ACTIVENAV

Data Security in ActiveNav Cloud

Dedicated to the understanding of unstructured data wherever it lies, we've been providing data discovery software across all industries and geographies for decades. Our North Star vision is Zero Dark Data, through which we enable our customers to meet the requirements of modern data regulations, reduce and protect their sensitive data holdings and lower the blast radius of the inevitable data breach or discovery event.

As our flagship product, ActiveNav Cloud is designed enable this vision and allow governance and compliance teams to maintain constant oversight into unstructured data composition, location and risk so they can protect the organization and reduce the burden of data ownership.

Ever-Present Threat

Be it from carelessness or accident, most security incidents and data spillages are a result of internal user error. Quite simply, users cannot be expected to stay ahead of evolving data policies and information architecture and so, in the event of the inevitable data breach, its highly likely that the threat actor will be able to readily access a range of sensitive or regulated data. ActiveNav Cloud provides aggregated insights across all unstructured data sources so that governance and compliance teams can identify and minimize sensitive data hotspots and drive a net reduction of data risk and threat surface area.

Industry Leading Protection

ActiveNav Cloud uses a comprehensive layered approach to information security, purpose built to protect our customers' data.

- Hosted in Microsoft's Azure's industry-leading cloud platform, ActiveNav Cloud's foundations are assured.
- Our high-performance discovery service collects only the minimum necessary data to provide the insights customers need.
- Any data that is persisted in the ActiveNav Cloud platform is encrypted at rest by Azure services. Any data in transit from discovery to through the service platform to users' web browsers is protected using industry standard secure protocols.
- The ActiveNav Cloud platform is subject to Static Application Security Testing and Software Composition Analysis while the deployed production environment is scanned weekly to check for potential vulnerabilities.
- The production ActiveNav Cloud environment is hosted in a dedicated Azure subscription which is continually monitored for vulnerabilities and suspicious activity using Microsoft Defender for Cloud.
- Our information security management system is certified to ISO27001 standards by LRQA, a leading independent global assurance provider.

Americas
Reston, VA, USA
+1 571 375 2780

EMEA
Winchester, UK
+44 01962 454401

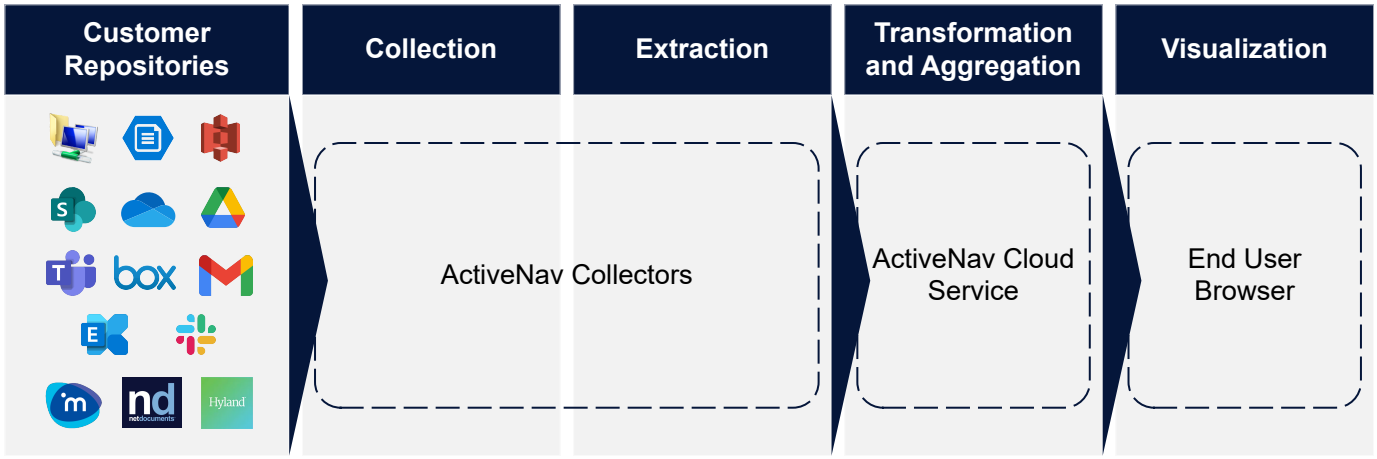
APAC
Melbourne, Australia
+61 3 9982 4543

