

A GUIDE FOR ENTERPRISES

The Cloud Native Playbook

Strategies for CIOs, Enterprise Architects,
and Cloud Architects



INTRODUCTION

The following is a guide to working in cloud native environments for enterprise architects (EAs), cloud architects (CAs), and CIOs. These three disciplines are integral to overseeing cloud native operations, and with this eBook, LeanIX presents scalable recommendations on how to align decentralized architectures to evolving business capabilities. Key to this document is a tool where technological standards can be collaboratively developed and enforced alongside real-time, integrated data from leading cloud vendors—the likes of which is available in the LeanIX Cloud Native Suite.

What is Cloud Native?	3
Cloud Native for CIOs	6
Cloud Native for Enterprise Architects	9
Cloud Native for Cloud Architects	11
The Market for Cloud Native Governance Tools	13
Introduction to LeanIX Cloud Intelligence	14
A Nine-Step Walkthrough of LeanIX Cloud Intelligence	16
Conclusion	30

What is Cloud Native?

A cloud native business is one which has progressed beyond using cloud computing only in terms of storage and convenience. These companies take advantage of the capacity gained from cloud providers to test new services at faster speeds while constructing them according to individual components that can be configured and improved upon independent of the whole. A staple of agile organizations, applications built in (or “native” to) the cloud offer faster time-to-market and opportunities to innovate against disruptive technologies.

Common elements of cloud native technologies include:

Containers

Portable file systems holding everything to run applications for easier movement across computing environments.

Service meshes

Infrastructure layers added to applications to ensure service-to-service communication is balanced and optimally routed.

Microservices

A form of software development where applications are comprised of modular and single-functioning services with their own supporting code base.

Immutable infrastructure

An architectural model where servers are made replaceable to accommodate iterative software development cycles and unique configurations.

Declarative APIs

Comparatively more accessible APIs based upon declarative programming to help business stakeholders integrate services with systems throughout operational domains.

Benefits of cloud native architectures include:



Improved flexibility



Agile methodology



Continuous iteration



Operating efficiency



Scalable services

Cloud native demands yet another reimagining of how IT and business must work together. Though elements of application portfolio management can be leveraged to support its aims, CIOs and cloud and enterprise architecture teams need increasingly automated methods to anchor decentralized teams and applications to enterprise objectives. In particular, the ease by which cloud components can be deployed (roughly 30 seconds using major vendors) and amassed (up to thousands of microservices, virtual machines (VMs) and interfaces for large-scale organizations) is conducive to a form of IT complexity unlike that in IT landscapes composed primarily of on-premises technology. Failing to efficiently map these granular IT assets to corresponding projects, processes, stakeholders, performance data and business capabilities will prevent CIOs and EAs from seeing the true state of their IT environments and thus make them an unreliable partner in the pursuit of competitive advantages.

The potential for cloud native rests on whether an organization can sustain disorienting rates

of procurement and technological risk without delaying a process of continuous innovation and development. This is true regardless of whether enterprises select a single-cloud, multi-cloud or hybrid-cloud approach to cloud native; same, too, if transformations are application-driven or infrastructure-led. A unifying authority is needed to develop the technical expertise and strategic vision to brace organizations for cloud native initiatives in the following ways:

- **Access to enterprise-wide data**
- **Cloud security protocols**
- **Targeted outcomes set to business value**
- **Rationalized applications and services**
- **Performance and resource monitoring**
- **Operational alignment**

Each of the above contributes to an enhanced form of interoperability that's key for bridging cloud native gaps and establishing information pathways between remote teams. But to enact these changes means the key champions of its IT model—CIOs and EAs and CAs—must accept distinct yet complementary paths to working together.

“Cloud native sits top of mind for everyone—but its success rests on the backs of very few.”

