BITSIGHT Luminate EXCHANGE

03

Bitsight Product Roadmap:

Cyber Risk Intelligence in an Agentic World

BITSIGHT

Speaker

Brian Mulligan

VP Product Management, Ratings & Data Engine, Bitsight

BITSIGHT Luminate EXCHANGE

PRODUCT ROADMAP / Cyber Risk Intelligence in an Agentic World

PRESS → TO BEGIN

A radically new landscape.

◆ EXPANSION

The attack surface is collapsing inward

Cloud, SaaS, AI, and supply chain are expanding faster than any team can map.

ASSETS DETECTED — 847 → 1,203 → 1,737 ↑

◆ THE ACCELERATION

In the **post-Mythos** world, exploits beat patches.

AI compresses disclosure-to-weaponization from years to hours. Most exploits now hit before disclosure.

◆ PRESSURE

CISOs are squeezed from both sides.

Boards want outcomes, not activity. Compliance consumes the hours that should be closing gaps.

◆ THE TIME COLLAPSE

From years to zero.

2018

771

days

Median time from disclosure to first exploit

2021

84

days

Log4Shell era — exploitation begins within hours

2024

4

hours

AI writes working exploits in minutes

2025

0

~~days~~ · ZERO-DAY

Most exploits now hit BEFORE disclosure

When exploit is instant, there is only **preparation**.

Source: Zero Day Clock · zerodayclock.com

The pieces exist. They just don't connect.

◆ RATINGS & MONITORING

Tell you what's changed.

Objective posture signals. Longitudinal trend data. Strong for governance and board reporting.

Posture over time

Gap: doesn't tell you what's happening right now.

GAP

◆ THREAT INTELLIGENCE

Tell you what's out there.

Adversary activity, IOCs, dark web signals. Rich context on actors and campaigns.

What adversaries are doing

Gap: not mapped to your specific environment.

GAP

◆ EXPOSURE & ATTACK SURFACE

Tell you what's exposed.

Assets, vulnerabilities, misconfigurations. Breadth of visibility across your environment.

What's exposed across your surface

Gap: too much signal. Not enough priority.

Each piece answers a different question.

Nothing connects the answers into a decision.

OUR NORTH STAR

Bitsight is building the cyber risk intelligence platform.

Turning the world's most powerful security data into decisions, actions, and outcomes at **AI speed**.

- The best data is becoming intelligent
- Tools are evolving into agents
- Signals are turning into connected workflows

Leading in Cyber Risk Intelligence

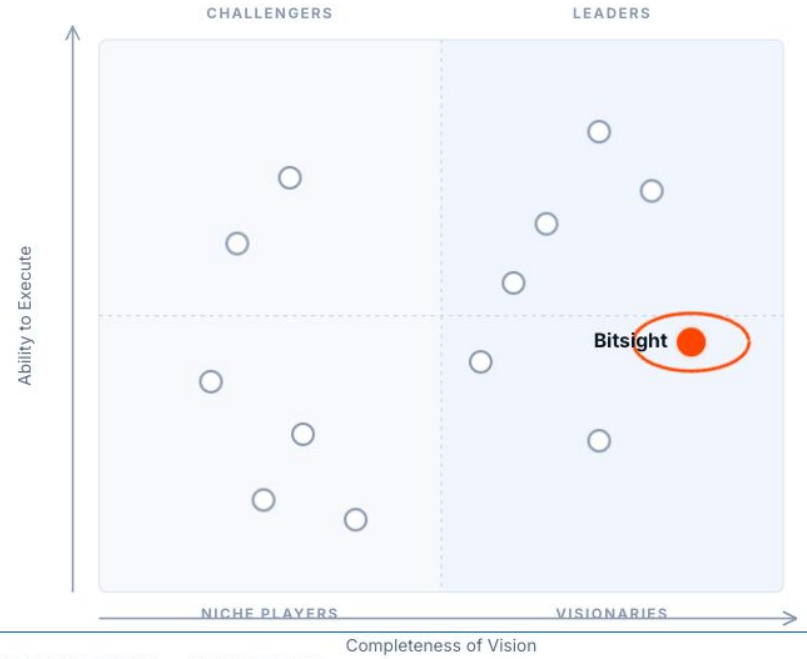
> The real value ... is in the **data and intelligence** underlying a rating and their ability to surface actionable risk findings when this data is used correctly.

— Paul McKay, Forrester Research

Forrester Wave™: Cybersecurity Risk Ratings, 2026

GARTNER® MAGIC QUADRANT™ 2026

Recognized as a Visionary in Cyber Threat Intelligence



GARTNER DEFINITION

Visionary

Visionaries stand out for their **innovative approach** and ability to **anticipate future market needs**, often introducing unique capabilities, **advanced AI-driven analytics** or novel delivery models that challenge traditional paradigms. These vendors play a critical role in **shaping the market** by driving innovation and influencing long-term strategies.

