ACTIVENAV

Data Security in ActiveNav Cloud:

An Overview for Prospective Customers

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 to 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.

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 an inevitable data breach, it's 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.

Our Approach to Information Security

Assurance and Compliance

Recognizing that 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 based upon 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. Our Information Security Policy is available at our Trust Center.

Independent external audits are conducted annually by certified ISO27001 auditors while internal auditors follow a planned program overseen by our information security management team. These audits cover all aspects of the business from our engineering and innovation to business operations and service delivery.

Through our Trust Center, we endeavor to provide evidence for assurance purposes through transparent access to key elements of our Information Security Management System. Requests for additional evidence should be made to the relevant account representative, and an amendment to the relevant service purchase terms may be required.

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

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. All vendors we engage with are subject to comprehensive 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 criticality. All vendors are reviewed periodically to ensure continued compliance.

Industry Leading Foundations

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

- Hosted in Microsoft Azure, ActiveNav Cloud's foundations are assured by that service. Microsoft's Azure platform maintains an industry-leading compliance program detailed here: https://docs.microsoft.com/en-US/compliance/regulatory/offering-home?view=o365-worldwide.
- Our high-performance discovery service collects only the minimum necessary data to provide the insights customers need, configured according to customers' use case.
- Any data persisted in the ActiveNav Cloud platform is encrypted at rest by Azure services. Any data in transit from discovery 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. Visit our Trust Center to download our certification.

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.

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. Manual Penetration Tests are performed by Veracode consultants on a periodic basis.

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.

Americas
Reston, VA, USA
+1 571 375 2780

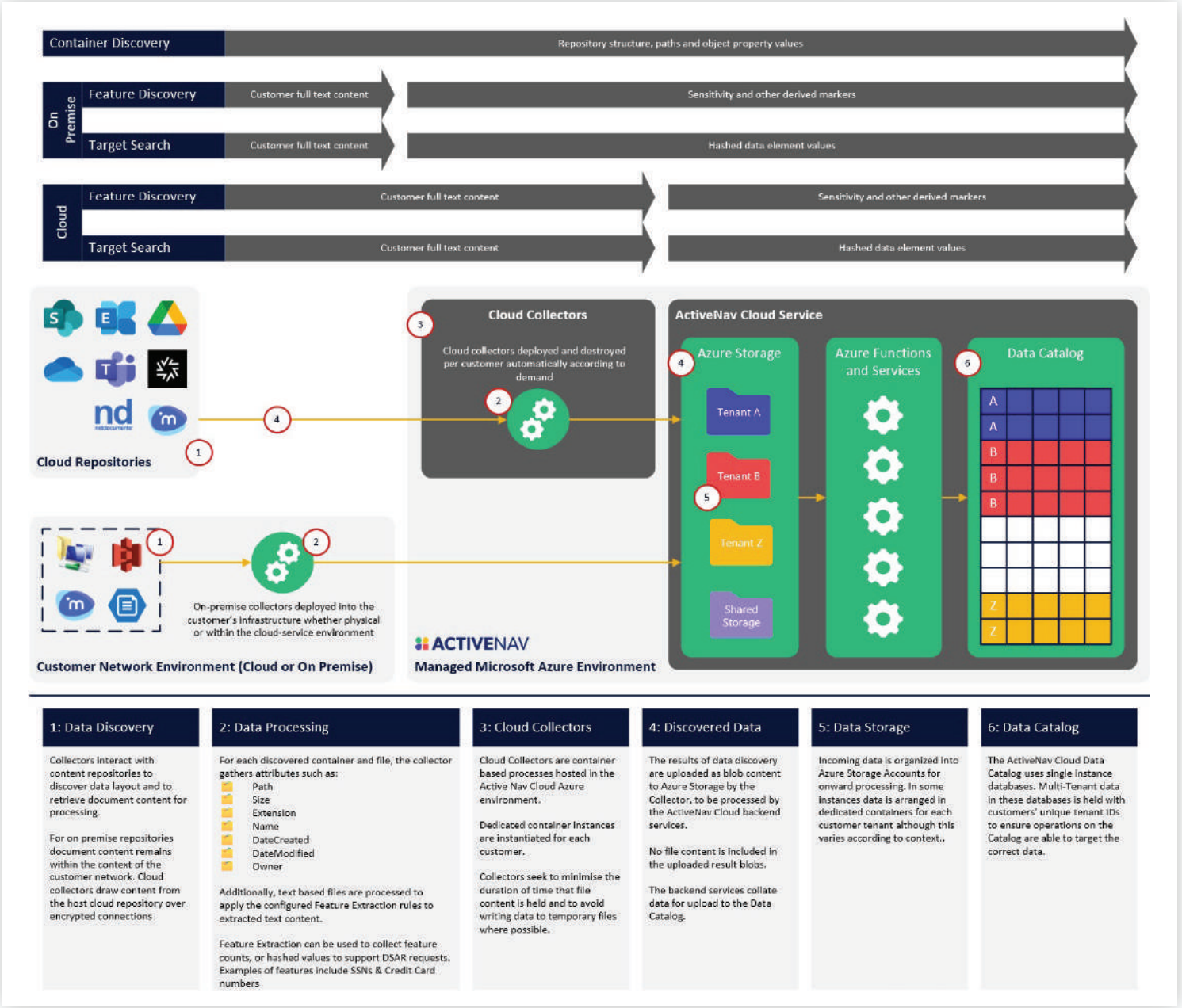
EMEA
Winchester, UK
+44 01962 454401

APAC
Melbourne, Australia
+61 3 9982 4543

activenav.com
sales@activenav.com

Data Flow and Minimal Data Collection

The diagram above provides an overview of our cloud data processing architecture. The diagram is intended to be read from left to right referring to the supporting text which describes the data that is processed in each part of the service.



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 hashed form using a tenant specific salt until disposed of by the customer.

ActiveNav Cloud uses 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.

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

Assessing the ActiveNav Cloud Security Architecture

ActiveNav Cloud is designed for use by governance, compliance and IT teams to provide insights into unstructured data wherever it is stored in the organization. It complements data repositories such as file shares, document management systems or collaboration platforms, capturing and presenting selected, aggregated metrics and metadata rather than file contents themselves. Its security architecture is therefore optimized to protect that component data but is not equivalent to that of the end repositories themselves.

In assessing our security posture, we recommend that vendor assessment teams consider the following key tenets:

- ActiveNav Cloud discovers but does not store the full content of data. Focus therefore on data flow and processing boundaries from the connected data repository.
- The metrics and metadata collected by ActiveNav Cloud is controlled strictly by its configuration. Focus therefore on the way your organization populates that metadata in order to understand its risk profile.
- ActiveNav Cloud is not intended for end user use, providing visualizations for governance, compliance and IT teams. Focus therefore on ensuring alignment between the privileged access already granted to these teams and the intended use of the service.

The remainder of this paper, supported by other content in our Trust Center, is intended to provide the information needed to facilitate that assessment. Our Trust Center provides the following documentation:

- This document, providing an introduction and overview of our security posture.
- Our Data Processing Addendum describing terms for data security and privacy.
- Our Information Security Policy, describing our approach and commitment to information security.
- A completed Cloud Security Alliance Consensus Assessments Initiative Questionnaire documenting our security controls.
- A copy of our ISO27001 certification.

We maintain a comprehensive security package providing additional evidence to support vendor assessment. That documentation can be obtained from the relevant sales or account representative

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