André Christ, LeanIX CEO

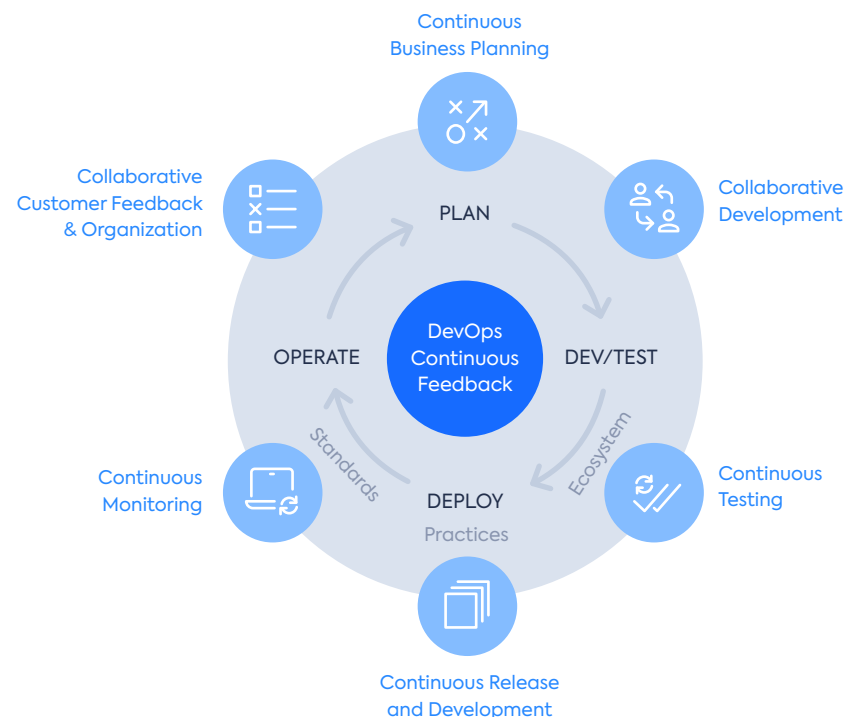
Cloud Native for CIOs

How cloud native has changed the role of CIOs—and how it hasn't at all

CIOs are still responsible for guaranteeing the basics in a cloud native world. Business alignment, IT complexity management, collaborative cultures: the cornerstones of traditional and agile enterprises alike haven't been displaced by the advent of microservices and serverless computing. If anything, the rise of fragmentized applications has exposed a knowledge gap among senior management from across all business units on how to incorporate cloud-based and cloud-run services into the long-term strategies of their respective corporate realms—a divide putting CIOs on the hook for continuous technical guidance and data-driven assurances.

CIOs owe these colleagues a sober inspection of cloud native technologies to determine whether they can realistically be sustained by their organization. But while this is true of any technological trend, the process of continuous integration and deployment necessitates an increased tolerance for failure and experimentation and thus new forms of risk management and compliance. “Fail fast” and “fix fast”, the twin tenets of building containerized applications, must be ground to a cohesive, enterprise-wide set of compliance protocols that take into account automated workflows, an application portfolio spanning multiple environments and infrastructure layers, and a need for frequent policy

exceptions to accommodate innovative yet un-tested designs. Security guidelines can't be based on generic templates, and in order to prepare and sign off on risk and compliance guidelines that reflect the ambitions of a business, CIOs require end-to-end visibility into the as-is states of IT environments to drive feasibility assessments.



As well as crafting proportionate yet fluid security models, CIOs are a final authority on the best practices that govern decentralized workflows. Much of this involves ensuring that DevOps—the processes and standards used by developers and IT operations to carry out rapid software delivery—is embedded to organizational structures. This can be accomplished by mandating items such as shareable databases, cross-functional teams comprised of varied specialists, or the use of particular metrics-based monitoring tools. In all cases, however, a cloud native business depends on the top-down authority of CIOs to standardize IT environments and promote ongoing exchanges between development and IT operations teams.

What CIOs can do for cloud native

It comes down to managing expectations. No company wants to be left behind in the rush for digital supremacy, and while the prevailing adage that “all companies will become software companies” rings true, CIOs are obliged to not only find ways to maximize the efficiency of IT teams and networks but also rationalize how to do so every step of the way. A DevOps environment is useless if the accompanying business is neither invested in the long-term demands of continuous software delivery nor if an IT model is misaligned to the customer experience.

The surest way for CIOs to create relevant cloud native services is to organize and make room for constant feedback from targeted customer groups. More opportunities exist than ever before to gauge consumer interests and market

trends—and consequently, more disadvantages in not doing so as often as possible using automated methods. Yet tantamount to gathering metrics on consumer interests via consistent beta and A/B testing is putting in place a central repository to store information once it's returned.

Every contributor to the DevOps iterative development process needs constant access to usage and performance data to keep innovation cycles moving. If application development is impeded due to a lack of information, CIOs need to equip their teams with the means to provide early alerts and collated insights on how to re-structure data flows. On occasion, these problems will require fundamental changes to applications underlying key organizational services—a challenge increasing the likelihood of business interruption. Only CIOs can expedite approval processes by demonstrating, in data-driven ways, the value of re-configuring essential products and creating timelines on how to do so.

How CIOs can help EAs manage cloud native

EAs rely on the support of extensive stakeholders to collectively build and maintain IT portfolios in large-scale organizations. Using an EA management tool as a common platform, EAs drive holistic assessments of applications using information collected throughout IT and business departments. A secure and dynamic way to evaluate cloud native readiness, a co-operative approach to IT management is driven equally through overarching corporate initiatives as it is an EA management tool's functionality.

CIOs must actively encourage senior technical leaders to share knowledge and give EAs what's needed to accelerate cloud migrations. Though it's up to EAs themselves to create roadmaps on integrating and optimizing infrastructure, the scale of digital transformation required to enable cloud native business models will inevitably be blocked by contractual limitations with software providers that can only be solved by executive order. CIOs can streamline passages to new cloud platforms by making such operational complexities transparent while also leveraging the same information collected by EAs to decide the futures of legacy systems

How CIOs can help CAs manage cloud native

Ranging from developing cloud native strategies to coordinating adoption to promoting cultural change, almost every aspect of managing cloud native is within the remit of cloud architects. These tasks naturally intersect with the concerns of CIOs and are contingent on the access they receive to assorted project teams and business units. Based on how quickly legal, financial and application data from these sources are made available to cloud architects will determine the speeds by which they can lead technological transitions.

