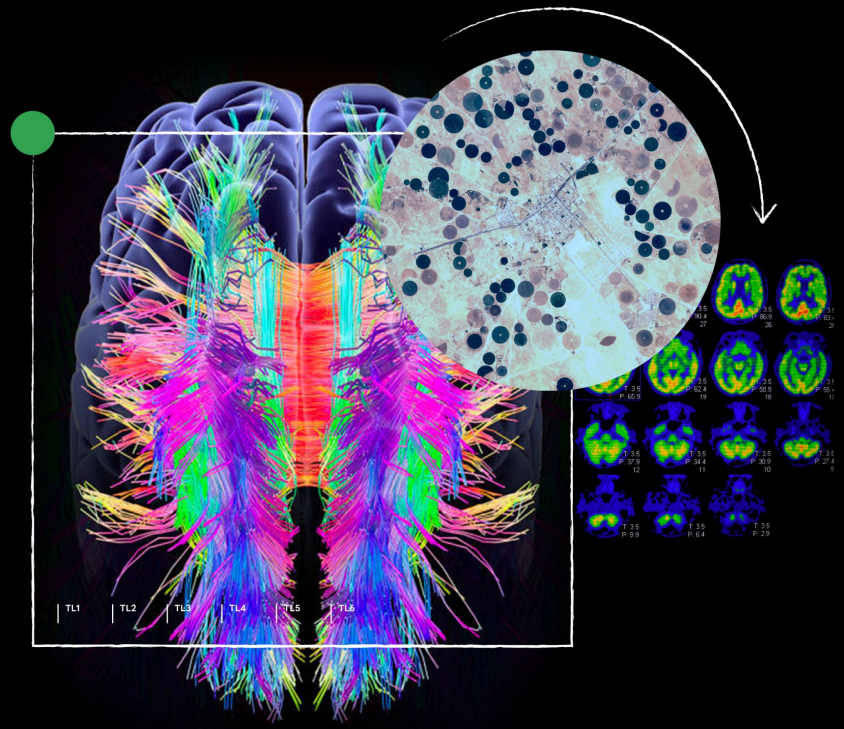
Attack Surface Intelligence

within Google Threat Intelligence

Unify discovery, posture, and frontline threat intelligence into one automated system.

Capability Overview Deck
September 2026



From Static Asset Lists to Automated Exposure Defense

New vulnerabilities and adversary campaigns are emerging faster than legacy tools can track. **We deliver an advanced, automated exposure management system** that continuously discovers exposed assets, validates real-world exploitability, and equips defenders to act first.

01

Product concepts walkthrough & key takeaways

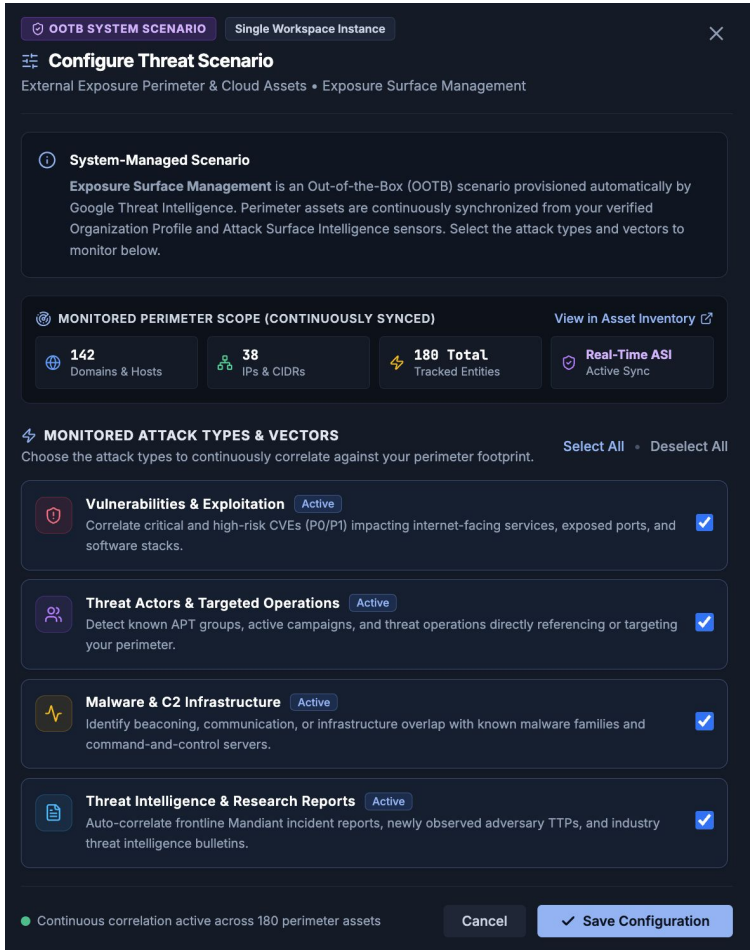
UX concepts for Google Threat Intelligence ASI

1

Exposure Surface Management Scenario

Unified setup for Native GTI ASM & Wiz integration

- Native GTI ASM: Configure external domains, IPs & Lite Scan discovery.
- Wiz Integration: Connect multi-cloud posture, IAM & Toxic Combinations.
- Org Profile 2.0: Syncs both paths into one governed exposure scope.