activenav.com
sales@activenav.com

ACTIVENAV

Minimal Data Collection

ActiveNav Cloud is designed to reduce data risk and event blast radius, not increase it. This means that our service collects the minimum data necessary to provide the insights essential to successful information compliance and governance. Our discovery service collects, transforms, and aggregates data through the stages shown below. Any collected data is stored in a secure Azure Instance in the Azure region chosen and agreed during the contracting process.



	Collection	Extraction	Transformation and Aggregation	Visualization
Where?	Chosen customer Azure region or on-location for on-premise collectors		Chosen customer Azure region	User location
What?	Files and text objects collected from the target repository	Collected metadata, presence and counts of data elements Selected data element values responsive to target search	Collected metadata, presence and counts of data elements Selected data element values responsive to target search	Collected metadata, presence and counts of data elements Selected data element values responsive to target search
Retained?	Metadata (such as object name, container name, age, date, type and size)	The presence and count of data elements Selected element values responsive to target search	The presence and count of data elements and related aggregations Selected element values responsive to target search	N/A
Disposed?	Files and text objects on completion	Values of data elements	Element values responsive to target search on deletion All data on termination of subscription	N/A

Secure Engineering

ActiveNav Cloud is engineered based upon our Product Delivery and Product Security Models that direct the practices necessary to assure the quality and security requirements inherent in a cloud-based SaaS solution. As part of our security model, our engineering team deploys a range of industry best practices for security modeling to identify, assess, prioritize, and mitigate potential issues. Threat models are continuously reassessed and updated as part of our continuous engineering processes. Identified issues are passed through the engineering team's Vulnerability Handling Process, where each potential vulnerability is reported, assessed, classified, and prioritized using the Common Vulnerability Scoring System model. Any vulnerabilities are addressed and subsequently disclosed based upon ISO/IEC 29147:2018 standards.

Americas
Reston, VA, USA
+1 571 375 2780

EMEA
Winchester, UK
+44 01962 454401

APAC
Melbourne, Australia
+61 3 9982 4543

activenav.com
sales@activenav.com

ACTIVENAV

Additionally, our engineering team employs industry recognized quality and security assessment tools including testing and profiling tools from Veracode. Veracode's Static Analysis solution is integrated into the continuous engineering process while Veracode's Dynamic Analysis is executed on a scheduled basis; further, Veracode's Software Composition Analysis (SCA) provides visibility into open-source software used within the service.

All development staff maintain awareness of secure coding practices through formal training courses while access to both test and production instances of the ActiveNav Cloud platform is controlled using role-based access. Access to the production environment Is limited to operations staff and changes in access level are managed according to our ISO27001 certified security management system.

Reduce Data Risk and Event Blast Radius

ActiveNav Cloud provides a complete picture of all your unstructured data assets to provide a transparent assessment of data holdings and compliance. The insights provided enable governance and compliance teams to identify and mitigate sensitive and regulated data hot spots to continually monitor compliance, data health and quality. As a foundation of any information governance program, ActiveNav Cloud drives down risk, reduces the blast radius of breach or e-discovery events and adds transparency to risk compliance.