CIOs must work side-by-side with cloud architects on developing and enforcing enterprise-specific standards related to cloud computing costs and violations (especially before deploying automated solutions). Clear instructions on monitoring open ports, replacing deprecated services, and setting cloud spend thresholds are just a few examples of items requiring top-down alignment.



Cloud Native for Enterprise Architects

How cloud native has changed the role of enterprise architects—and how it hasn't at all

When firing on all cylinders, a cloud native business is always evolving—a vehicle constantly being outfitted with better parts while moving without delay to new destinations. But no matter how quickly new services and platforms are acquired, a balance between technological capacity and organizational ambition must be upheld. It's the role of EA to secure this equilibrium in cloud native environments while simultaneously defining the optimal balance itself.

Iterative software development, customer-centricity, and the many other fundamentals of cloud native models aren't existential threats to the discipline of EA. As with past advancements in IT, the familiar challenges of EA—application sprawl, technology obsolescence, IT complexity—must still be overcome to create unobstructed pathways for the performance of these technical feats. What's changed, however, is the equal focus EAs now give to designing and governing cloud native architectures to benefit semi-autonomous teams dedicated to individual services as much as complete business units themselves.

This optimization can only be accomplished with granular perspectives on decentralized applications—a pre-requisite incapable of being met without information sent directly from major hyperscalers. EAs rely on up-to-date data on the manifold varieties of cloud components and deployment policies to perform cloud native security and rationalization, and no matter how mature an EA program or extensive its network of contributors, these details can't be gathered without automated assistance.

Why EAs are necessary for cloud native

Intermediaries between application owners and senior leadership, EAs are essential to distilling corporate visions throughout all corners of an enterprise's IT network. The modernization roadmaps they collectively build alongside their stakeholders are strong indicators of a company's future success—and based on the authority they're extended, clues as to their likelihood of sustaining it. Yet as cloud native organizations transition to new skillsets and methods of delivering value, EA programs must be the very first to exemplify new working styles or else risk being chased back into the ivory tower.

Cloud native is less about technology gatekeeping than producing repeatable and measurable outcomes, a shift pushing EAs to co-create *and* co-execute on business targets. With more applications and performance metrics in unfamiliar locations than ever before, operational details are bound to get lost by those at both ends of the application development spectrum unless EAs take a hands-on approach to validating processes and services and technologies. EA management tools have kept pace with maintaining visibility into cloud native landscapes, but it is up to EAs themselves to combine their technical and business acumen with multi-cloud governance solutions to minimize communication errors between operations and developers. Sometimes this means leading conceptual designs of new technologies; other times, perhaps, by helping finance departments make sense of scalable billing.

This versatility has always been intrinsic to EA but is especially useful for essential strategies of cloud native operations: cross-functional governance (strategic, finance, operational); culture-building (DevOps, employee roles and accountability, skills training); and change management (platform set-up, cloud-readiness assessments, setting organizational targets).

How EAs can help CIOs manage cloud native

Timely, relevant, and organized data. If seeking stakeholder buy-in on intangible future states, a CIO's vision is only as strong as the number of fears they can eliminate. To help, EAs can use collaborative IT portfolios as more than just an efficient means of gathering application data but as a way to portray, in data-driven and interactive elements, the diverse priorities of

top-level management. By segmenting cloud native technologies alongside business capabilities, attaching roles and associated responsibilities to cloud migration timelines, and putting clear thresholds and measurements for controlling cloud risks, EAs can take advantage of enterprise-wide and customizable application inventories to give complete shape to an IT department's cloud native readiness.

How EAs can help CAs manage cloud native

Every organization needs a CA but not every company is ready for one. Without the bridges EAs create between IT and business, a CA can't concentrate on what they do best and architect scalable cloud services. By helping CIOs, developers, and finance teams dismantle contractual or technical roadblocks to the cloud, EAs safeguard the growth of cloud native offerings and give room to the many principles required for its continuing expansion. An overlap between these two disciplines emerges as an organization's cloud native maturity increases, but until that point in time, EAs should incorporate their needs to their own and co-operatively put together the right personnel, data, and standards in accessible patterns.

Cloud Native for Cloud Architects

How cloud native has changed the role of cloud architects—and how it hasn't at all

Even disciplines as young as CA have been re-defined by the demands of cloud native business models. As representatives of an enterprise's cloud initiative—a role with responsibilities extending from cloud-based adoption to cloud-based strategizing—the tasks performed by CAs directly improve a business's ability to leverage cloud services for new gains. These individuals define as well as enforce standards on cloud hosting and performance, and by ensuring that cloud services and their myriad of constituent parts are transparent for each invested business unit to analyze, serve as messengers on the commercial, technical, and legal issues affecting those at every level of IT and operations.

