



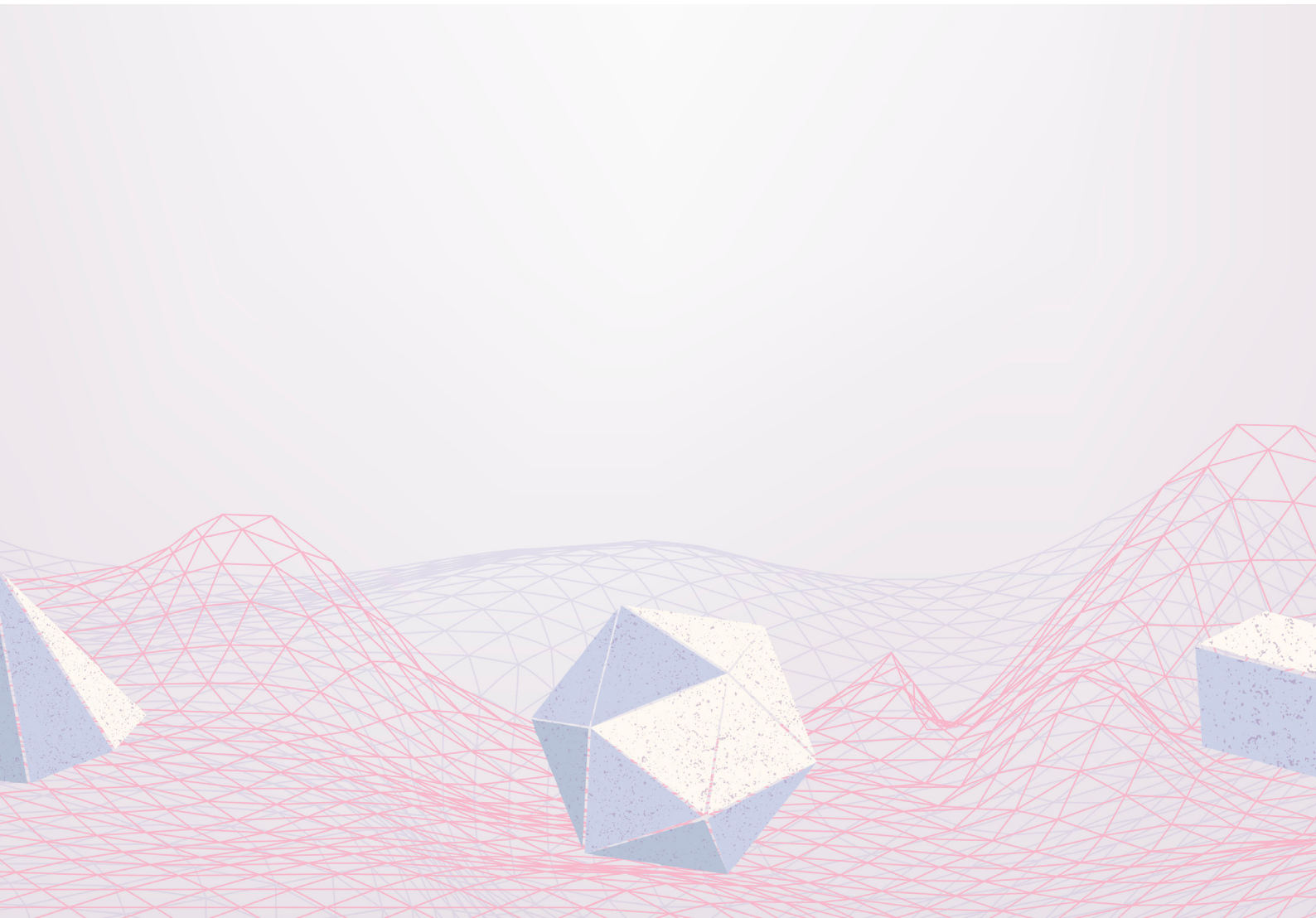
Connect the Dots in Data & AI

Know your data and AI. Control your data and AI.

Cloud-native and agentless — built for speed, accuracy, and scale.

BigID Data Activity Monitoring

Unify visibility, monitoring, and remediation across **AWS S3, OneDrive, SharePoint, File Shares**, and **Google Drive** — detect insider threats, mitigate breach risk, and enforce Zero Trust with AI-powered insights.



Connect the Dots in Data & AI



Know your data and AI. Control your data and AI.