- Continuous inventory of unstructured data holdings and compliance
- Insights into controlled data elements scored against relevant regulations and policies
- Actionable workflows to identify and mitigate controlled data hotspots
- Reporting for stakeholders engagement, regulatory fulfilment and customers audit transparency

ZERO DARK DATA

VERACODE VERIFIED TEAM

LRQA CERTIFIED ISO/IEC 27001 — UKAS MANAGEMENT SYSTEMS 0001

About Us

We're data experts, and our North Star is Zero Dark Data. We believe that all organizations should be aiming for a state of Zero Dark Data so that they can act as good stewards of that data to minimize their cyber risk surface area, protect the interests of their customers, their staff and their other stakeholders. We've been working continuously with unstructured data in the wild for well over a decade and we think the market deserves data discovery products that just work. As a result we are trusted by leading companies and government agencies to help them understand and control their data assets to drive regulatory compliance, reduce the cost of data ownership and improve data quality.

- 15 Years of Experience
- 6 Continents and 28 Countries
- 15+ Billion Files Discovered
- 30K+ hrs Customer Deployments
- 300+ Customers and Counting

Aside from our fascination with Dark Data, we're engineers, designers, runners, gardeners, chefs, photographers, bikers, parents, skiers, cosplayers, hikers, gamers, travelers, mountain climbers, friends, race car drivers, readers, volunteers, and car enthusiasts. We value loyalty, accountability, and communication and care deeply about creating a sustainable future, supporting charitable causes as proud members of Pledge 1%.

Americas
Reston, VA, USA
+1 571 375 2780

EMEA
Winchester, UK
+44 01962 454401

APAC
Melbourne, Australia
+61 3 9982 4543

Contact sales@activenav.com
LinkedIn activenav
Visit activenav.com

ACTIVENAV

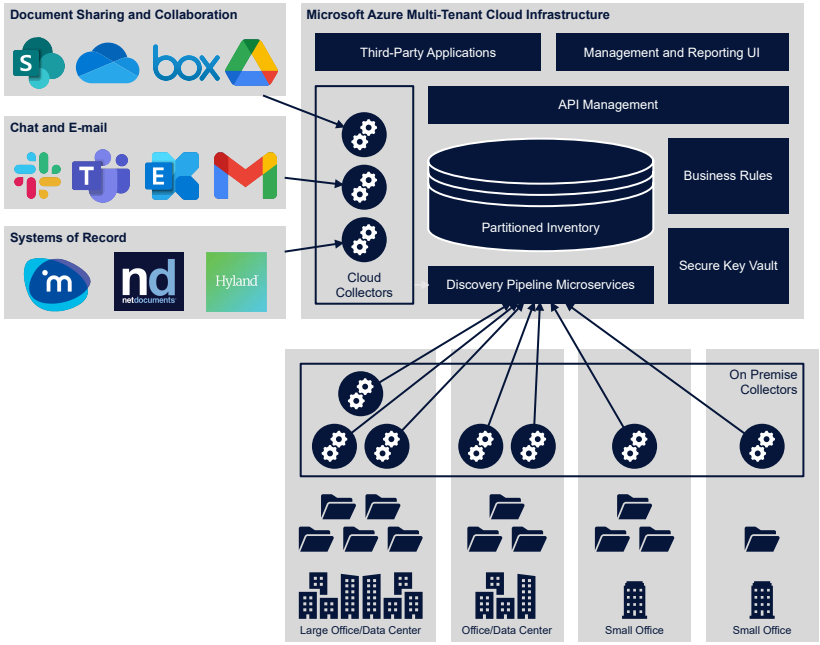
Security FAQ

Overview

ActiveNav Cloud is designed to provide customers with unparalleled insight into their unstructured data. To achieve this, our solution uses a hybrid architecture whereby product components, known as collectors, are deployed close to data repositories, either on premise or in the cloud. These collectors are assigned authority to discover the structure and content of a broad range of unstructured data repositories.

Collectors identify regulated and risky data elements deep in unstructured data formats and pass a de-identified representation of key facts to the cloud platform for further analysis and presentation.

Recognizing that new customers will be seeking assurance that their data is adequately protected, this FAQ provides detailed responses to questions we are often asked about the security of the ActiveNav Cloud platform in its general operation and its storage of data.



