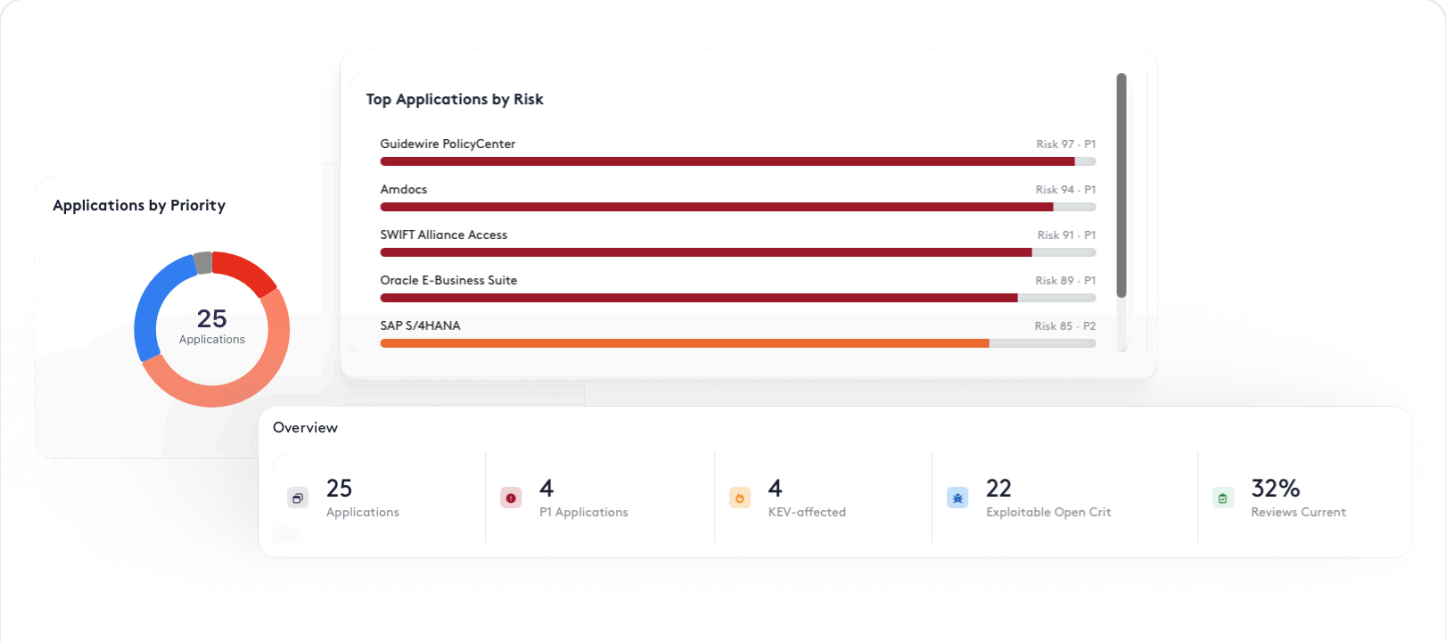
DataBee® for Frontier AI Defense

Turn thousands of vulnerability findings into the handful of fixes that matter most.

DataBee for Frontier AI Defense helps organizations move beyond vulnerability discovery and focus on vulnerability reduction by connecting findings to business applications, ownership information, and remediation workflows. DataBee doesn't scan. It makes the scanners you already own agree with each other. Instead of presenting thousands of findings, DataBee identifies the small number of fixes that can deliver the greatest reduction in business exposure.



Application Risk Posture — exposure, ownership, and top applications by risk in one view.

The New Reality: Attackers Are Moving Faster Than Defenders

When a critical vulnerability emerges, security leaders must quickly answer four business questions:

01 **Which applications are exposed?**

02 **Who owns them?**

03 **What should be fixed first?**

04 **Was it actually fixed?**

The information needed to answer those questions is typically distributed across multiple systems. Vulnerability scanners identify findings. CMDB platforms maintain infrastructure ownership. Application inventories track business systems. Service management tools coordinate remediation. Bringing these data sources together often requires manual effort, delaying remediation and increasing risk.

How DataBee Reduces the Risk of Frontier AI

DataBee for Frontier AI Defense transforms vulnerability management from findings-based prioritization to risk-driven exposure remediation. Rather than focusing on individual findings, DataBee combines vulnerability intelligence, exploitation evidence, business application context, ownership information, and remediation workflows into a unified operating model.

Three capabilities differentiate this approach.

01

One Exposure Score Across the Enterprise

Organizations frequently operate multiple vulnerability tools, each with its own scoring methodology and prioritization model. DataBee normalizes exposure data across tools and supplements vulnerability information with exploitation intelligence, helping organizations evaluate risk using a common framework. Open any application and the score breaks into the numbers behind it — no black box, and nothing to take on trust.

02

Business Application-Centric Prioritization

Most tools prioritize individual hosts or devices. DataBee prioritizes business applications. By correlating assets, vulnerabilities, application inventories, and ownership information, DataBee connects findings to business applications, ownership, and remediation workflows. This allows organizations to focus resources on the assets that matter most to business operations.

03

Thousands of Findings Become a Manageable Set of Actions

DataBee for Frontier AI Defense cuts remediation complexity by grouping vulnerabilities according to the fixes that resolve them, so security teams work from a short, actionable list instead of a flood of individual findings. For example, 888 open findings become 15 distinct fixes that clear 807 of them — a week of scheduled work instead of an impossible backlog, creating a more actionable remediation plan for operational teams,

Accelerate Zero-Day Response with DataBee

Zero-day events place extraordinary pressure on security teams. When a newly exploited vulnerability emerges, organizations must rapidly determine exposure, identify affected systems, locate owners, and coordinate remediation. These activities often involve multiple teams operating across disconnected systems.

DataBee for Frontier AI Defense lets you type in the CVE and see every exposed application, the specific servers, and the person who owns each one — then compiles the change requests straight from that view. This provides security leaders with a single view of exposure while helping operational teams move more quickly from detection to remediation.

Key Business Outcomes

Organizations that use DataBee for Frontier AI Defense improve their ability to:

- Prioritize remediation using business context rather than technical severity alone.
- Correlate vulnerabilities to applications, assets, and owners.
- Reduce remediation backlog complexity by focusing on high-impact fixes.
- Improve accountability through owner-based remediation workflows.
- Accelerate response to actively exploited vulnerabilities and zero-day events.
- Demonstrate remediation progress through SLA tracking and executive reporting.

When the next critical vulnerability lands, the difference between hours and days comes down to whether the answer is already assembled. DataBee for Frontier AI Defense makes sure it is, connecting the vulnerability, asset, ownership, and workflow data organizations already have into one continuously prioritized view.

To see how it works against your own application and vulnerability data, schedule a demo at **databee.ai**.