Cloud-native and agentless — built for speed, accuracy, and scale.

► Cloud-native

► Agentless

► Enterprise-Scale

► Fast & Accurate

BigID Data Activity Monitoring

Monitor, Detect, and Remediate Data Risks Across Cloud, On-Premises, and Hybrid Environments

BigID's Data Activity Monitoring (DAM) delivers continuous, contextual insight into who is accessing your data, when, how, and why — across users, service accounts, automated workflows, and AI agents. By unifying deep data intelligence with continuous monitoring, Activity Explorer, and automated remediation, BigID empowers organizations to detect insider threats, address over-permissioned identities, catch risky data sharing, and enforce Zero Trust at scale.

With native Cloud DLP integration, support for critical sources like AWS S3, OneDrive, SharePoint, File Shares (SMB), NetApp, and Google Drive, and AI-powered threat detection, BigID enables teams to move from reactive alerts to proactive action — reducing breach risk, strengthening compliance, and minimizing disruption.

- Continuously monitor sensitive data activity across AWS S3, OneDrive, SharePoint, File Shares, NetApp, Google Drive, and others
- Detect insider threats, over-permissioned users, suspicious downloads, and data shared to personal accounts
- Monitor and analyze activity across user accounts, service accounts, and AI agents
- Investigate incidents quickly using Activity Explorer's unified audit log
- Accelerate investigations with AI-powered detection and contextual correlation
- Support required audit logging for HIPAA, GLBA, GDPR, CCPA, and other regulations
- Automate remediation and Cloud DLP enforcement to reduce exposure
- Maintain audit-ready trails for compliance, governance, and executive reporting

FRAGMENTED MONITORING LEAVES DATA RISKS UNDETECTED

Traditional monitoring tools and DDR approaches lack data sensitivity context and do not unify activity across hybrid environments — creating blind spots across unstructured data, collaboration platforms, and cloud file shares.

False positives overwhelm analysts while true insider threats, accidental misuse, AI-driven access, and over-permissioned accounts go unnoticed.

With the rise of SaaS, Google Drive sprawl, service accounts, and AI agents accessing enterprise data, security teams face more exposure than ever — without the insight to separate normal behavior from risky or malicious activity. This fragmented visibility makes it difficult to enforce Zero Trust, investigate breaches, or meet regulatory requirements for complete auditability.

CONTEXTUAL MONITORING THAT POWERS PROACTIVE PROTECTION

BigID's DAM brings together access visibility, deep data context, Activity Explorer, and automated remediation in one unified solution. By combining data classification, identity-aware sensitivity, ownership, and entitlements with continuous monitoring and AI-powered detection, BigID delivers actionable intelligence — not noise.

Security teams can detect insider threats earlier, respond faster, and enforce least privilege without disrupting business. With coverage across AWS S3, OneDrive, SharePoint, File Shares (SMB), NetApp, Google Drive, and email, BigID eliminates blind spots, helps prevent breaches, and strengthens DSPM and Cloud DLP programs.

Get Complete Visibility

Continuously monitor activity across sensitive data — structured and unstructured — with full context on who accessed what, when, how, and why, including activity from users, service accounts, automated workflows, and AI agents.