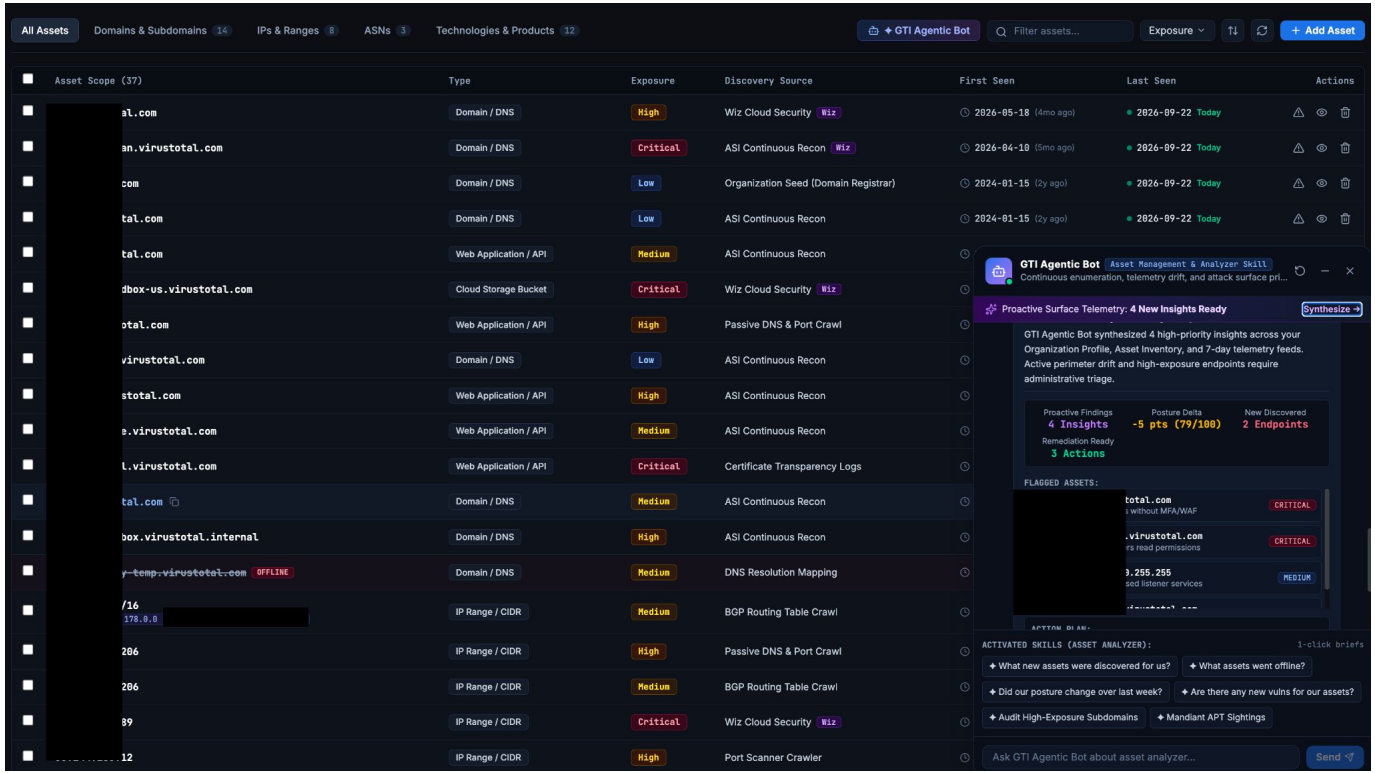


2

New Asset Inventory

Single inventory hosting all discovered & cloud assets

- Multi-Source Host: Unifies Native GTI ASM external assets & Wiz cloud resources.
- Auto-Fingerprinting: Maps banners, ports & certs into normalized CPE tech stacks.
- Constantly updated: Asset inventory discovered and updated automatically to display the latest state of resources.