Roadmap Guiding Principles

SEE

Surface what matters

THE CISO SAYS

My attack surface and ecosystem are expanding faster than I can keep up.

AIM

Connect threat to exposure

THE CISO SAYS

I can't connect what my SecOps team sees to what I report to the board.

ACT

Do the work at scale

THE CISO SAYS

My team is drowning. We can't hire our way out of this.

NORTH STAR

Create the intelligence layer for the CISO

Unite operations and governance on a shared foundation of cyber risk.

AI
is the engine that transforms all three.

THE PLATFORM

One Platform, Two Ways to Access It

BITSIGHT AGENTS

We build the agents. You get the outcomes.

New vendor alert: critical finding
acme-supplier.com · High severity

Bitsight AI

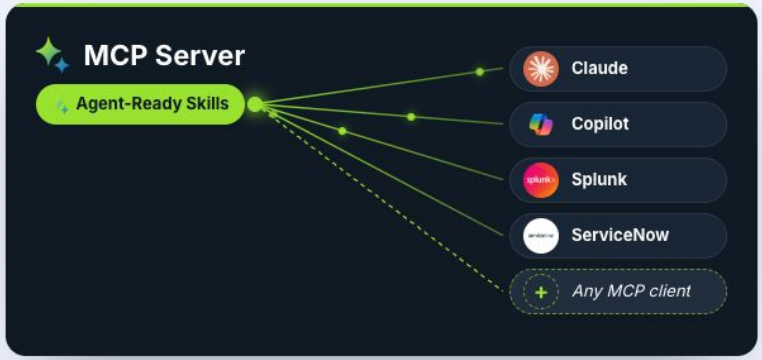
Analyzing risk | Checking dark web | Drafting response

BRING YOUR OWN AGENT

Our intelligence. Your AI. Fully connected.

REST API
Programmatic access

Data Feeds
Bulk delivery at scale



UNIFIED INTELLIGENCE

One Intelligence Layer. Two Ways to Win.

Whether you use our agents or your own,
the See-Aim-Act lifecycle is fully integrated.

	Bitsight Agents	Bring Your Own Agent
SEE	**Curated risk views** Out-of-the-box dashboards & alerts	**Asset & exposure feeds** Streamed into your data lake
AIM	**AI-prioritized findings** Bitsight AI ranks what matters	**Bring your context to bear** Context to power custom analytics
ACT	**Agents drive remediation** Automated triage & response	**Trigger SOAR & SIEM** Native APIs into your runbooks

THE OUTCOME | A unified foundation of cyber risk that scales with your team's maturity.

The foundation: why our data is different

The internet's external attack surface

4.4B+ addresses continuously scanned

100M+ active CVE instances | Deep product fingerprints

The threat landscape, in real time

1B+ credentials tracked weekly

7M+ intelligence items daily | 130M+ threat actors monitored

Entity and attribution graph

12+ years of rich historical data

Comprehensive global organization monitoring | Full supply chain attribution

DEEP DIVE · SEE

Illuminating the Modern Attack Surface

SECOPS FEED
Third-Party Exposure
Live

- HIGH — Citrix NetScaler CVE-2026-3104 — CVE partner-c.net · 9m ago
- MEDIUM — OpenClaw admin panel public — API vendor-d.ai · 12m ago
- HIGH — Shadow asset · forgotten subdomain — ASSET supplier-e.io · 18m ago
- MEDIUM — Leaked LLM API key in JS bundle — API vendor-f.app · 23m ago
- CRITICAL — Exposed LiteLLM gateway · auth bypass — AI vendor-a.io · 2m ago

Streaming detections · To SIEM · SOAR

AI ATTACK SURFACE
Securing the AI Stack
Drill in →

HIGH-DEFINITION MAPPING
Discovery & Fingerprinting
Drill in →

M&A DISCOVERY
Keep Pace with Change
Drill in →

Overview · AI Attack Surface · Discovery & Fingerprinting · M&A Discovery

← → to drill in

Securing the AI Stack

AI INFRASTRUCTURE SCAN

- **MCP Server** · Model Context Protocol — Reachable without TLS · auth optional — CRITICAL
- **LiteLLM Gateway** · LLM proxy — Auth bypass via /v1/models endpoint — CRITICAL
- **OpenClaw Admin** · Agent orchestrator — Public admin panel · default creds — WARNING
- **Vector DB** · Pinecone-compatible — Index browsable · no rate limits — WARNING
- **Foundation Model API** · OpenAI-compatible — Mutual TLS · rotated keys — SECURED

100k+ OPENCLAW DETECTIONS / MONTH

50k+ OTHER AI DETECTIONS / MONTH

40+ NATIVE AI FINGERPRINTS

MARCH 2026 · CASE FILE

When LiteLLM was compromised, our customers knew in hours.

