Morgan Stanley

APPLICATION SECURITY · LOW-CODE · AI AGENTS

Why your security pipelines miss citizen developers

The fastest-growing group of software builders do not use pipelines

Keval Prabhudesai
November 16, 2026



About Me



Keval Prabhudesai

Morgan Stanley | Application Infrastructure

Power Platform | Low-Code | Application Security

keval.prabhudesai@morganstanley.com

www.linkedin.com/in/kevalprabhudesai

A statement to review

“Security gaps in applications are detected by scanners during deployment.”

Review objective – Does this statement truly apply to ALL applications?

This coverage extends to only the applications that are visible to the pipeline.

THE VISIBILITY GAP

What runs vs what the pipeline sees

WHAT RUNS YOUR BUSINESS

What your pipeline sees
Repositories · commits · builds · deploys

- Low-code apps
- Workflow automations
- Spreadsheet tools
- RPA bots
- AI agents

Built on approved low-code platforms yet invisible to regular application controls.

A LOW-CODE EXAMPLE

An analyst automates a daily reconciliation using Power Automate.

A few months later, it grows an arm and three legs, used by multiple teams and is considered a production app.

It never used pipelines.

AGENDA

Where we're going

1	Who is building, and what pipelines assume	3:00
2	Control Gaps	8:00
3	Defense in depth: six control layers	13:00
4	Pipeline-grade assurance, with Microsoft	20:00

WHO IS BUILDING

Citizen developers build four kinds of thing

Low-code apps
Forms, approval apps, small portals

Workflow automations
Move data between systems on a trigger

Bots
Drive other applications through the user interface

AI agents
Read content, call tools, take actions

80%

of low-code tool users expected to sit outside formal IT by 2026

Gartner forecast

Citizens are not the problem. Our security model needs to adapt.

Source: Gartner forecast on low-code development tool users.

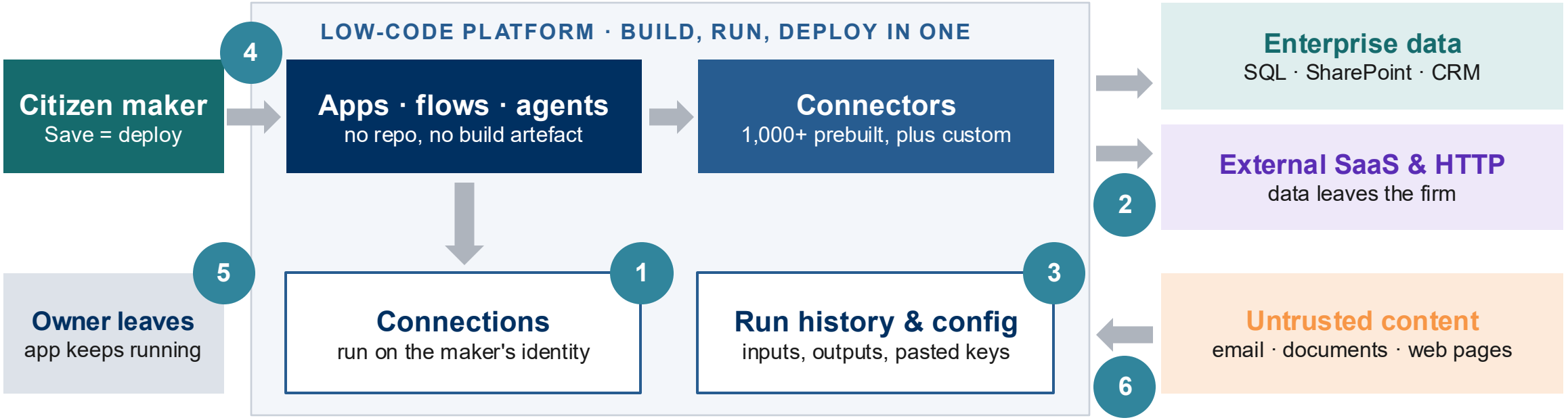
Assumptions that no longer hold

Traditional pipeline assumptions…		A citizen-built app…
Code lives in a repository	→	**Lives as metadata inside the platform**
Changes arrive as reviewed commits	→	**Changes on Save, with no diff and no reviewer**
A build produces an artefact to scan	→	**Has no build; interpreted at run time**
Deployment passes a gate we control	→	**Publishes the moment the maker decides**
An engineering team owns it	→	**Belongs to one person who may change roles**

Each mismatch means one less control

THE BLIND-SPOT MAP

Where citizen-built software escapes the pipeline



1 **Borrowed identity**

2 **Data exfiltration**

3 **Exposed secrets**

4 **Unreviewed change**

5 **Orphaned assets**

6 **Prompt injection**

CONTROL COVERAGE

Which pipeline control catches it? None.

Risk	SAST	Secret scanning	SCA / libraries	Peer review	DAST / pen test	CMDB / asset mgmt
1 Borrowed identity	✗	✗	✗	✗	✗	✗
2 Data exfiltration	✗	✗	✗	✗	Partial	✗
3 Exposed secrets	✗	✗	✗	✗	✗	✗
4 Unreviewed change	✗	✗	✗	✗	✗	✗
5 Orphaned assets	✗	✗	✗	✗	✗	✗
6 Prompt injection	✗	✗	✗	✗	Partial	✗

Six material risks undetected by any pipeline. The control point has to move into the platform.