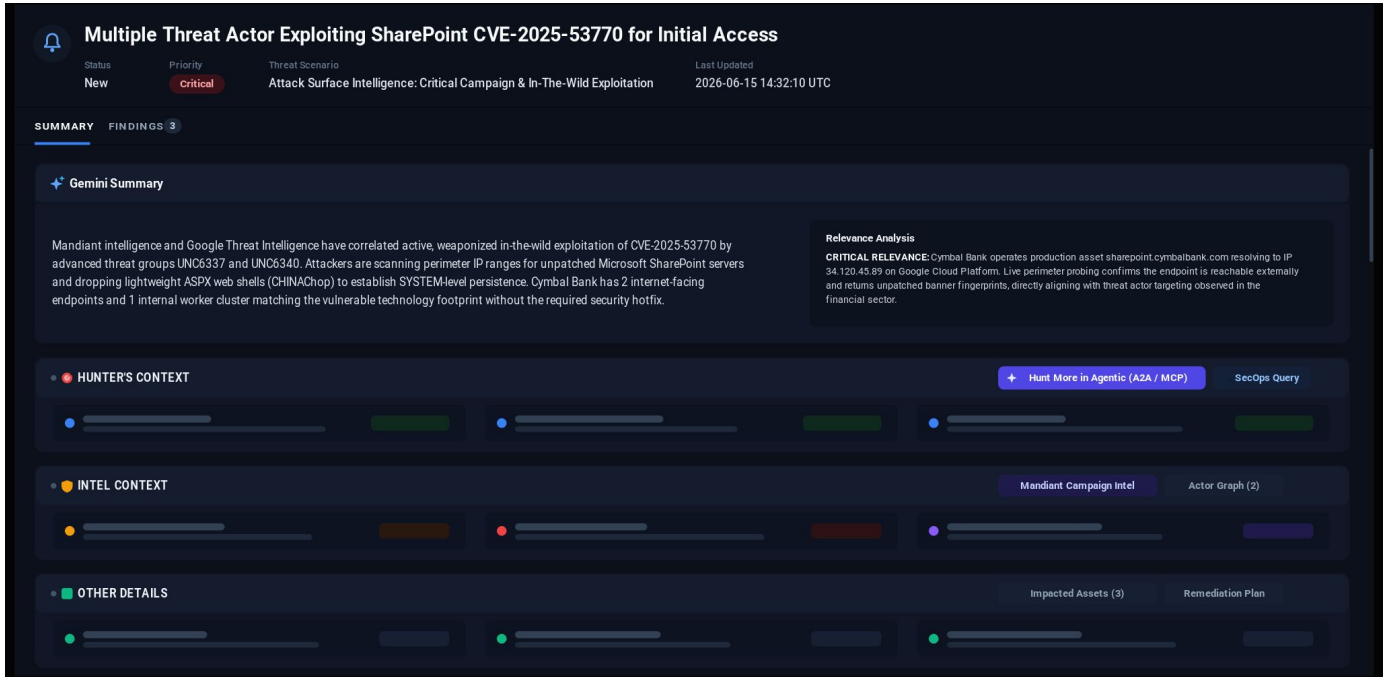


3

Exposure Alert: Example Overview

Exposed asset, severity & relevance in one view

- Alert Summary: Links the impacted asset directly to the active exposure.
- High-Signal Priority: Fires only when exposure intersects with live threat activity.
- CTI Analyst Context: Tailored for Hunting & Threat Intel.

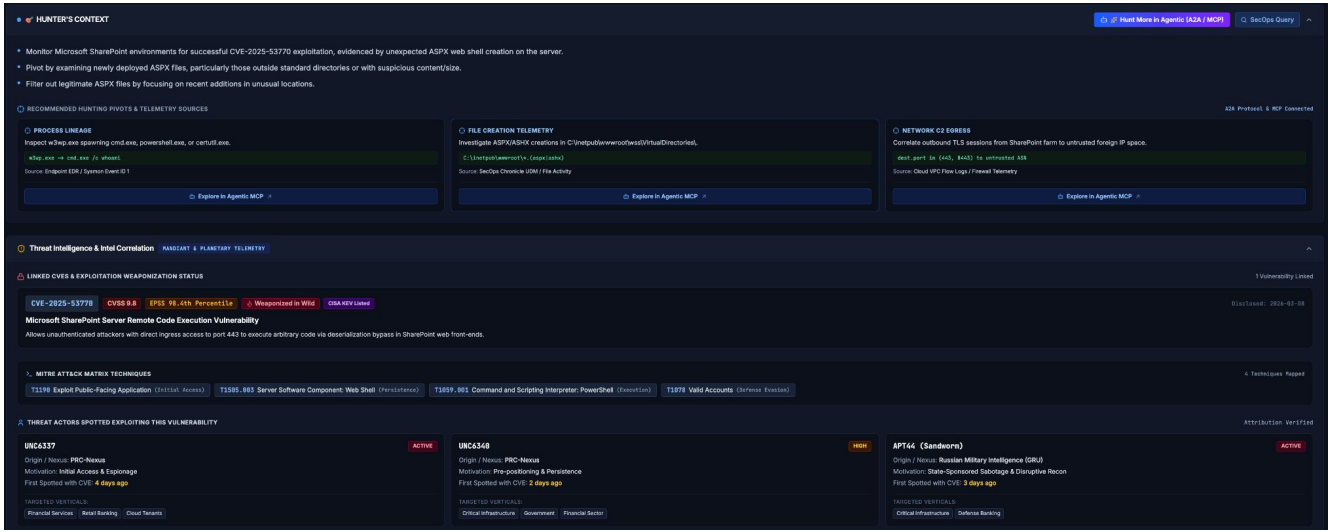


4

Alert: Hunting & Intel Context

Actionable hunting context & adversary intelligence

- Hunter's Context: 1-click hunts, IOCs & breach verification.
- Exploit TTPs: Web shells, C2 infrastructure & MITRE ATT&CK behaviors.
- Threat Intel Insights: Mandiant IR proof, actor attribution & targeting match.