LiteLLM is the front door to the AI stack — one breach, every model behind it.

THE TARGET
LiteLLM in production at scale
Already fingerprinted across our customers' third parties.

THE WARNING
TeamPCP activity surged 300%
Threat Activity Index spike, days before any public disclosure.

THE COMPROMISE
TeamPCP inserts malware into LiteLLM
The front door to AI infrastructure becomes the attacker's door too.

THE RESPONSE
Customers notified within hours
Major security event published with affected vendor and asset list — no customer left guessing.

This is what fingerprinting + threat intelligence looks like together.

From Unknown Asset to Actionable Detection

ASSET FINGERPRINT REVEAL

WHY THIS MATTERS NOW

AI will find vulnerabilities faster than humans can patch.

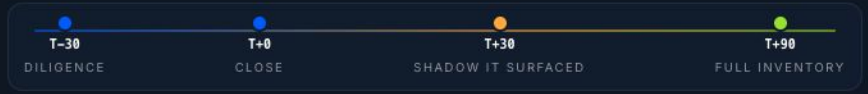
So we map the software first.

When the next zero-day hits, our customers already know where it lives.

Risk Profiles That Keep Pace with Change

PRE-MERGER → POST-CLOSE

Inheritance scan



+3,400
INHERITED ASSETS

127
FORGOTTEN SUBDOMAINS

8
CRITICAL EXPOSURES

WHY IT MATTERS

Corporations change — risk profiles move with them. Bitsight keeps your view of the attack surface in lock-step with every merger, divestiture, and structural shift.

- **Pre-deal:** surface diligence on the target's exposure
- **Day-0:** instant inventory of inherited internet assets
- **Day-30:** shadow-IT, forgotten infra, and orphan domains surfaced
- **Continuous:** every divestiture and rebrand auto-rescanned

DEEP DIVE · AIM

Prioritize What Matters

THE EQUATION

Combine exposure, threat, and business context

One intelligence layer aligns the asset, the adversary, and what it means for the business — so every finding arrives pre-prioritized.

Exposure · Threat · Business Context

THE LEVERAGE

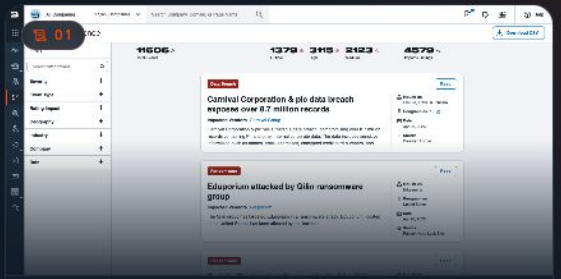
Data + workflow crossover

The same intelligence that drives prioritized findings inside Bitsight is delivered to your SIEM, SOAR, and data fabric — closing the loop without duplicating work.

Workflow Apps · APIs · Feeds · SIEM · SOAR · Lake

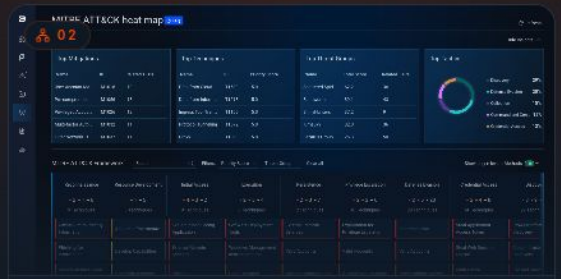
THE AIM EQUATION

Exposure what's reachable + Threat who's targeting + Context what it means = AIM prioritized action