Similar to EA but more specialized in the feasibility of cloud-based services, CAs help development teams maximize cloud-based applications to solve individual business use cases and align with enterprise-specific policies and procedures. Of note, CAs are relied upon to monitor the business value of cloud native applications in comparison to its overall costs (or “cloud spend”). Their analysis on how to optimize costs by team, region, staging/production environment, or according to IaaS or PaaS components is used to guide corporate investments and shape the balance of multi-cloud strategies. CAs rely on tool-based platforms with built-in integrations to hyperscalers

for creating such segmented reviews of global cloud expenditure and cloud security protocols. These tools offer functionality for contextualizing the business purposes of cloud components, allocating roles and responsibilities for cloud maintenance, and promoting cross-departmental exchanges on the shared use of technologies. This reporting is performed at speeds that lend themselves to operating cloud environments of scale.

Why cloud architects are necessary for cloud native

Like it or not, the benefits of multi-cloud (a single network with numerous cloud computing services) and hybrid cloud (a mix of on-premises, private cloud and public cloud services) outweigh the upfront complexities they bring to cloud native IT operations. The same is true with edge computing and serverless containerization and just about every other current trend in the world of cloud native. But as history has shown that competitive businesses never forsake innovation at the risk of taking on new forms of complexity, there's clear value in employing disciplines such as CA with formalized methods of tracking high rates of data dispersion and resource consumption.

Put simply, too much is at stake to employ what Gartner refers to as “ad hoc” approaches to cloud development and adoption. Though many cloud vendors offer applications for helping enterprises accomplish specific

aspects of cloud native governance, any truly pro-active approach to cloud native implementation must be anchored by those with enough competency to re-align broken processes themselves or communicate internally to others how to do so. It's the basics of leadership—to show first by example—and its value can't be undersold when pivoting to an unfamiliar business model.

How CAs can help CIOs

CAs drive the visibility to rationalize cloud spend and help CIOs and finance teams procure discounted options from cloud providers—a top priority according to Flexera's 2019 “State of the Cloud” report. Yet as cloud native organizations expand, the drivers of wasted cloud spend are guaranteed to cover additional cloud services from more business units and regions. CAs have to sustain this transparency despite the size of cloud native operations to help CIOs uncover further value levers.

How CAs can help EAs

EA has always struggled to demonstrate value to those it governs. The rise of cloud native technologies—a seismic change in how IT landscapes are balanced and conceptualized—has made matters even more difficult. To help EAs share winning business insights from concepts like automation strategies, CAs need to promote accessibility when rearchitecting business-critical software for cloud.



The Market for Cloud Native Governance Tools

The volume of data in cloud native environments has made automated solutions for sourcing and contextualizing IT assets a necessity. In addition to stand-alone offerings from leading hyperscalers, the market is saturated with tools for carrying out singular aspects of cloud management (security, finance, diagramming, SaaS/PaaS management, etc.). These offerings vary dramatically in applicability to businesses of particular sizes and industries. In particular, a gap exists in solutions for nurturing collaboration between EA and CA teams and their network of common stakeholders.



Introduction to LeanIX Cloud Intelligence

Developed in tandem with LeanIX's industry-leading customers, LeanIX Cloud Intelligence (powered by Cloudockit and part of the larger LeanIX Cloud Native Suite) offers out-of-the-box functionality to generate visibility into cloud native environments. LeanIX Cloud Intelligence is structured upon the following data model to store data imported via integrations with major cloud vendors.

C

Cloud Component

Any service that can be provisioned from a cloud vendor (virtual machines, a storage bucket, an API gateway, a machine learning service, etc.).

T

TBM Category

Groupings based on the definitions and best practices of the Technology Business Management (TBM) framework.

C

Component Type

Categories of vendor-specific functionality (GCPBucket for GCP storage, DynamoDB for AWS databases, MicrosoftVault for Azure security, etc.).

R

Region

The physical locations where cloud components are hosted.

O

Organizational Unit

Technical ownership of the cloud component (multi-level and vendor-specific).

S

Software

The functional business purpose of cloud components.