Reduce Risk & Enable Zero Trust

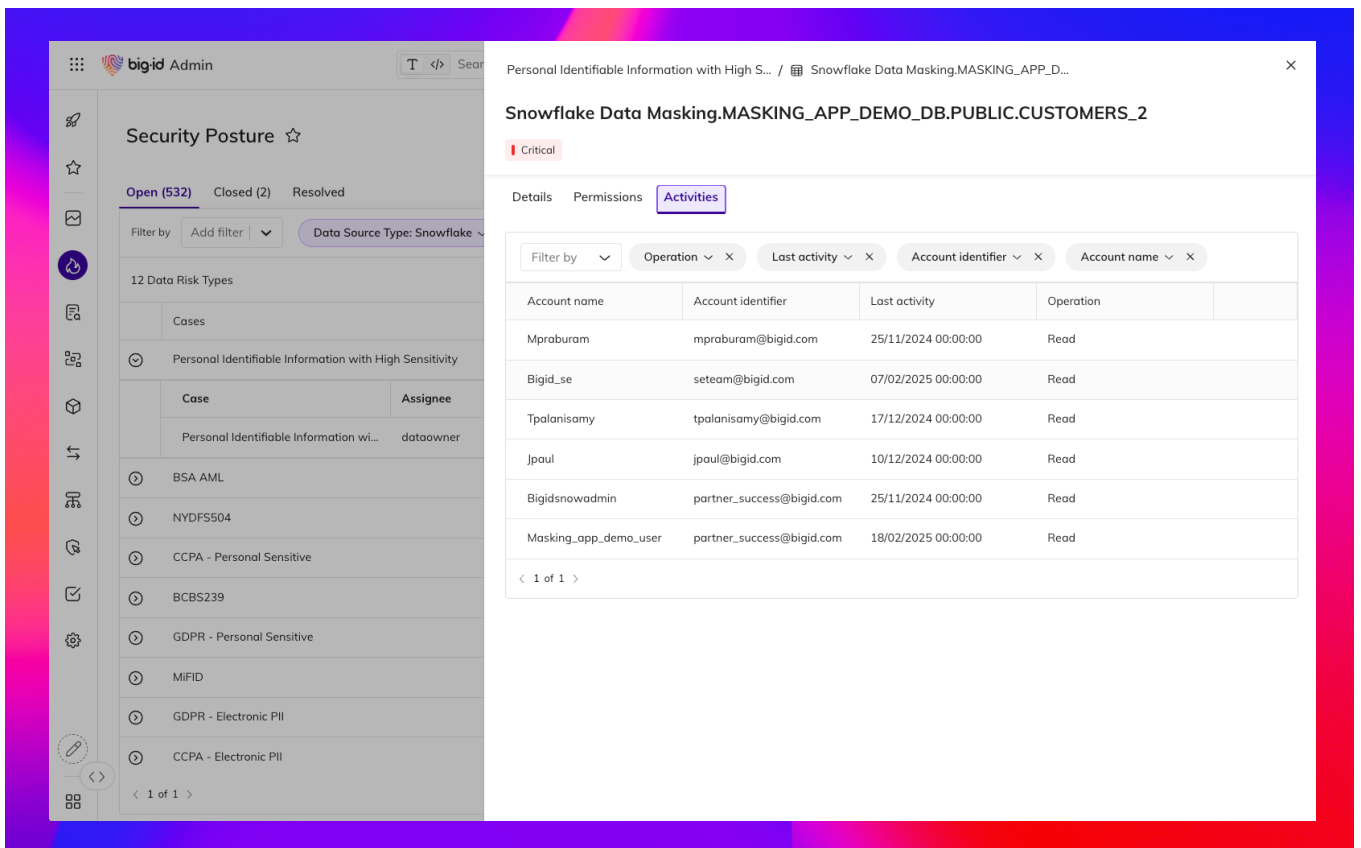
Detect over-permissioned users, insider threats, suspicious downloads, and personal email exfiltration — and remediate before risks become breaches.

Accelerate Investigations

Leverage Activity Explorer and AI-powered insights to filter activity by identity, operation, resource, or date — cutting investigation time and helping teams quickly answer questions like “Who deleted this file?” or “What did this account access yesterday?”

Automate Risk Response

Enforce access policies, revoke permissions, or trigger Cloud DLP actions directly from BigID's Action Center — or integrate with IAM and security tools for automated response.



The screenshot displays the big.id Admin console. On the left, the 'Security Posture' section is active, showing a list of 12 Data Risk Types. The main panel on the right shows the 'Snowflake Data Masking.MASKING_APP_DEMO_DB.PUBLIC.CUSTOMERS_2' dataset with a 'Critical' status. The 'Activities' tab is selected, displaying a table of user activities.

Account name	Account identifier	Last activity	Operation
Mpraburam	mpraburam@bigid.com	25/11/2024 00:00:00	Read
Bigid_se	seteam@bigid.com	07/02/2025 00:00:00	Read
Tpalanisamy	tpalanisamy@bigid.com	17/12/2024 00:00:00	Read
Jpaul	jpaul@bigid.com	10/12/2024 00:00:00	Read
Bigidsnowadmin	partner_success@bigid.com	25/11/2024 00:00:00	Read
Masking_app_demo_user	partner_success@bigid.com	18/02/2025 00:00:00	Read

CAPABILITIES THAT POWER DATA ACTIVITY MONITORING

Unified Investigation & Response

Correlate access patterns with metadata, sensitivity, and ownership for a 360° view of data activity. Activity Explorer provides a unified audit log for users, service accounts, and AI agents — streamlining investigations and guiding remediation to minimize time-to-action.