Breach Intelligence

Real-world incidents, mapped to your supply chain



MITRE ATT&CK Mapping

Adversary techniques scored against your environment

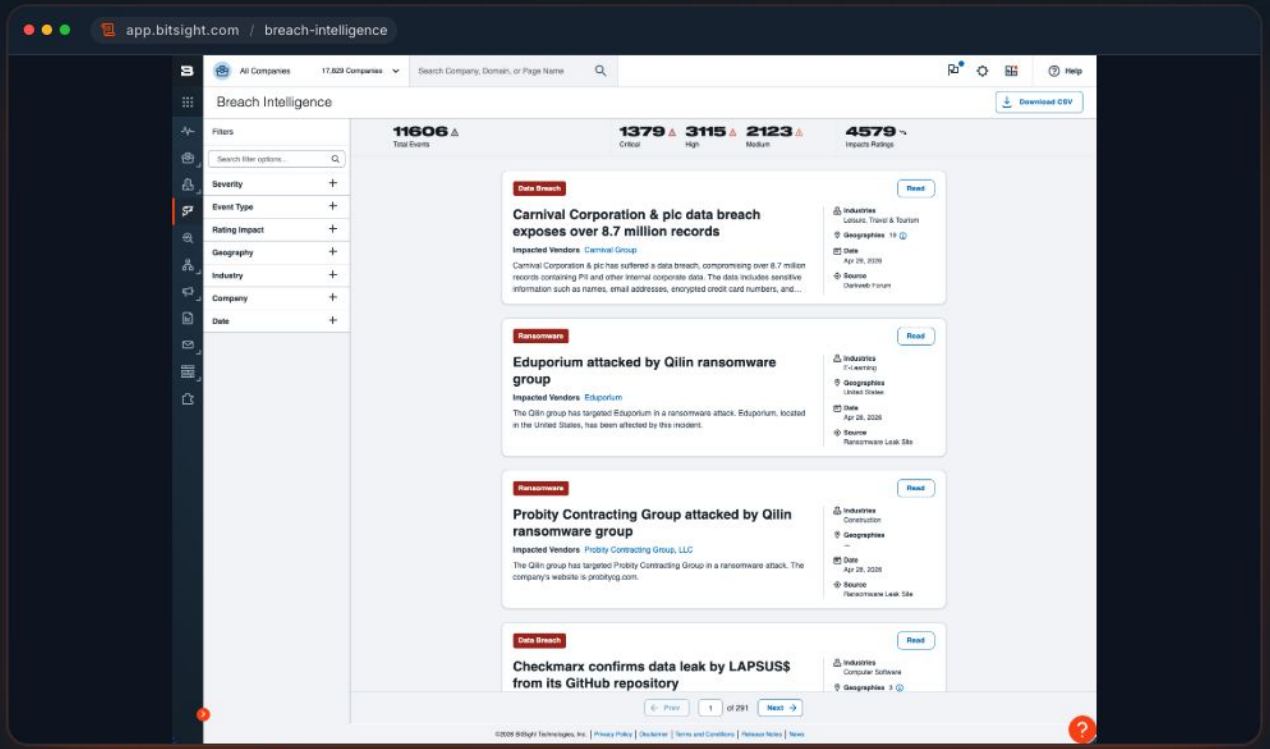
Sectoral Intelligence

Transform global noise into sector-specific action

Overview · Breach Intelligence · MITRE ATT&CK Mapping · Sectoral Intelligence

← → navigate Esc overview

Breach Intelligence



WHAT YOU'RE LOOKING AT

Breach Intelligence

Automatically scored against your supply chain. Every breach is matched to your inventory, geography, and rating — so you see the ones that matter, not all of them.

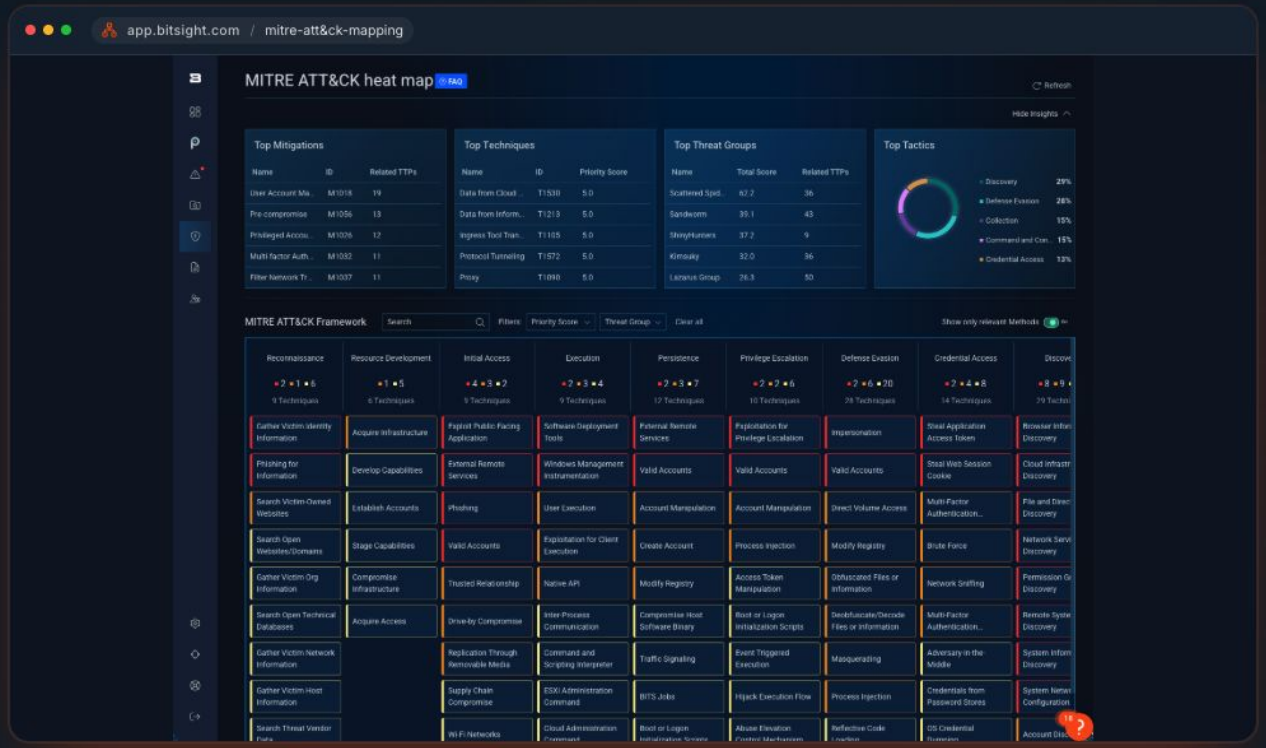
- **Severity Assessment** — (Critical · High · Medium) summarize blast radius at a glance
- **Vendor-mapped** — events feed third-party risk and concentration analysis
- **Filterable** — by event type, rating impact, geography, industry, company, date