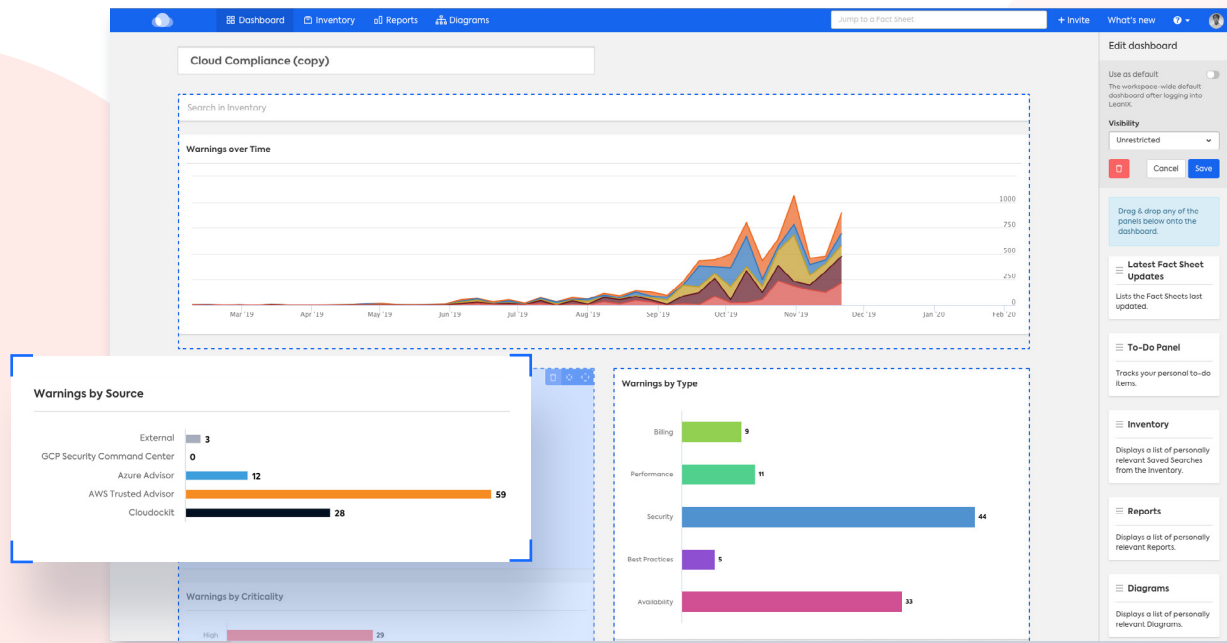
V

Violations

Comprises the security, availability, performance, and other warnings of cloud components.



A Nine-Step Walkthrough of LeanIX Cloud Intelligence

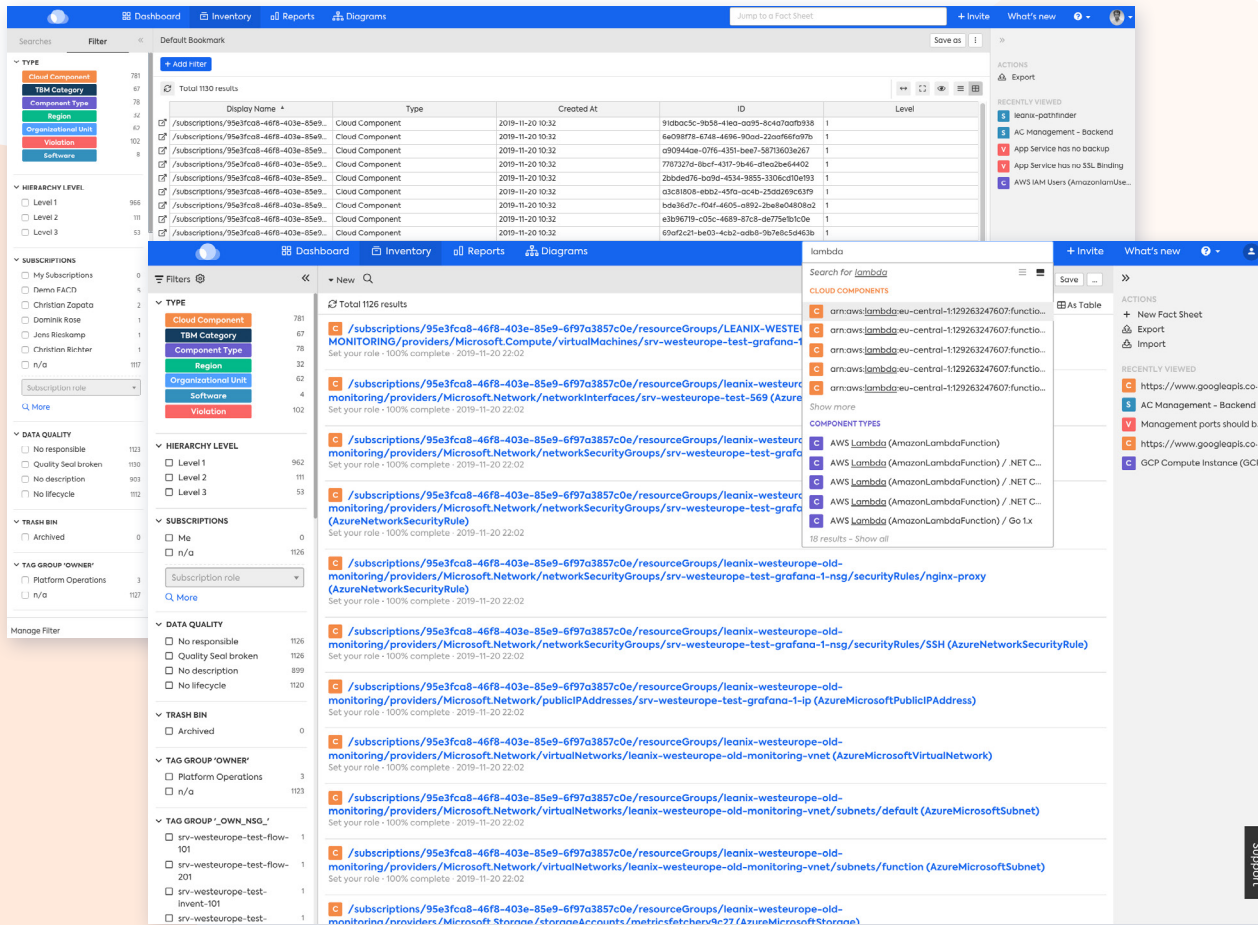
**STEP 1****Automated data importing and customizable workspaces**