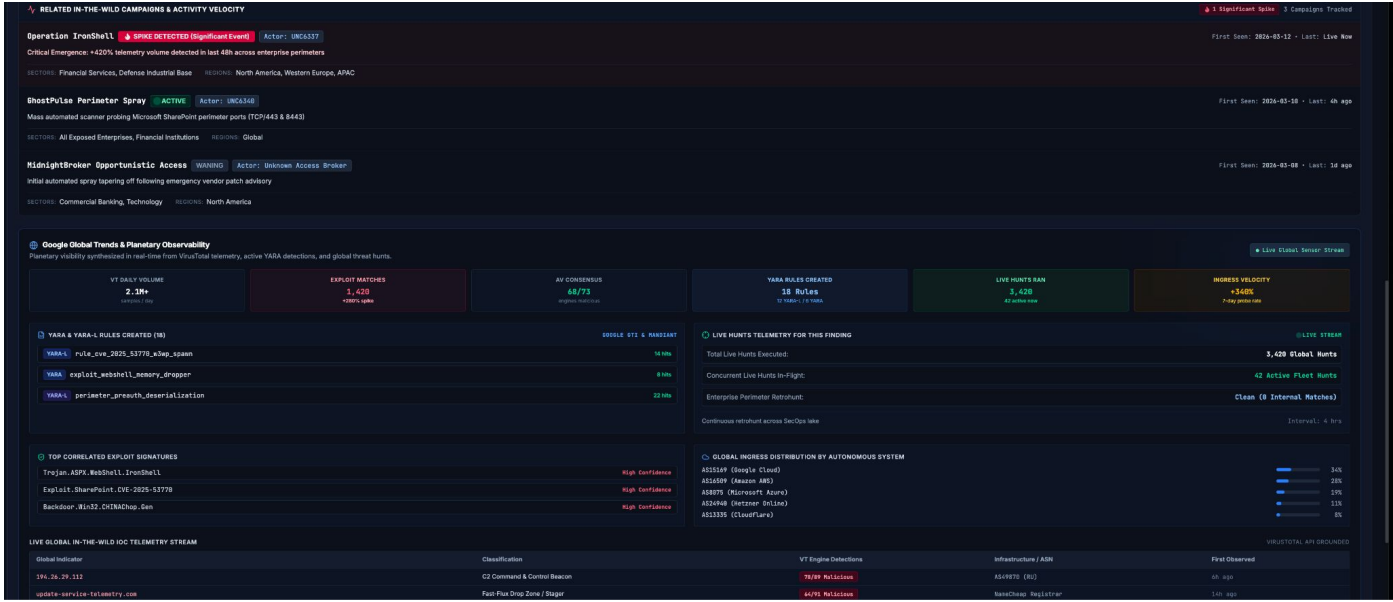


5

Alert: Google Global Insights

In-the-wild campaigns, global trends & observability

- ITW Campaign Tracking: Live tracking of related in-the-wild exploitation campaigns.
- Google Global Trends: Exploitation velocity across industries, regions & tech stacks.
- Global Observability: Planet-scale telemetry & early-warning signals unique to Google.



02

Background

Why standalone external scanners fail modern security operations

Why legacy standalone ASM pipelines break down

Legacy scanners chain discovery and static CVE matching together—without threat intelligence in the loop.

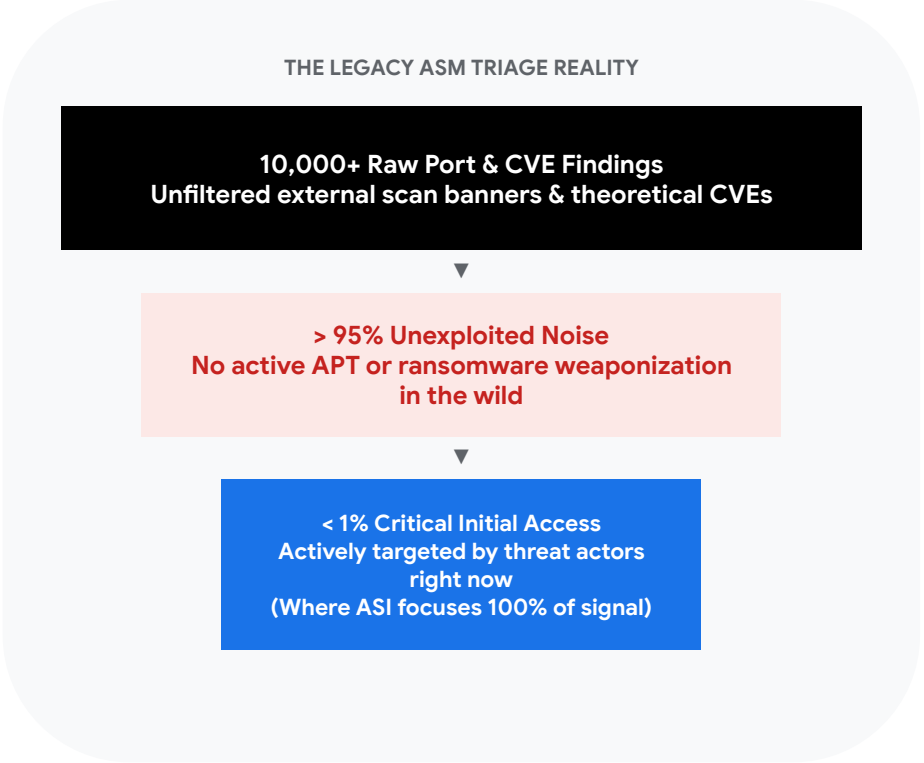
- Steps 1 & 2 operate mechanically: External crawlers discover open ports and immediately match banners against static NVD CVE tables.
- Step 3 is the critical blind spot: Rules engines score risk without knowing if threat actors actually target that software or if cloud paths are exposed.
- Step 4 overwhelms defenders: Every theoretical CVE becomes a ticket, burying real initial access vectors.



Standalone ASM tools are known for alert fatigue

Without answering "Which exposure matters right now?", vulnerability teams drown in low-severity CVEs.