AIM: this view is one input. Bitsight fuses all three into a single prioritized action queue.

Overview | **Breach Intelligence** | MITRE ATT&CK Mapping | Sectoral Intelligence

← → navigate Esc overview

MITRE ATT&CK Mapping



WHAT YOU'RE LOOKING AT

MITRE ATT&CK Mapping

Adversary techniques mapped across your environment, ranked by relevance. Top mitigations and threat groups surface the highest-leverage controls — not just the loudest CVEs.

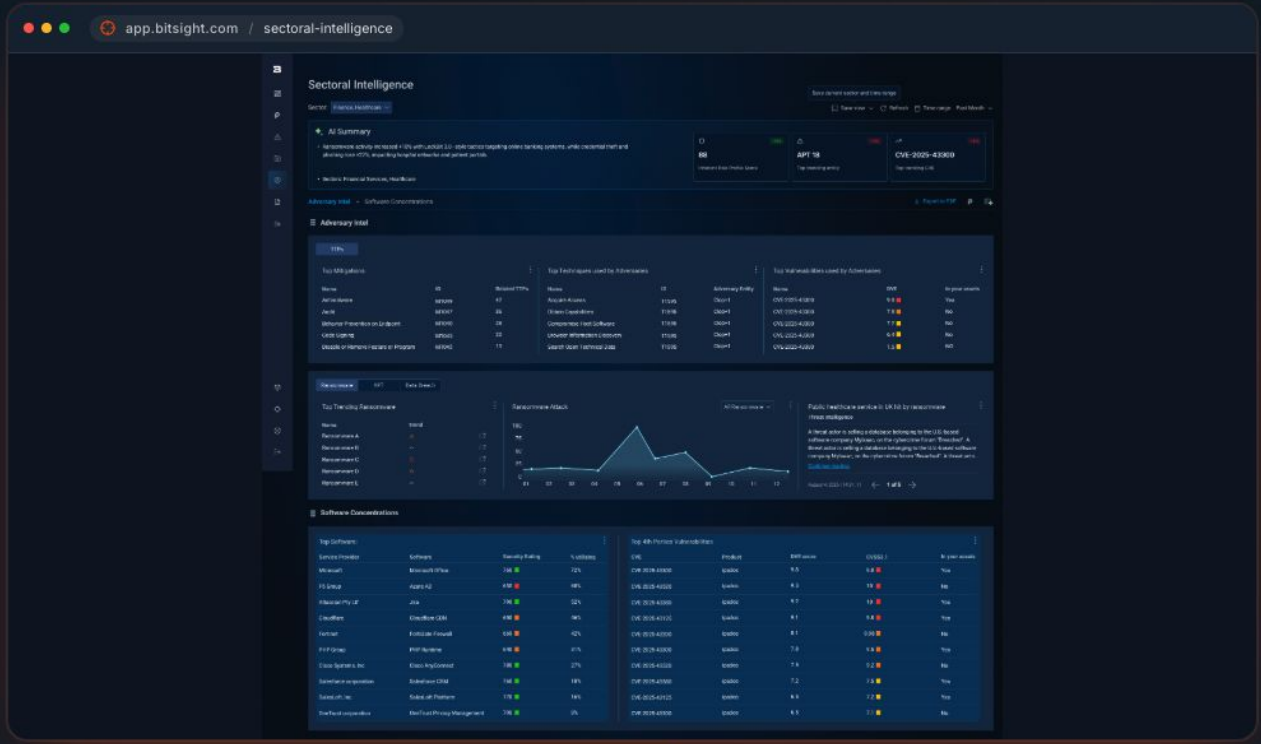
- **Top Mitigations** — identify the controls with the broadest TTP coverage
- **Top Tactics donut** — shows where adversary effort is concentrated
- **Heat-map cells** — light up by Priority Score and active Threat Group

AIM: this view is one input. Bitsight fuses all three into a single prioritized action queue.