Context-Rich Intelligence

Fuse activity with permissions, classification, entitlements, and identity context to deliver accurate, context-aware insights across AWS S3, OneDrive, SharePoint, File Shares (SMB), NetApp, and Google Drive.

Sensitive Data Sharing Alerts

Catch sensitive files being shared with personal email accounts or external domains. AI distinguishes accidental misuse from suspicious insider activity, with customizable policies by data type, user group, or sensitivity.

Google Drive Monitoring

Gain visibility into file access, sharing, copying, downloads, and movement in Google Drive. Correlate activity with identity, sensitivity, and policy violations to reduce sprawl and enforce governed sharing.

Breach Investigation & Blast-Radius Analysis

Determine the full scope of a breach by identifying every file or dataset a compromised account accessed during a defined window. Accelerate containment with precise exposure mapping.

Safe, Automated Remediation

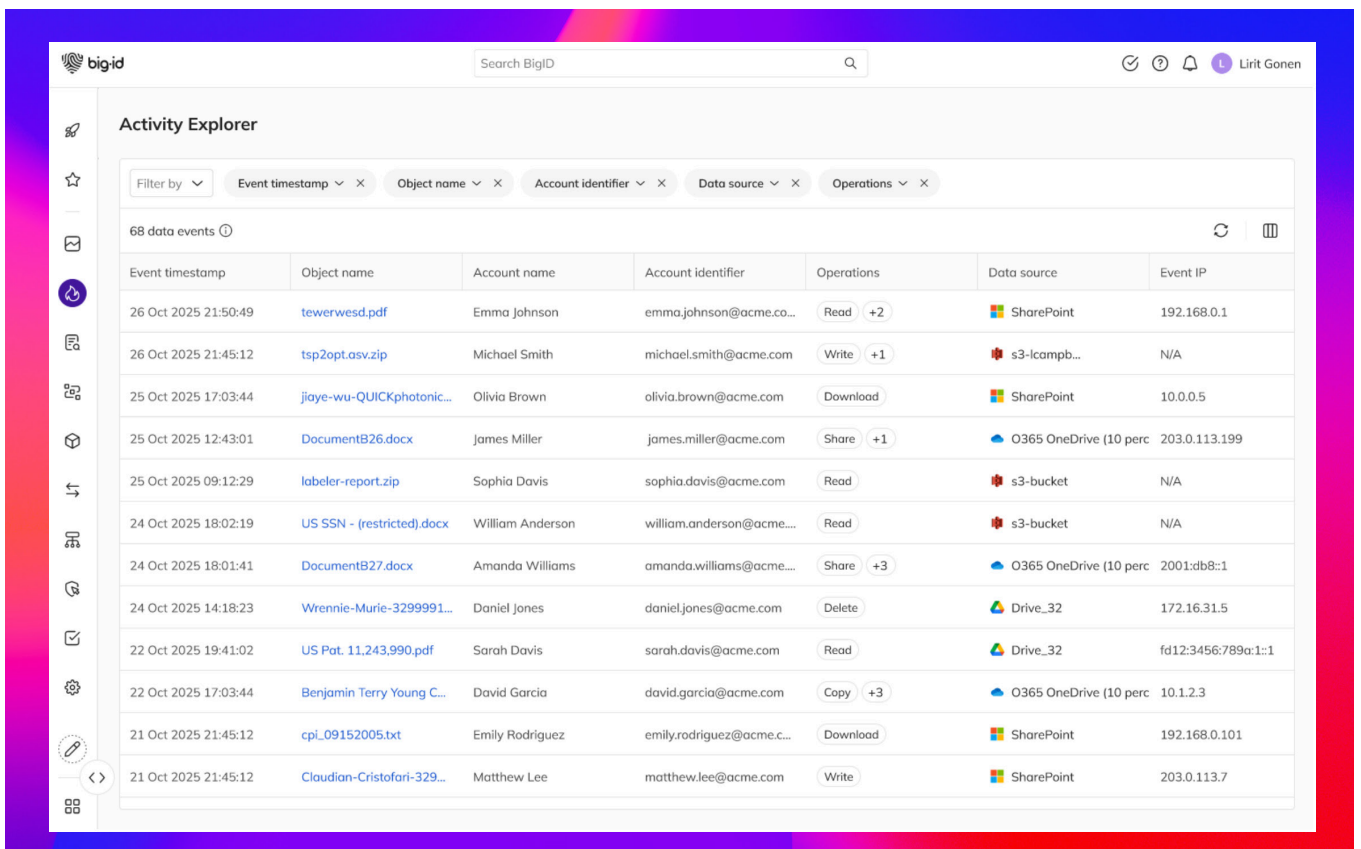
Revoke unnecessary access, enforce entitlement policies, reduce over-permissions, and trigger Cloud DLP workflows — all directly through BigID or integrated IAM/SOAR tools.

