buckets, permissive IAM roles, exposed admin panels, and default credentials left unchanged.

Weak Authentication

Missing MFA, weak passwords, leaked API keys, and OAuth scopes that are broader than needed.

Exposed Services

Unintentionally public databases, development endpoints, and services running without TLS encryption.

Third-Party Risk

Plugin vulnerabilities, outdated dependencies, and integrations with overprivileged data access.

Layer 3

Continuous Monitoring Stay Ahead of Change

Why Continuous Matters

A one-time security scan is a snapshot in time. Cloud-native environments change constantly new deployments, updated plugins, changed configurations. A vulnerability introduced today may not be detected until a breach occurs unless monitoring is continuous.

01

Baseline Established

Initial scan creates a security posture baseline across all discovered assets.

02

Change Detection

Automated monitoring flags deviations from baseline new assets, config changes, new exposures.

03

Alert & Correlate

Changes are correlated with known risk patterns and prioritized for action.

04

Owner Notified

Plain-language alerts are surfaced to the business owner with clear next steps.

Layer 4

AI Correlation & Intelligence Connect the Dots

Individual vulnerabilities rarely tell the full story. The AI correlation layer analyzes findings across all assets simultaneously, identifying patterns and risk chains that a human reviewer or a simple scanner would miss.

Cross-Asset Risk Correlation

AI models link vulnerabilities across your website, APIs, and cloud services to surface compound risks where two low-severity issues together create a high-severity exposure.

Plain-Language Remediation

Technical findings are automatically translated into clear, jargon-free guidance. You get clear guidance like: "Your store checkout API is publicly accessible; here's how to restrict it in three steps."

Threat Intelligence Integration

AI models are informed by current threat intelligence, so emerging attack patterns relevant to SMB cloud environments are prioritized automatically, with no manual feed management required.

Layer 5

Business-Aligned Risk Scoring — Prioritize What Matters

Traditional security tools score vulnerabilities using CVSS, a technical scale designed for security professionals. A raw CVSS score means nothing to a small business owner deciding what to fix first on a Saturday morning.

The business-aligned risk scoring layer translates technical severity into **business impact language** weighing factors like revenue exposure, customer data at risk, regulatory obligations, and operational disruption to surface a prioritized, actionable to-do list.

🔴 Critical — Act Today

Exposed payment data or customer PII. Direct regulatory and financial risk.

🟠 High — Fix This Week

Weak authentication on admin accounts. High likelihood of exploitation.

🟡 Medium — Schedule Soon

Outdated plugin with known CVE. Low immediate impact but growing risk.

🟢 Low — Monitor

Minor misconfiguration with no current exploit path. Track and review.

Layer 6

Continuous Attestation — Prove You're Protected

Security is not a one-time event. The attestation layer provides **ongoing, automated evidence** that security controls are in place and effective closing the loop on the entire framework.

Compliance Evidence

Automated documentation for PCI-DSS, GDPR, and state privacy law requirements ready when you need it.

Posture Trending

Track how your security posture improves over time as issues are remediated and new assets are secured.

Trust Signals

Shareable security summaries for customers, partners, and insurers who need assurance about your data practices.

Evaluation Results What the Framework Found

The framework was evaluated in **simulated small business cloud environments** modeled on realistic SMB stacks — e-commerce sites with SaaS integrations, serverless backends, and third-party payment APIs.