Overview | Breach Intelligence | MITRE ATT&CK Mapping | Sectoral Intelligence

← → navigate Esc overview

Sectoral Intelligence



WHAT YOU'RE LOOKING AT

Sectoral Intelligence

Context is your best defense. The industry-wide threat landscape — adversaries, software concentrations, and peer benchmarks — fused into a sector-specific radar so you see what's coming before it hits the fence.

- **Know the Adversary** — real-time TTPs and ransomware trends specific to your industry
- **Map the Surface** — systemic software concentrations and 4th-party vulnerabilities inherent to your sector
- **Benchmark Your Stance** — security ratings, credential exposure, and vulnerability density vs. industry peers

AIM: this view is one input. Bitsight fuses all three into a single prioritized action queue.

Overview | Breach Intelligence | MITRE ATT&CK Mapping | Sectoral Intelligence

← → navigate Esc overview

DEEP DIVE · ACT

Accelerate Remediation at Scale

FROM INSIGHT TO REMEDIATION

MEAN TIME TO REMEDIATE

~~Days~~ › Minutes

Bitsight Agents triage, route, and act on findings the moment they appear — at machine speed, with human oversight.

SHIFT TO OUTCOMES
01

Native Agent Workflows

Watch embedded agents triage, route, and resolve critical findings autonomously.

SUPERCHARGE YOUR AGENT
02

MCP Integration

Plug your custom agents into Bitsight Skills via the Model Context Protocol.

OUT-OF-THE-BOX
03

Bitsight Integrations

Plug-and-play connectors across TPRM, SPM, and CTI — ServiceNow, JIRA, Splunk, Sentinel and more.

Accelerate Remediation at Scale

PLAY DEMO

Triage & Routing — Live

AUTO-PILOT

CRITICAL	Exposed LiteLLM gateway · auth bypass vendor-a.io	Auto-ticketed → Jira INC-2417	just now
HIGH	MCP server reachable without TLS supplier-b.com	Vendor email drafted · awaiting approve	2m
HIGH	Citrix NetScaler CVE-2026-3104 partner-c.net	Routed to Patch Squad · ServiceNow	6m
MEDIUM	Leaked LLM API key in JS bundle vendor-f.app	Slack alert → #appsec-triage	9m

Embedded Agent Logic

Findings flow through a deterministic agent before reaching humans.

Score & Contextualize
Severity × business criticality

Policy Check
Match against GRC standards

Auto-Action
Ticket · email · escalate · notify

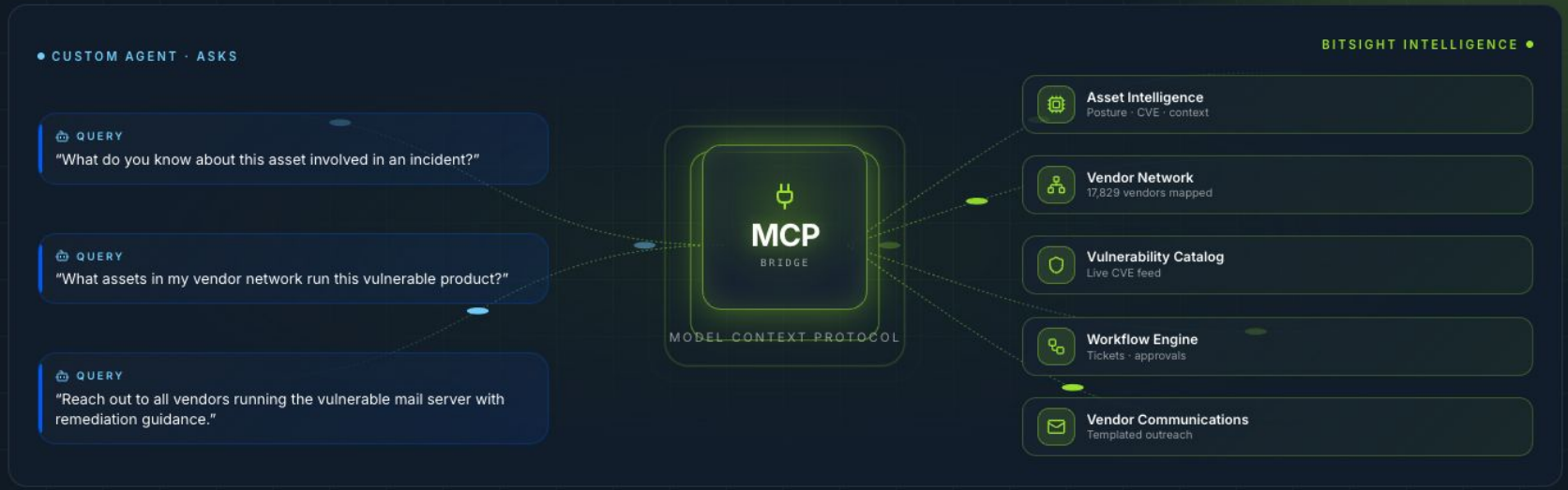
Report Outcomes
Summarize actions taken and risk reduced

OUTCOME

82% reduction in manual SecOps triage on Bitsight findings.