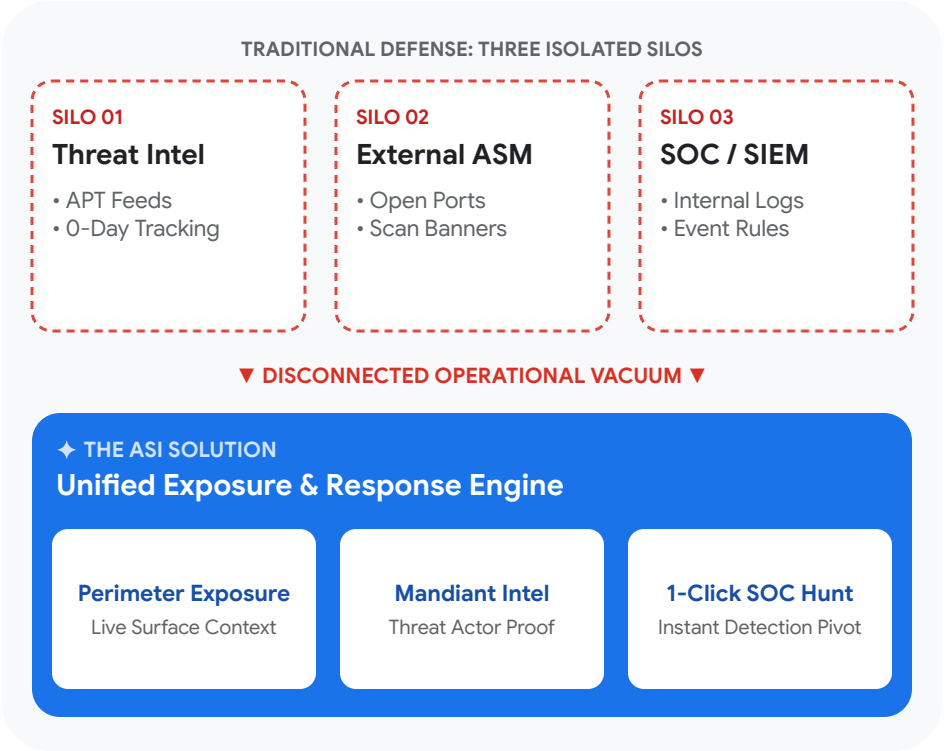
- Generates thousands of open port and low-severity CVE alerts every week.
- Lacks context on actual in-the-wild exploitability or active ransomware usage.
- Forces analysts to manually cross-reference every CVE against threat feeds.



Disconnected from Threat Intel & SOC hunting

Remediation happens in an operational vacuum when exposure tools cannot pivot into SOC detection workflows.

- Missing Threat Context: An exposed port doesn't tell you which APT group or campaign is targeting that technology.
- Siloed Defense: Standalone scanners operate completely disconnected from SOC and SecOps tools.
- Slow Response: Analysts lack rapid validation paths to check if an exposed asset was already compromised.



03 • ATTACK SURFACE INTELLIGENCE

How ASI fights modern security challenges

Defenders don't have a visibility shortage—they have a prioritization and speed crisis.

Attack Surface Intelligence transforms exposure management from a static compliance checklist into an AI-powered defense system—answering what is exposed, who is targeting it, and how to hunt it in seconds.

CHALLENGE 01
Compressed Time-to-Exploit
Adversaries weaponize newly disclosed perimeter CVEs within hours—long before routine patch cycles.

→

ASI ADVANTAGE
Real-Time Adversary Intersection & Prioritization
Automatically correlates your live tech stack with Mandiant frontline APT & ransomware weaponization.

CHALLENGE 02
Ephemeral Cloud & Perimeter Sprawl
New cloud services, shadow IT, and unmanaged endpoints appear faster than periodic scans can track.

→

ASI ADVANTAGE
Continuous Discovery
Unites frictionless Native Baseline ASM with deep Wiz cloud & graphs visibility add on*.

CHALLENGE 03
Siloed Vulnerability & SecOps Teams
VM teams see CVEs without threat proof; SOC analysts lack perimeter context to hunt effectively.

→

ASI ADVANTAGE
Agentic Validation & 1-Click Hunt
Gemini validates exploitability and launches instant hunts from the same alert.