Misconfigurations Identified

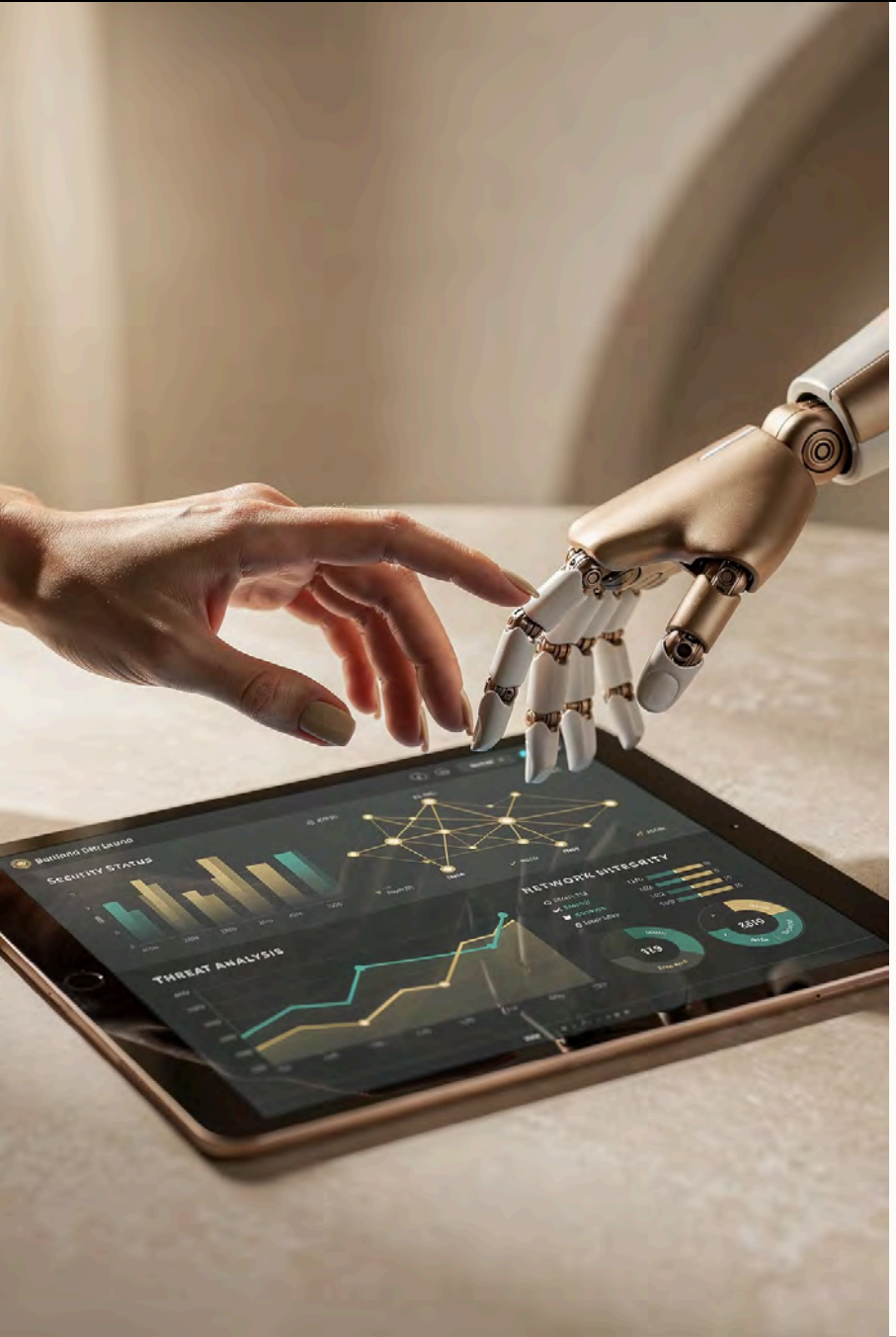
Exposed cloud storage buckets, overpermissioned service accounts, and publicly accessible admin interfaces all detected automatically, without any manual configuration.

Weak Authentication Surfaced

Missing MFA on admin accounts, hardcoded API keys in code repositories, and OAuth tokens with excessive scope were flagged and prioritized for immediate action.

Minimal False Positives

AI correlation significantly reduced noise findings were contextually filtered to ensure the owner's attention is directed only to genuine risks.



Human AI Collaboration at the Core

The framework is not fully autonomous it is designed around **human–AI collaboration**. AI handles the complexity: scanning, correlating, prioritizing, and explaining. The business owner retains agency: reviewing findings, making decisions, and taking action with confidence.

AI Does the Heavy Lifting

Automated discovery, continuous monitoring, cross-asset correlation, and risk translation happen without any manual effort from the owner.

Humans Stay in Control

Plain-language findings empower the owner to understand their risk posture and make informed security decisions no security degree required.

Continuous Feedback Loop

Owner actions feed back into the system, improving prioritization over time and adapting to the specific profile of each business.

Key Takeaways

Bringing Enterprise Security to Every Small Business

The **securemystore.ai** framework demonstrates that continuous, cloud-native security is achievable for small and home-based businesses without requiring dedicated expertise, complex tooling, or enterprise budgets.

By addressing the four systemic gaps visibility, ownership, third-party exposure, and tool misalignment and delivering results in plain, actionable language, the framework makes automated risk intelligence a practical reality for every small digital business.

01

Identify Your Full Cloud Footprint

Start with asset discovery you can't protect what you can't see.

02

Automate Detection & Monitoring

Replace manual reviews with continuous, AI-driven vulnerability detection.

03

Prioritize by Business Impact

Focus on what threatens your revenue, customers, and compliance first.

04

Close the Loop with Attestation

Continuously prove your security posture to customers, partners, and insurers.

Thank you!
For attending the conference, We welcome any questions or discussions you might have.

Vaishali Mahavratayajula · AI Security Architect, Wells Fargo

Conf42 Cloud Native 2026