Assurance and Compliance

What is ActiveNav's overall security posture?

Recognizing that both our cloud and on-premises products are granted access to the breadth of our customers' data, ActiveNav places security at the top of its business priorities. To achieve this, we maintain a comprehensive Information Security Management System designed around the requirements of the ISO27001 (Information Security Management) standard. This system is applied continuously to all our products and business functions, and compliance with this standard is audited annually by an external body.

What security audits are conducted for ActiveNav's cloud solutions? Can we conduct our own?

External audits are conducted annually by certified ISO27001 auditors. Internal auditors follow a planned program at quarterly intervals overseen by our information security management team. These audits cover all aspects of the business including all aspects of our engineering and services. Audit results can be made available on a case-by-case basis.

We seek to provide adequate evidence for assurance purposes through transparent access to key elements of our Information Security Management System on request. Where a customer seeks to secure additional evidence through its own or third-party audit, that provision would need to be accounted for through an amendment to the standard service purchase terms.

Americas
Reston, VA, USA
+1 571 375 2780

EMEA
Winchester, UK
+44 01962 454401

APAC
Melbourne, Australia
+61 3 9982 4543

activenav.com
sales@activenav.com

ACTIVENAV

What documented security policies and standards do you maintain?

Policies, standards, and procedures are captured and maintained as part of our Information Security Management System which includes our Product Delivery Model which defines our approach to the software delivery lifecycle. As part of our Product Delivery Model we define a Product Security Model for each product. This allows development teams to establish product-specific approaches to secure development and requires the maintenance of a threat model and risk assessment that is reviewed quarterly.

Do any third parties maintain or have access to your cloud solutions?

All engineering and processes relating to the solution are managed by ActiveNav staff. The ActiveNav Cloud platform is hosted in Microsoft Azure, and therefore Microsoft Azure staff support and maintain the underlying host environment.

In general, all vendors that we engage with are subject to vendor risk assessment prior to engaging their services. The assessment considers information technology, operations and information security aspects of the relevant service and assigns a rating according to the nature of the service provided and its business criticality (data security and privacy, financial risk and reputational risk). High criticality vendors are subject to annual review. Vendor performance exceptions are reviewed as part of quarterly management review.

How are employees verified and trained for confidentiality and security?

Pursuant to local laws, regulations, ethics, and contractual constraints, all employees are subject to 10-year background checks, inclusive of federal, state, municipality criminal checks, sexual predator lists, SSN verification, education search, employment verifications, global watchlist search, and professional licenses verification. Confidentiality agreements and/or NDAs are maintained for all staff. These assurances are complemented by annual training and continuous verification of staff security education.

Architecture and Integration

What are key components of ActiveNav's cloud solutions?

ActiveNav Cloud is hosted in Microsoft's Azure's platform and is comprised of the following core components:

- On-premises and cloud-hosted collectors.
- A serverless discovery and processing pipeline.
- Web application for administration and visualization with associated API.

What change management controls are in place to ensure the ongoing availability and security?

All changes to the platform are subject to testing in our development environment and are then deployed to the production environment after formal review and approval.

Rare exceptional changes that may have significant impact are handled by a formal change management process.

Where is the host environment located and how is it secured?

Microsoft's Azure platform maintains ISO 27001, 27017, 20018 and SOC2 compliance amongst others. Full details can be found at the Microsoft compliance page: https://docs.microsoft.com/en-US/compliance/regulatory/offering-home?view=o365-worldwide.

The production instance of ActiveNav Cloud is hosted in USA, within the Microsoft Azure East US2 region (Virginia). All data is either processed in the hosting region (Virginia, USA) or the customer's premises where collectors are installed. The service is operationally maintained from the UK; UK-based staff do not have access to personal data beyond that provided by the customer as part of the user account management process.