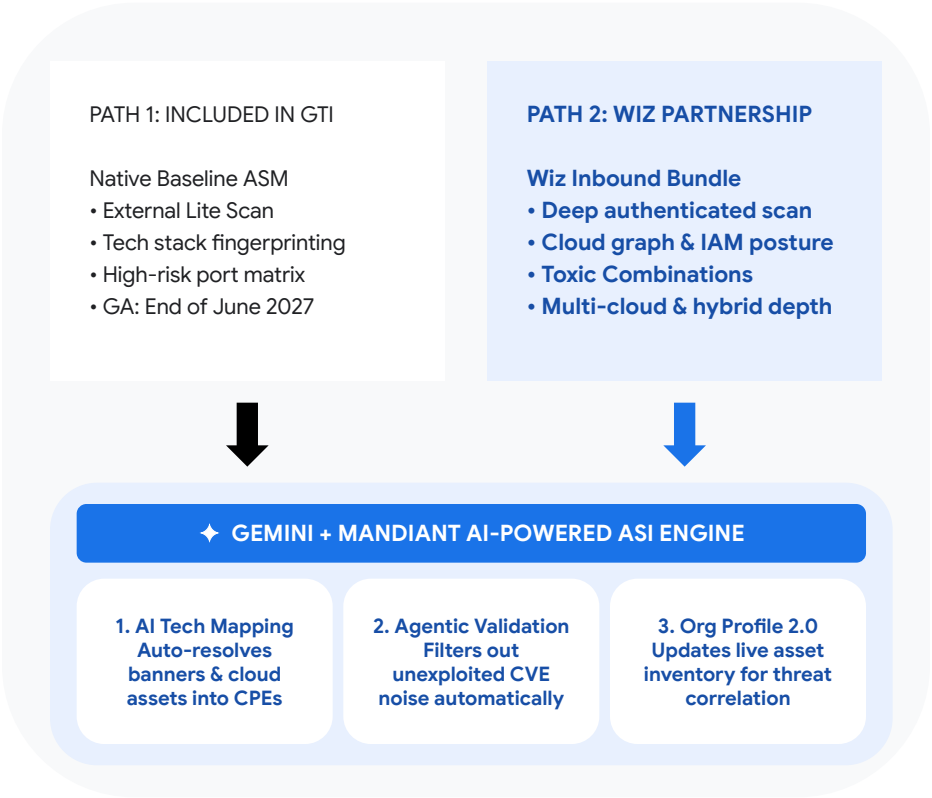
1

Ingestion Layer

Two purpose-built paths into one intelligence brain

- Native Baseline ASM: Included natively in GTI at no additional cost for lightweight non-authenticated external discovery and tech fingerprinting.
- Advanced Inbound Integration (Wiz): Deep authenticated cloud scanning, container/VM posture, and multi-risk Toxic Combinations. **Bought separately from GTI.**
- Bring Your Own Truth: In next releases, connect existing EASM and asset tools (e.g., Tenable, Axonius).

Eliminates the need to maintain redundant standalone perimeter scanners.



2

Org Profile 2.0

No more static asset lists, just living context

- Centralized Context Brain: Dynamically aggregates confirmed organizational tech stacks, versions, and perimeter scopes.
- Multi-Source Truth: Maps domain structures, ASNs, public IPs and confirmed security stance in one profile.
- Continuous Auto-Sync: Automatically adapts as new cloud workloads spin up or external gateways change.

Powers GTI Relevance System and Attack Surface Intelligence.

✦ **Organization Profile 2.0 — Confirmed Tech & Perimeter Stance Examples:**

Confirmed Edge & VPN Stack
Source: Native Lite Scan + Cert Transparency
Citrix NetScaler ADC (v13.1) • Ivanti Connect Secure • Palo Alto PAN-OS

Enterprise & Collaboration
Source: Fingerprinting + Org Profile
Microsoft SharePoint Server • Atlassian Confluence • Okta SSO

Multi-Cloud & IAM Scope
Source: Wiz Inbound Graph Connector
AWS Prod (142 VMs, 8 Public S3) • GCP (GKE Clusters, IAM Roles)

High-Risk Exposed Services
Source: Port/Service Categorization Matrix
Port 443 (TLS Gateways) • Port 22 (Bastion SSH) • Port 3389 (Blocked)

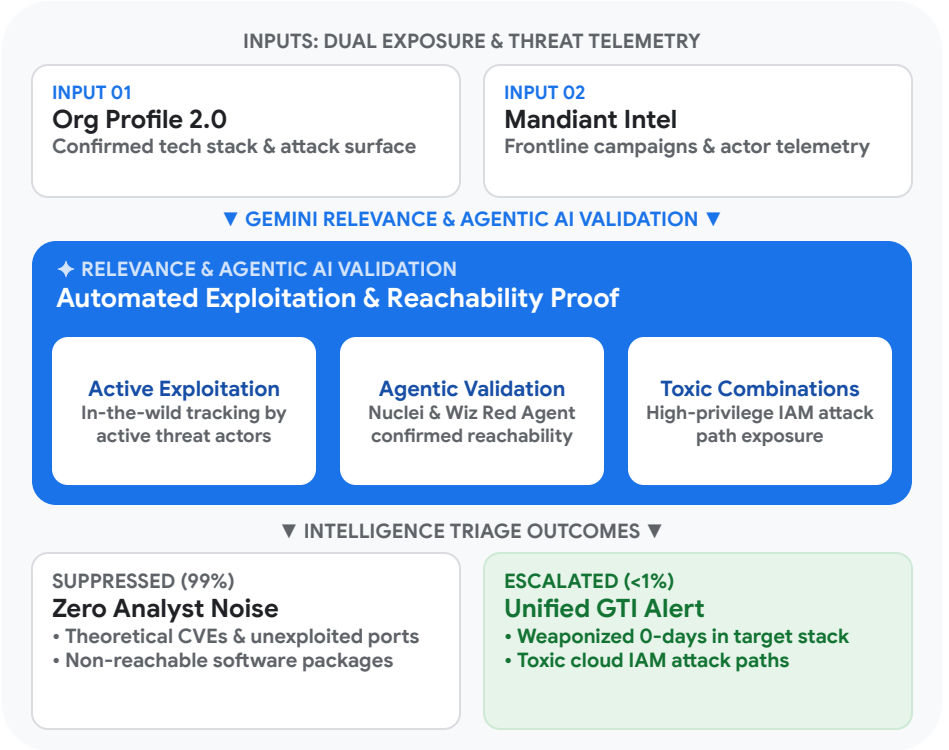
3

Relevance System

Mandiant frontline telemetry + GTI Agentic AI

- Gemini Relevance Filtering: Cross-references Org Profile 2.0 against millions of daily threat intelligence signals.
- Mandiant Campaign Correlation: Identifies whether active APT groups, initial access brokers, or ransomware crews are targeting your stack.
- Active Exploit Validation: Pairs templated checks and GTI Agentic AI with Wiz Native + Red Agent exploit validation.