LeanIX Cloud Intelligence offers IT and business leaders a shareable repository of real-time data on cloud components. This information is sourced and categorized directly from major cloud providers (currently AWS, Azure and GCP) through automated integrations. For daily planning, users can organize their LeanIX Cloud Intelligence main page with customizable dashboards for quick views on cloud costs, compliance protocols, cloud components, and security risks.

- To-do panels
- Dashboard restrictions (Unrestricted, Write Restricted, Read & Write Restricted)
- Subscriptions (all Fact Sheets the user is subscribed to)
- Metric charts (based on Provisioning State and/or Costs)
- Report panels
- Saved searches and recommended searches
- Latest updates

LeanIX Smart Xplore™

Cloud Intelligence's user interface is powered by LeanIX Smart Xplore™ technology, a set of functionalities proven to help enterprise architects and CIOs navigate and segment their IT portfolios. LeanIX Smart Xplore enables faster transitioning between LeanIX Cloud Intelligence's core areas—Dashboard to Inventory to Reports to Diagrams—to accelerate information-gathering.



The screenshot displays the LeanIX Cloud Intelligence interface. The top navigation bar includes 'Dashboard', 'Inventory', 'Reports', and 'Diagrams'. A search bar is present with the text 'Jump to a Fact Sheet'. The main content area is divided into several sections:

- Filters:** Includes 'TYPE' (Cloud Component, TBM Category, Component Type, Region, Validation), 'HIERARCHY LEVEL' (Level 1, Level 2, Level 3), 'SUBSCRIPTIONS' (My Subscriptions, Domain FQDN, Christian Zepato, Dominik Rose, Jens Rickamp, Christian Richter, n/a), 'DATA QUALITY' (No responsible, Quality Seal broken, No description, No lifecycle), 'TRASH BIN' (Archived), and 'TAG GROUP 'OWNER'' (Platform Operations, n/a).
- Table:** A table with columns 'Display Name', 'Type', 'Created At', 'ID', and 'Level'. It lists various cloud components like 'Cloud Component' and 'Cloud Component' with their respective IDs and levels.
- Search Results:** A panel on the right showing search results for 'lambda'. It lists several AWS Lambda functions with their ARNs and names, such as 'arn:aws:lambda:eu-central-1:129263247607:funcio...' and 'arn:aws:lambda:eu-central-1:129263247607:funcio...'.

STEP 2

Scalable storage and integrated information

No matter how broad your IT portfolio, LeanIX Cloud Intelligence is purpose-built to store dynamic volumes of data on every type of cloud native asset. This information is stored within individual scorecards (“Fact Sheets”) containing fields that reflect the key properties of an IT entity. Fact Sheets form the basis of the LeanIX Cloud Intelligence reporting network and can be filtered according to common architectural attributes (i.e., data quality, ownership, hierarchy) plus user-made ‘tag’ groups. Of note, users can pivot from their general inventory to a customized analytics report based on whatever information is filtered for during a search query.

- Inventories can be viewed and edited as a table
- Assets differentiated according to data quality
- Inventories segmented according to levels of business hierarchy
- Subscription-based user grouping