Retention & Minimization Insights

Use real-access patterns (not just last-modified timestamps) to identify unused or ROT data for archival or deletion. Enforce retention and lifecycle policies with confidence.

Audit & Compliance Reporting

Generate audit-ready activity logs and reports for GDPR, CCPA, HIPAA, GLBA, PCI, and emerging AI governance requirements. Demonstrate full access visibility and compliance with mandated audit logging.



The screenshot shows the BigID Activity Explorer interface. At the top, there's a search bar labeled "Search BigID" and a user profile for "Lirit Gonen". Below the search bar, the "Activity Explorer" section is active. It features a "Filter by" dropdown and several filter buttons: "Event timestamp", "Object name", "Account identifier", "Data source", and "Operations". Below the filters, it indicates "68 data events". The main table displays a list of activity events with columns: "Event timestamp", "Object name", "Account name", "Account identifier", "Operations", "Data source", and "Event IP".

Event timestamp	Object name	Account name	Account identifier	Operations	Data source	Event IP
26 Oct 2025 21:50:49	tewerwesd.pdf	Emma Johnson	emma.johnson@acme.co...	Read +2	SharePoint	192.168.0.1
26 Oct 2025 21:45:12	tsp2opt.asv.zip	Michael Smith	michael.smith@acme.com	Write +1	s3-lcampb...	N/A
25 Oct 2025 17:03:44	jiaye-wu-QUICKphonic...	Olivia Brown	olivia.brown@acme.com	Download	SharePoint	10.0.0.5
25 Oct 2025 12:43:01	DocumentB26.docx	James Miller	james.miller@acme.com	Share +1	O365 OneDrive (10 perc	203.0.113.199
25 Oct 2025 09:12:29	labeler-report.zip	Sophia Davis	sophia.davis@acme.com	Read	s3-bucket	N/A
24 Oct 2025 18:02:19	US SSN - (restricted).docx	William Anderson	william.anderson@acme...	Read	s3-bucket	N/A
24 Oct 2025 18:01:41	DocumentB27.docx	Amanda Williams	amanda.williams@acme...	Share +3	O365 OneDrive (10 perc	2001:db8::1
24 Oct 2025 14:18:23	Wrennie-Murie-3299991...	Daniel Jones	daniel.jones@acme.com	Delete	Drive_32	172.16.31.5
22 Oct 2025 19:41:02	US Pat. 11,243,990.pdf	Sarah Davis	sarah.davis@acme.com	Read	Drive_32	fd12:3456:789a:1::1
22 Oct 2025 17:03:44	Benjamin Terry Young C...	David Garcia	david.garcia@acme.com	Copy +3	O365 OneDrive (10 perc	10.1.2.3
21 Oct 2025 21:45:12	cpi_09152005.txt	Emily Rodriguez	emily.rodriguez@acme.c...	Download	SharePoint	192.168.0.101
21 Oct 2025 21:45:12	Claudian-Cristofari-329...	Matthew Lee	matthew.lee@acme.com	Write	SharePoint	203.0.113.7



Connect the Dots in Data & AI

Know your data and AI. Control your data and AI.

Cloud-native and agentless — built for speed, accuracy, and scale.

► Cloud-native

► Agentless

► Enterprise-Scale

► Fast & Accurate

About BigID

BigID helps organizations connect the dots across data & AI: for security, privacy, compliance, and AI data management. BigID enables customers to find, understand, manage, protect, and take action on high risk & high value data, wherever it lives.

Customers use BigID to reduce their AI & data risk, automate security and privacy controls, achieve compliance, and understand their data throughout their entire data landscape: from the cloud, on-prem, and everywhere in between.



Tools like BigID are the future.

Organizations should be leveraging these tools to remove the manual processes from data discovery, provide better visibility, and help with prioritization of controls.



Ryan O'Leary

Future of Trust: Battling Data Discovery Confusion