Partial: DAST reaches public-facing portals only; it cannot see internal flows or agent actions.

Closing the gaps

Recommended controls and continuous hardening

Morgan Stanley



SECURITY ASSURANCE AND GOVERNANCE THAT SCALES

Partnering with Microsoft to tighten controls

THE PLATFORM BASELINE

Microsoft

Tenant isolation, Entra ID identity, encryption and compliance certifications built into Power Platform.

OUR CONTROL LAYER

The Firm

Firm policy enforced inside the platform at multiple layers. Goals extend far beyond bare minimum security.

TIGHTENING TOGETHER

Joint engagement

Continuous work with Microsoft product teams on the gaps that are foreseen before they occur.

Microsoft secures the platform. We govern everything built on it, and we keep pushing for more.

Source: Microsoft docs for Power Platform

DEFENSE IN DEPTH

Six control layers between a maker and a breach



1. **Identity & access**
   Entra ID, Conditional Access, service principals
2. **Environment isolation**
   Managed Environments, tenant isolation, routing
3. **Data loss prevention**
   Deny-by-default DLP, endpoint filtering, labels
4. **Secrets & connections**
   Key Vault variables, scoped connection references
5. **Release assurance**
   Solution checker, gated pipelines, approvals
6. **Detect & govern**
   Audit logs to Sentinel, inventory, owner attestation

PIPELINE-GRADE ASSURANCE

Every pipeline control has a low-code equivalent

CLASSIC APPSEC PIPELINE



LOW-CODE EQUIVALENT · ENFORCED IN THE PLATFORM

Git-backed solutions
Every change exported and unpacked to Git with the Power Platform CLI.

Solution checker
Static rules on apps and flows; critical findings block promotion.

Scan + vault
Secret scanners run on unpacked solutions; secrets only via Key Vault.

Connector governance
Connector inventory, DLP classification, custom connector review.

Gated pipelines
Managed solutions promoted only through approved pipeline stages.

Continuous detection
Audit logs to Sentinel; alerts on sharing, new connectors and agents.

The same assurance outcomes as an AppSec pipeline, enforced where makers actually build.

WITH MICROSOFT

Tightening controls, together

FOCUS 1	FOCUS 2	FOCUS 3	FOCUS 4
Agent governance	**Data boundaries**	**Threat detection**	**Roadmap influence**
Authentication on every agent; maker credentials restricted for autonomous actions.	Endpoint filtering and sensitivity labels take policy down to the data itself.	Platform telemetry feeding security analytics for faster detection and response.	Regulated-industry requirements shared directly with Microsoft product teams.

Security on these platforms is never a done job. As threats keep evolving, we continue to raise the bar.

Morgan Stanley

THE TAKEAWAY

Stay ahead of the curve

Count everything that runs the business, not only what passes through the pipeline.

1. **Count everything that runs the business.**
2. **Enforce controls where makers build.**
3. **Partner with your vendor to keep tightening.**

Thank you



Industry frameworks and research

1. **OWASP Citizen Development Top 10**
   https://owasp.github.io/www-project-citizen-development-top10-security-risks/

2. **OWASP Low-Code/No-Code Top 10 (original project)**
   https://owasp.org/projects/low-codeno-code-top-10

3. **OWASP Top 10 for LLM Applications: LLM01 Prompt Injection**
   https://genai.owasp.org/llmrisk/llm01-prompt-injection/

4. **NIST SP 800-218, Secure Software Development Framework (SSDF) v1.1**
   https://csrc.nist.gov/pubs/sp/800/218/final

5. **Gartner forecast: 80% of low-code users outside IT by 2026 (secondary source)**
   https://ninox.com/en/resources/blog/gartner-called-it-low-code-is-eating-software-development

Microsoft platform documentation

6 **Managed Environments overview**
https://learn.microsoft.com/en-us/power-platform/admin/managed-environment-overview

7 **Cross-tenant isolation**
https://learn.microsoft.com/en-us/power-platform/admin/cross-tenant-restrictions

8 **Connector endpoint filtering (preview)**
https://learn.microsoft.com/en-us/power-platform/admin/connector-endpoint-filtering

9 **Environment variables for Azure Key Vault secrets**
https://learn.microsoft.com/en-us/power-apps/maker/data-platform/environmentvariables-azure-key-vault-secrets

10 **Solution checker**
https://learn.microsoft.com/en-us/power-apps/maker/data-platform/use-powerapps-checker

11 **Solution checker enforcement**
https://learn.microsoft.com/en-us/power-platform/admin/managed-environment-solution-checker

12 **Pipelines in Power Platform**
https://learn.microsoft.com/en-us/power-platform/alm/pipelines

13 **Dataverse Git integration**
https://learn.microsoft.com/en-us/power-platform/alm/git-integration/overview

14 **Microsoft Sentinel solution for Business Apps**
https://learn.microsoft.com/en-us/azure/sentinel/business-applications/solution-overview

15 **Copilot Studio security and governance**
https://learn.microsoft.com/en-us/microsoft-copilot-studio/security-and-governance

16 **Authentication controls for agents (preview)**
https://learn.microsoft.com/en-us/power-platform/admin/security/configure-authentication-controls-for-agents