Personalized and Predefined Searches

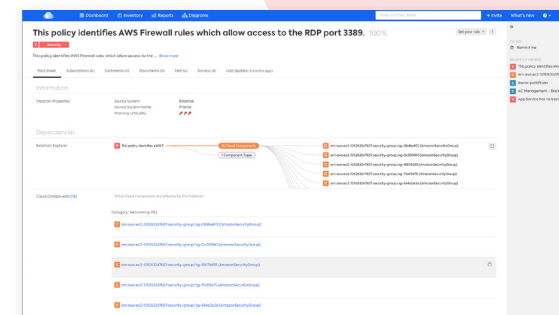
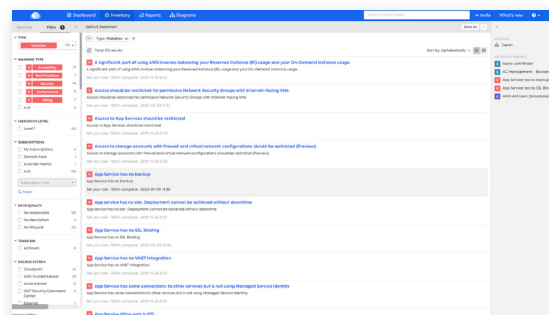
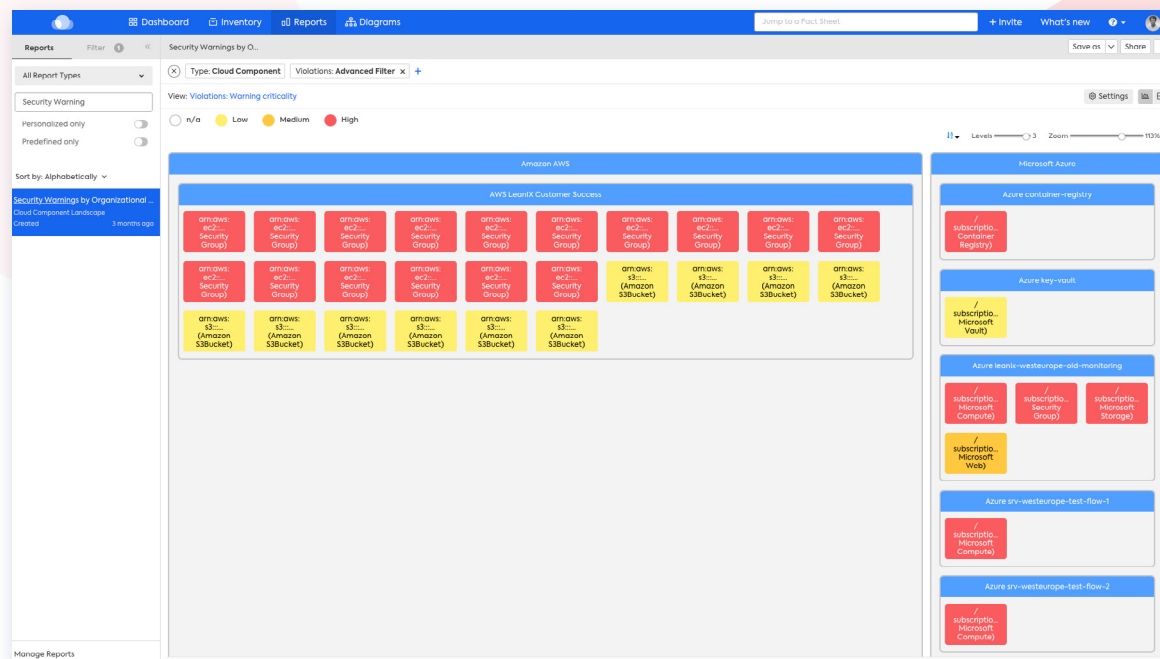
Searches can be saved and used to create both personalized and predefined views of inventories.

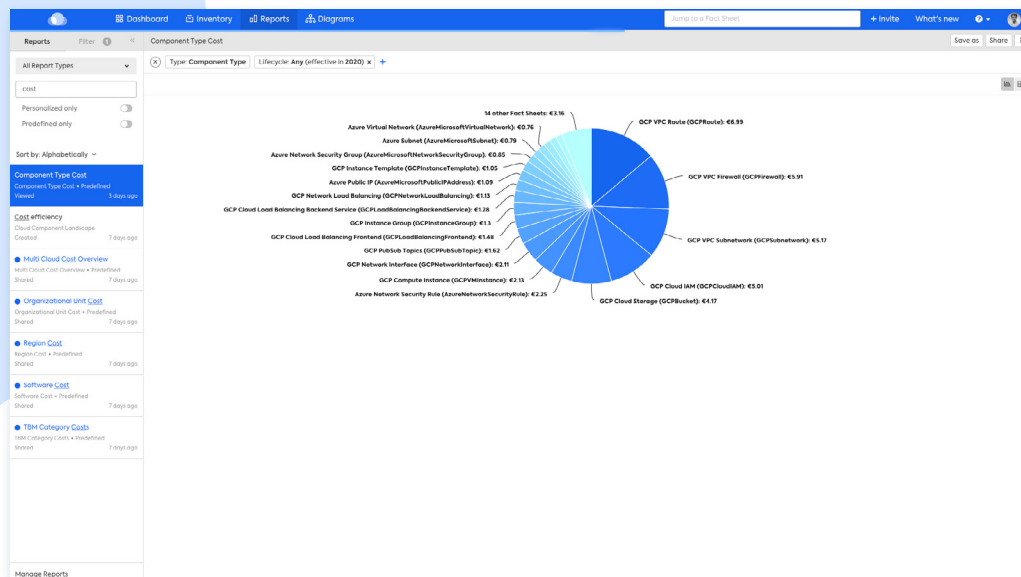
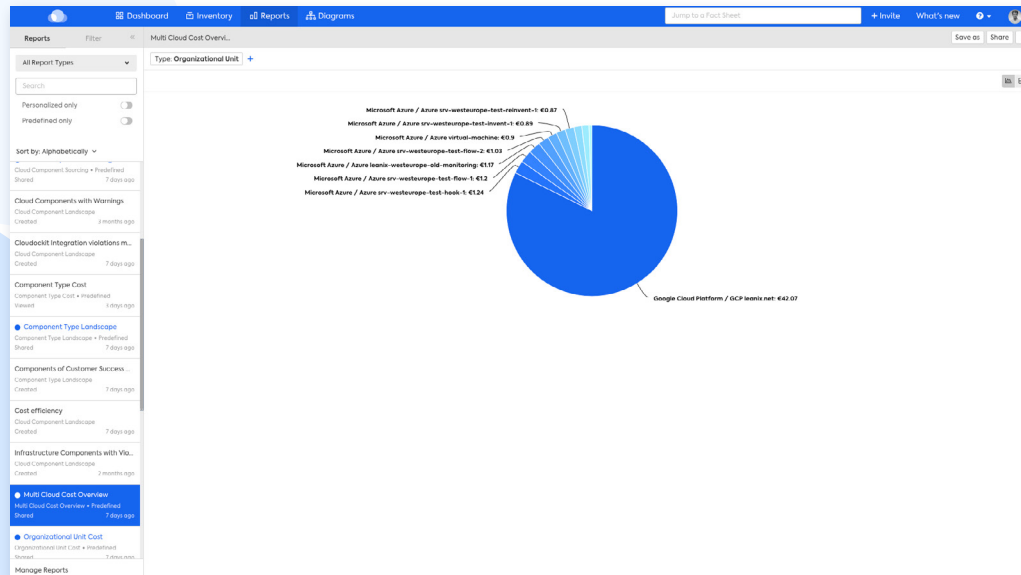
STEP 3