What integrations are required with the customer's environment?

Customers have access to Collector components for different data repository types according to purchased subscription terms.

Collectors require access to each repository using the relevant supported repository API. For example, file share integration uses SMB while SharePoint online uses the SharePoint Graph API. Customers are responsible for configuring and providing the relevant authentication credentials to allow Collectors to access data.

What data is held within the ActiveNav Cloud platform?

ActiveNav Cloud builds a catalog of a customer's unstructured data. To be able to present actionable findings in our visualization of data we record details of the metadata for the cataloged objects – this includes the filename, path, size, and dates associated with each object.

Text based objects are inspected to identify data elements of interest to the customer according to defined feature extraction rules. We store counts of the identified data elements to support our risk scoring model but no values identified within objects are persisted.

If customers utilize our targeted search functionality, matched search values will be persisted in a double encrypted form using a tenant specific encryption key until disposed of by the customer.

How are updates to the platform managed?

Our development processes utilize a continuous deployment model for deployment of platform changes. New or updated features are deployed to the production environment as soon as they have passed through test and review quality gates. As a customer, access to some features may be controlled according to your subscription agreement.

For on-premises Collector installations the availability of updates is flagged within the ActiveNav Cloud user interface, and these must be installed by customer staff.

Do we have the option to not participate in or postpone an upgrade to a new release?

No. As the ActiveNav Cloud platform is a multi-tenant SAAS environment, new functions are made available to all tenants when deployed.

Will we be notified of major changes that could impact our use of the platform?

Yes. While changes that impact security are unexpected, customer contacts are informed via email of any notable changes, in particular any change that requires specific action from customers such as an upgrade of on-premises Collectors.

ACTIVENAV

Identity and Access

How do users authenticate with the service?

The cloud solutions use Microsoft Azure AD B2C for all authentication and authorization, including MFA required by default. Support for SSO is available for customers who use Microsoft Entra ID (formerly known as Azure AD), other SSO integrations will be prioritized according to customer demand. All authentication and authorization requests, including for privileged users, are logged within the Microsoft Azure AD B2C service.

How are user accounts managed?

All user account management is currently handled through the administrative interface of ActiveNav Cloud. A customer tenant is created with an initial administrative user and customers may then add additional users as required. User roles are used to control the level of access assigned to individual users.

What controls are in place to manage ActiveNav's access to the service?

ActiveNav's staff access to the environment is controlled using role-based access. We use a least privilege approach for access to the production system so that only employees that require access are granted access; any required changes or exceptions are handled through a review process. All users and administrators are provided a unique login ID and shared credentials are strictly prohibited.

What controls are available for customers to restrict network access to the service?

Typically, approaches such as IP address whitelisting per customer, would meet this requirement. However, such approaches are impractical for multi-tenant services and are therefore not available. Our roadmap includes provision for a subscription tier which provides dedicated instances subject to customer demand.

Application and Data Security

How does ActiveNav verify that all software development adheres to industry standards?

ActiveNav's Product Delivery Model and the supporting product security engineering practices describe our approach to the software delivery lifecycle and associated engineering standards.

A key component of our secure development practice is the use of security testing services from Veracode. Every ActiveNav Cloud build is subject to security tests using Veracode SAST with additional SAST, SCA and DAST scans scheduled on a weekly basis. Veracode SCA allows us to monitor 3rd party components for vulnerabilities. A manual penetration test is scheduled at least once per year.

ActiveNav Cloud is certified at "Team" level within the "Verified by Veracode" program.

https://www.veracode.com/verified/directory/activenav

Americas
Reston, VA, USA
+1 571 375 2780

EMEA
Winchester, UK
+44 01962 454401

APAC
Melbourne, Australia
+61 3 9982 4543

activenav.com
sales@activenav.com

How is interaction between customer environments and ActiveNav Cloud protected

User interactions with the ActiveNav Cloud user interface, and interactions between Collector processes and the backend ActiveNav Cloud platform are all carried out using encrypted connection using TLS1.2 or greater.

