DataBee
A COMCAST COMPANY

SOLUTION BRIEF

DataBee® for Frontier AI Defense

Built for the AI-accelerated exposure management landscape.

> **When a critical vulnerability breaks, DataBee tells you within hours—not days—which applications are actually at risk, who owns them, and which fixes to prioritize first for the best remediation outcome. No spreadsheets to reconcile, no owners to chase down, no guessing which CVE actually matters.**

With the average time-to-exploit shrinking from 5 days to –1 in a year, the time to find and fix vulnerabilities has closed. Now the problem is prioritizing the right exposure to close. When a new CVE lands, most teams don't have the information on hand to act—ownership and business context are scattered across disconnected CMDBs, application provisioning directories, and detection tools, so the first critical hours get spent reconciling spreadsheets instead of remediating.

That's where DataBee for Frontier AI Defense comes in: it connects the vulnerability, asset, and ownership data you already have into one always-current view, so the moment a zero-day breaks, you already know what's at risk and what to fix first.

Validated fixes
to ensure the vulnerability is actually closed

Hundreds of findings
collapsed into a handful of fixes*

Application risk score
not device vulnerability counts

Key Outcomes

01 **Focus on what matters first.** Application business risk combines with scanner severity and asset criticality, so teams know exactly which fixes to apply first for the best remediation outcome—not just a raw list of CVEs.

02 **Know who owns it on day one.** Ownership is attributed automatically from your existing organizational data, so the right person is identifiable immediately, not after rounds of escalation.

03 **See what's actually at risk.** DataBee connects the vulnerability and application data you already have into one current view, so nothing gets reconciled by hand across spreadsheets and tools.

04 **Full lineage, start to finish.** Every risk, priority, and ownership decision traces back to its source data—the same lineage responders, leadership, and audit all rely on.

How It Works

01
Connect
Connects to the vulnerability and application data you already have—no lengthy integration project, no new tools for your team to learn.

02
Resolve
Deduplicates and connects records into one current inventory behind the scenes, pulling in business application and owner context wherever your CMDB or application provisioning system maps it.

03
Respond
When a CVE lands, DataBee surfaces every exposed asset with owner and business context already attached. Security teams login and business owners receive the tickets that matter to them..

04
Verify
Validate that the applied patch fixed the vulnerability, ensuring that your critical systems are actually protected.

Key Capabilities

Risk prioritization. Scanner severity combines with asset criticality, confirmed exploitation, and business context, so teams move beyond raw CVE scores to what to fix first.

Unified vulnerability & asset data. Scanner findings are continuously correlated to the asset inventory, so every finding is linked to its owner and ready for assessment instantly.

Business application context. Where your CMDB maps devices to applications, that mapping travels with every asset and finding, so impact and owner are never separated.

Entity resolution (patent-pending). One continuously updated record per real-world entity, deduplicated and connected across every source—no inflated or fragmented exposure counts.

Ownership travels with every finding. The business owner who funds the application and the remediation owner who patches the device, both read from data you already maintain. Where ownership is missing, DataBee flags the gap.

Remediation workflow orchestration. Findings meeting your criteria trigger tickets in your ITSM with full asset, application, and owner context, recorded for accountability.

Built for Cybersecurity Teams

ROLE	WHAT THIS DELIVERS
CISO / BISO	A defensible “are we exposed?” answer on day one—risk, impact, and owners ready for leadership and the board.
Vulnerability & Threat Response	A continuously updated inventory with ownership and vulnerability correlation, so exposure assessment is fast.
SOC, IR & Threat Hunting	Instant exposure assessment with business context and ownership attached, so triage doesn’t stall on lookups.

Why DataBee

One platform, many outcomes. Every DataBee solution runs on the same connected data foundation, so investment compounds across your program. Start with Frontier AI Defense and then scale across your entire program.

Your data, your storage. DataBee processes your data, then places it in your own data lake or cloud storage. No vendor lock-in.

Works with what you already have. Connects to your existing security, IT, and business systems—no disruption to the platforms your teams rely on.

Current and defensible. What you see reflects your environment today, and every result traces back to its source data.

**For example, 888 findings collapse into 15 fixes that close 807 of them – a week of scheduled work, not an impossible backlog.*