Suppresses theoretical CVEs; surfaces only verified initial-access risks.



4

Unified Threat Scenario

One alerting engine for new Native ASM and Wiz Integration

- Single 'Exposure Surface Management' Scenario: Both Native Baseline and Wiz feed the same alerting pipeline in GTI.
- Prioritized, Intel-driven Alerts: Warns immediately when zero-days or new campaigns target software in your stack (e.g., Citrix, SharePoint).
- Gemini Hunter's Context: Embeds adversary TTPs, actor attribution, and post-exploitation objectives directly on the alert card with 1 Click hunt pivots to speed up investigation.

No fragmented dashboards—every exposure alert lives in Unified GTI Alerts.

GTI ALERT • SCENARIO: EXPOSURE SURFACE MANAGEMENT

CRITICAL | Active Campaign Targeting Confirmed Citrix NetScaler (CVE-2026-XXXX)

Confirmed Asset Match (Org Profile 2.0)

vpn-gw-01.corp.example.com (198.51.100.24) • Fingerprinted via Native Baseline & Wiz

Mandiant Frontline Campaign Context

Actively exploited by UNC5221 & Ransomware affiliates for initial perimeter access in the last 48h.

Gemini Hunter's Context & TTPs

Adversaries deploy web shells post-auth bypass, dump credentials, and pivot via RDP/SMB ⟶ Define and Attach 1 Click Hunt Pivots for SecOps or SIEM tools

5

Actionable Defense

1-Click SecOps hunting & CISO Autobriefs

- Assume-Breach 1-Click Pivot: 'Run Hunt' button embedded directly on GTI Unified Alerts launches instant SIEM investigations.
- Pre-Curated Hunt Packs: Automatically provides detection rules, search queries, and actor IoCs for SecOps/SIEM tools..
- Executive Autobriefs: Auto-generates CISO-ready briefings and 30/90/180-day risk trend reports in seconds.

Bridges external perimeter discovery directly into internal SOC response.

WORKFLOW 1: ASSUME-BREACH SOC HUNTING

[1-Click 'Run Hunt']

- Provides detection rules & Mandiant IoCs to insert into SecOps/SIEM tools
- Hunts internal telemetry for lateral movement from exposed perimeter IPs
- Closes the loop between Vulnerability Triage and SOC Threat Hunting
- A2A and MCP integrations coming to speed up operationalization

WORKFLOW 2: AUTOMATED EXECUTIVE AUTOBRIEFS powered by GTI Agentic

[On-Demand CISO & Stakeholder Reporting]

- Generates board-ready executive briefings in seconds
- Tracks 30 / 90 / 180-day exposure reduction & targeted campaign posture
- Quantifies security ROI across Native Baseline ASM and Wiz investments

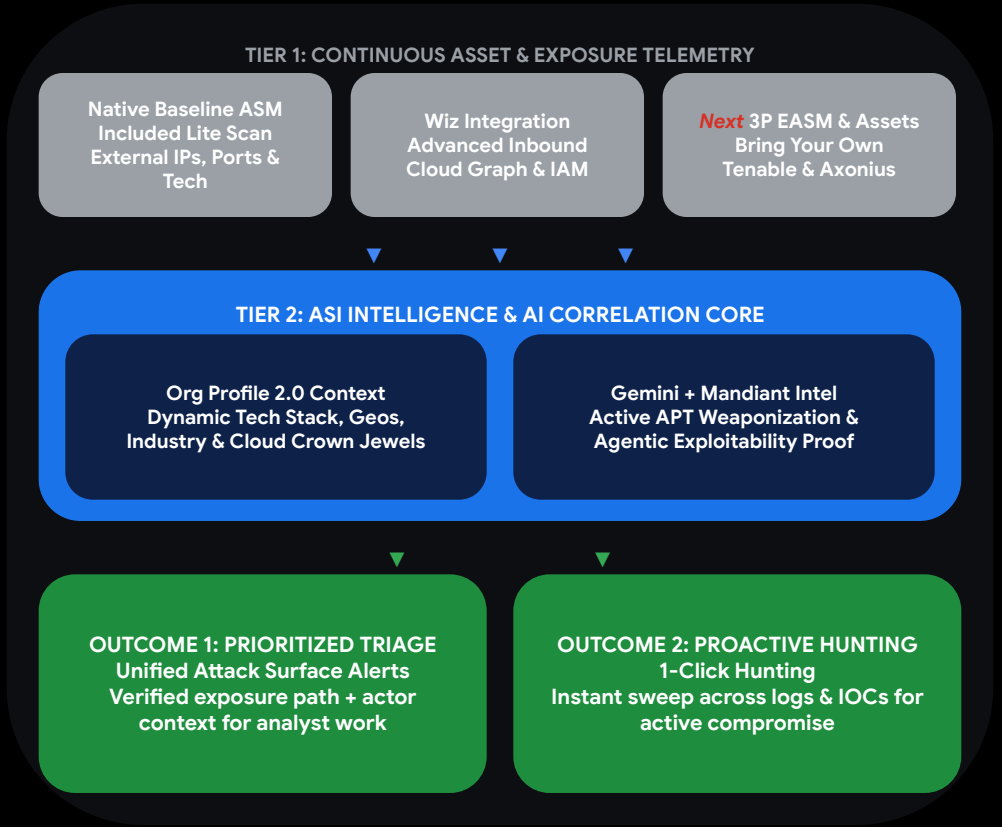
Attack Surface Intelligence

End-to-End Architecture

Unifies outside-in discovery, inside-out cloud posture, and frontline threat intelligence into one automated system.