Accelerate Remediation at Scale

CONNECT YOUR AGENTS TO BITSIGHT'S INTELLIGENCE LAYER.



BYO AGENT **Your code, our intel** — over a single audited protocol. Plug any agent into Bitsight Skills and stream live exposure context back into your workflow.

Accelerate Remediation at Scale

OUT-OF-THE-BOX CONNECTIVITY ACROSS TPRM, SPM, AND CTI.

WORK WHERE YOU LIVE

Bitsight is the data layer inside the tools your teams already use — minimum swivel-chair, maximum time-to-value.

EASY · MEDIUM · ROADMAP

GRC · VRM

VENDOR RISK · PROCUREMENT

Operationalize risk across the entire vendor lifecycle — from procurement through continuous monitoring.

- ServiceNow TPRM — EASY
- Archer — MED
- Auditboard — EASY
- Coupa — COMING APR
- OneTrust — COMING Q2

Risk-informed decisions across the vendor lifecycle.

SECOPS

REMEDIATION · RESPONSE

Transform findings into traceable work inside the engineering and security ticket queues your team already lives in.

- ServiceNow ITSM · VR · SIR — EASY
- JIRA — MED
- Splunk — EASY
- Sentinel — EASY
- Cortex XSOAR — EASY

Faster remediation — issues tracked where work happens.

REPORTING

DASHBOARDING · BI

Communicate risk posture to practitioners and the Board using the business intelligence tools you already standardize on.

- PowerBI — EASY
- Tableau — EASY

AUDIENCES

Executive · Practitioner · Board

Live data feeds — single source of truth for risk reporting.

THE STATE OF THIRD-PARTY RISK

30%

of breaches now originate in your supply chain.

Source: Verizon DBIR, 2025

The signals exist. They're just hard to find —
buried in noise, scattered across sources, and detached from the vendor context your team needs to act.

We built the detection layer that closes that gap.

◀ SEE IT IN ACTION

When the Breach Hits, The Signals Were Already There

ONE OF THE 30% · RECENT CASE

Acme Financial · April 12, 2026

SEC · FORM 8-K · MATERIAL CYBERSECURITY INCIDENT

Data breach via third-party logistics supplier

DISCLOSED	April 12, 2026 · 8:04 AM ET
RECORDS EXPOSED	2.4M customer records · PII · financial data
ATTACK VECTOR	Compromised vendor credentials
INITIAL ACCESS	97 days prior to disclosure

BLACKBASTA LEAK PORTAL · TOR HIDDEN SERVICE

ACME FINANCIAL

● RANSOM UNPAID · COUNTDOWN ACTIVE

02:14:37:12 UNTIL FULL DUMP

Negotiations terminated. 4.2 TB customer data pending release.

BLOOMBERG · FINANCE · BREAKING

Acme Financial CEO faces Senate inquiry after supply chain breach exposes 2.4M customers

Shareholders file class action. Credit rating placed on negative watch. Third-party supplier had known unpatched vulnerabilities for 62 days.

2h ago · 847 comments

◆ INCIDENT FALLOUT · ONGOING

CLASS ACTION	Filed · $180M+ sought
REGULATORY	FTC probe opened · 48 state AGs notified
GDPR FINE	Estimated €50–120M
VENDOR CONTRACT	Terminated · transition cost $4.2M

Estimated total incident cost: $340M — still growing

This is what a third-party breach actually costs — long after the initial compromise.

Every one of these breaches has a timeline. Most teams only see the end of it.

◀ REWIND THE TIMELINE

When the Breach Hits, The Signals Were Already There

REWINDING THE KILL CHAIN

● PRE-INCIDENT · INFRASTRUCTURE EXPOSURE

Exposed PostgreSQL instance detected on vendor infrastructure

VENDOR	logistics-partner-07.acme-sc.io
CVE	CVE-2023-4891 — Unpatched, CVSS 9.8
PORT	5432/tcp exposed to public internet
ATTRIBUTION	Subsidiary acquired 2023 · not in primary CMDB

SIEM-READY PAYLOAD

```
{"signal":"exposure","severity":"critical","mitre":"T1190","siem_ready":true}
```

When the Breach Hits, The Signals Were Already There

REWINDING THE KILL CHAIN

● PRE-INCIDENT · INFRASTRUCTURE EXPOSURE

Exposed PostgreSQL instance detected on vendor infrastructure

VENDOR	logistics-partner-07.acme-sc.io
CVE	CVE-2023-4891 — Unpatched, CVSS 9.8
PORT	5432/tcp exposed to public internet
ATTRIBUTION	Subsidiary acquired 2023 · not in primary CMDB

SIEM-READY PAYLOAD

```
{"signal":"exposure","severity":"critical","mitre":"T1190","siem_ready":true}
```