Collector interactions with unstructured data repositories are encrypted if the target repository supports this.

How is document content managed during processing?

It is impossible for Collector processes to carry out Feature Extraction tasks without access to the content of the documents that are discovered. To protect this content from unnecessary exposure, Collector processes are engineered to limit the time that content is available for and to minimize the use of temporary files.

The results shared with the backend ActiveNav Cloud platform after Feature Extraction only include counts of the type of information found. No actual data from within documents is persisted at the Collector host or in the backend platform.

How is data encrypted at rest?

The service uses Microsoft Azure storage with transparent data encryption enabled. Azure SQL Transparent Data Encryption technology is used to protect all data in SQL databases while Microsoft Azure platform functionality ensures that the same level of encryption for backups. All communication between services and data transfer uses TLS 1.2, as provided and maintained by the Microsoft Azure hosting platform.

All key management and the selection of cryptographic standards is handled via the Microsoft Azure platform.

How is customer data logically or physically segmented?

Our cloud services are multi-tenant and logically partitioned and keyed by a unique tenant identifier. Furthermore, to enhance this separation we deploy dedicated per-tenant instances of Azure Key Vault for storage of any customer-supplied credentials or other tenant secrets. Cloud Collectors that are deployed to process cloud-based repositories are dedicated to a specific customer tenant.

How does ActiveNav ensure production data is not replicated in non-production environments?

We do not use or replicate production data in non-production environments. Operational system administrator accounts have the authority to access tenant data with access kept to the minimum required by role base accessed control.

How is data recoverable in the case of a failure or data loss?

The ActiveNav Cloud platform is multi-tenant in nature with disaster recovery implemented for the complete cloud instance. We have robust systems in place, using services provided by the Microsoft Azure hosting platform, to backup and restore all critical customer data in the event of failure or data loss. Recovery of specific tenants in isolation is not supported.

What is your process for performing secure data deletion?

Management of the secure deletion of data and decommissioning of customer-specific storage and compute resources is handled via the Microsoft Azure platform. All customer data held within multi-tenant databases is deleted as part of tenant deletion end of the account subscription lifecycle.

Identity and Access

How does ActiveNav manage security incidents?

Our incident management system is documented and regularly tested as party of our information security management system audited as part of our ISO27001 compliance program. The process is actively managed across all parts of the organization from engineering to operations and facilities and includes triage, escalation, and notification procedures to ensure both appropriate executive oversight and timely customer, and other stakeholder, notification.

How does ActiveNav monitor the service for issues?

Our cloud host infrastructure, using Azure Application Insights, collects network and application logs and includes comprehensive monitoring and alerting capabilities to identify, triage and remediate issues. This data is monitored as a key function of our engineering operations team.

How are hosts, appliances and other infrastructure components scanned for vulnerabilities?

Vulnerability scanning for our cloud host infrastructure is handled by the Microsoft Azure platform which identifies and resolves issues affecting the service.

Additionally, our team uses Microsoft Defender for Cloud and SQL including Advanced Threat Protection to automatically monitor, detect and alert suspicious activities and unusual access patterns. Veracode DAST performs regular automated assessments for OWASP Top 10 and similar threats to the platform. Microsoft Azure provides DDoS protection for API services.

How does ActiveNav ensure the service is regularly patched?

All operating systems and application patches are applied regularly across the service's environment using Microsoft Azure's platform services. Where virtual machines are used ActiveNav ensures automatic updates for underlying operating system patches are enabled.

How is access to security management systems controlled?

Access to all aspects of the service environment is controlled by ActiveNav's AzureAD and Azure RBAC. This ensures that access to audit logs is restricted to authorized personnel. Only limited numbers of staff have access to the detailed security management elements of the Azure hosting environment. Role assignment is regularly reviewed by engineering and security management.