Threat-Validated Signal
Suppresses theoretical CVE noise by intersecting live assets with Mandiant campaign telemetry.

Closed-Loop Hunting
Bridges exposure triage directly to 1-click hunting and remediation.



Two Paths & Capability Matrix

WORKLOAD RUBRIC

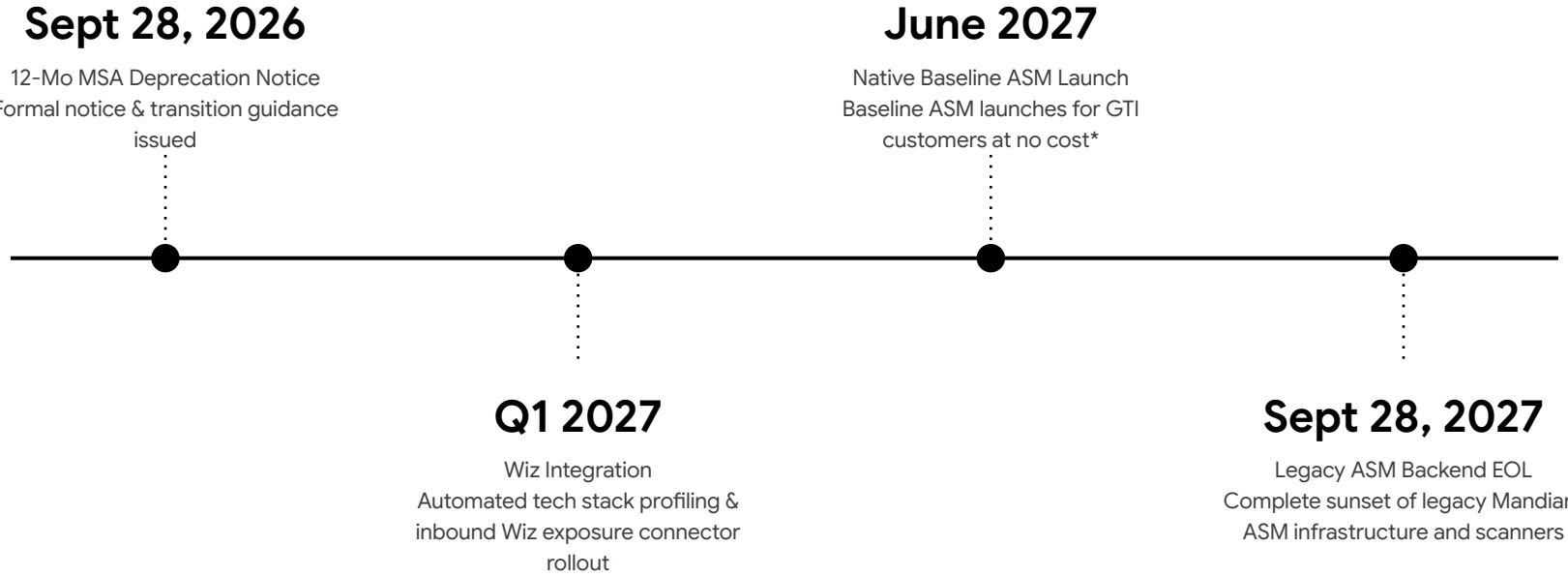
Choose Baseline ASM if:
Focus is continuous external discovery, tech stack tracking & non-authenticated scans (Included at no extra cost).

Choose Wiz ASM if:
You need authenticated cloud posture, code/VM scanning & Toxic Combinations via integration with Wiz.
(Bought separately).

Capability Dimension	Path 1: Native Baseline ASM Included in GTI	Path 2: Wiz Integration Advanced Bundle
Commercial & Availability	**Included at no extra cost*** **ETA: End of June 2027**	**Wiz CNAPP + ASM Bundle** **Wiz bought separately** **ETA: Q1 2027**
Scan Type & Depth	Non-authenticated external discovery & tech fingerprinting	Deep authenticated inspection across VMs, containers & code
Exposure Scope	Public IPs, domains, open ports & web service headers	Multi-cloud infrastructure graph, IAM, secrets & internal assets
Exploitation Validation	Passive checks + GTI Agentic AI	Wiz Native Validation + automated Red Agent exploit proof
Risk Correlation	Org Profile 2.0 stance + Mandiant active campaign intel	Toxic Combinations (Public IP + CVE + IAM graph) + GTI Intel
Prioritization	Threat-informed relevance intersected with Google visibility	Multi-vector graph blast radius, exploitability & threat relevance

Transition timeline

A 12-month migration window from legacy GTI ASM to modern Attack Surface Intelligence.



To transition smoothly to Attack Surface Intelligence...

1

Review your ASM scenarios

Audit your current external scanning workflows and determine whether passive external discovery (Native Baseline ASM) or deep authenticated cloud inspection (Wiz) fits your posture.

2

Schedule an architecture review

Connect with your Google Account Executive or TAM to discuss new ASI, transition milestones, and long-term cloud security strategy.

3

Select your target ASI path

Adopt Native Baseline ASM (included in GTI) for continuous external discovery, or integrate Wiz for deep multi-cloud posture and toxic combination graphs.

Questions? Contact your representative or visit the Google Cloud Security Community.