● ACTIVE INTRUSION · MALICIOUS ACTIVITY

C2 beacon traffic from vendor infrastructure

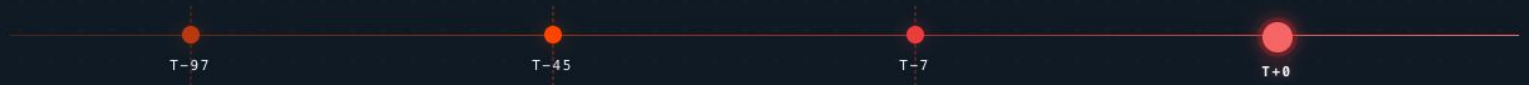
VENDOR	logistics-partner-07.acme-sc.io
C2 DESTINATION	185.×××.×××.42 · known APT infrastructure
BEACON INTERVAL	300s ± 15s jitter — consistent with CobaltStrike
MITRE ATT&CK	T1071.001 · Application Layer Protocol

SIEM-READY PAYLOAD

```
{"signal":"c2_beacon","mitre":"T1071.001","siem_ready":true}
```

When the Breach Hits, The Signals Were Already There

REWINDING THE KILL CHAIN



● PRE-INCIDENT · INFRASTRUCTURE EXPOSURE

Exposed PostgreSQL instance detected on vendor infrastructure

VENDOR	logistics-partner-07.acme-sc.io
CVE	CVE-2023-4891 — Unpatched, CVSS 9.8
PORT	5432/tcp exposed to public internet
ATTRIBUTION	Subsidiary acquired 2023 · not in primary CMDB

SIEM-READY PAYLOAD

```
{"signal":"exposure","severity":"critical","mitre":"T1190","siem_ready":true}
```

● ACTIVE INTRUSION · MALICIOUS ACTIVITY

C2 beacon traffic from vendor infrastructure

VENDOR	logistics-partner-07.acme-sc.io
C2 DESTINATION	185.×××.×××.42 · known APT infrastructure
BEACON INTERVAL	300s ± 15s jitter — consistent with CobaltStrike
MITRE ATT&CK	T1071.001 · Application Layer Protocol

SIEM-READY PAYLOAD

```
{"signal":"c2_beacon","mitre":"T1071.001","siem_ready":true}
```

● POST-COMPROMISE · BREACH EVIDENCE

Vendor credentials on ransomware leak site

SOURCE	BlackBasta leak site · monitored
CREDENTIAL COUNT	847 vendor employee credentials
INCLUDES	VPN access · Okta admin · portal tokens
CONFIDENCE	98% — domain match, email pattern

SIEM-READY PAYLOAD

```
{"signal":"leaked_creds","source":"blackbasta","siem_ready":true}
```

When the Breach Hits, The Signals Were Already There

REWINDING THE KILL CHAIN

● PRE-INCIDENT · INFRASTRUCTURE EXPOSURE

Exposed PostgreSQL instance detected on vendor infrastructure

VENDOR	logistics-partner-07.acme-sc.io
CVE	CVE-2023-4891 — Unpatched, CVSS 9.8
PORT	5432/tcp exposed to public internet
ATTRIBUTION	Subsidiary acquired 2023 · not in primary CMDB

SIEM-READY PAYLOAD

```
{"signal":"exposure","severity":"critical","mitre":"T1190","siem_ready":true}
```

● ACTIVE INTRUSION · MALICIOUS ACTIVITY

C2 beacon traffic from vendor infrastructure

VENDOR	logistics-partner-07.acme-sc.io
C2 DESTINATION	185.×××.×××.42 · known APT infrastructure
BEACON INTERVAL	300s ± 15s jitter — consistent with CobaltStrike
MITRE ATT&CK	T1071.001 · Application Layer Protocol

SIEM-READY PAYLOAD

```
{"signal":"c2_beacon","mitre":"T1071.001","siem_ready":true}
```

● POST-COMPROMISE · BREACH EVIDENCE

Vendor credentials on ransomware leak site

SOURCE	BlackBasta leak site · monitored
CREDENTIAL COUNT	847 vendor employee credentials
INCLUDES	VPN access · Okta admin · portal tokens
CONFIDENCE	98% — domain match, email pattern

SIEM-READY PAYLOAD

```
{"signal":"leaked_creds","source":"blackbasta","siem_ready":true}
```

● LIVE · PUBLIC DISCLOSURE

T + 0

PUBLIC FALLOUT

Breach hits the headlines

If you're only reacting at T+0, you've already lost. The signal at T-97 is where the breach was preventable.

• INTRODUCING

Bitsight Beacon

SUPPLY CHAIN EXPOSURE MANAGEMENT

Give your SOC and TPRM teams deeper visibility into critical vendors with validated, evidence-backed intelligence — and enable faster remediation.