Contextualized security and compliance warnings

Alerts on common cloud violations (availability, best practices, security, performance and billing) are imported directly into LeanIX Cloud Intelligence from vendor-specific monitoring tools (AWS Trusted Advisor, Azure Advisor, GCP Security) and contextualized to region, ownership, service, and business capabilities. When filtered by cloud components and cloud component types, this automation facilitates efficient reviews of workspace security policies no matter what enterprise-specific risk tolerance is in place.

- Evaluate system or internal security reviews
- Measure warnings via levels of criticality (low, medium, high)
- Quickly determine responsibility
- Accommodate policy exceptions with tags to mark violations by “Development” and “Production” environments



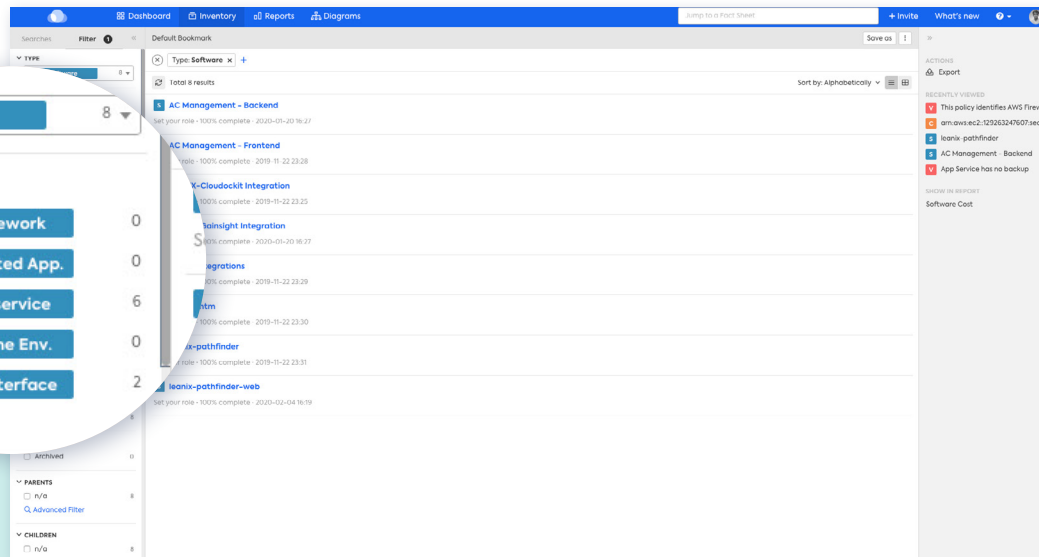


STEP 4

Dedicated analytics on cloud spend

The costs of cloud native initiatives can be rationalized using numerous categories of out-of-the-box LeanIX Cloud Intelligence reports. Monthly or real-time cost statements on total cloud spend across multi-cloud environments, regions and organizational units can be measured alongside business capabilities and service lifecycles. All information arrives directly from hyperscalers and is guaranteed for accuracy. Of note, users are capable of managing costs related to IaaS and PaaS components to holistically assess resource consumption.

- Identify cost optimization hotspots
- Isolate cloud costs by provider to balance multi-cloud strategies
- Make sure vendor costs are proportionate to business value
- Link costs with best practice TBM categories



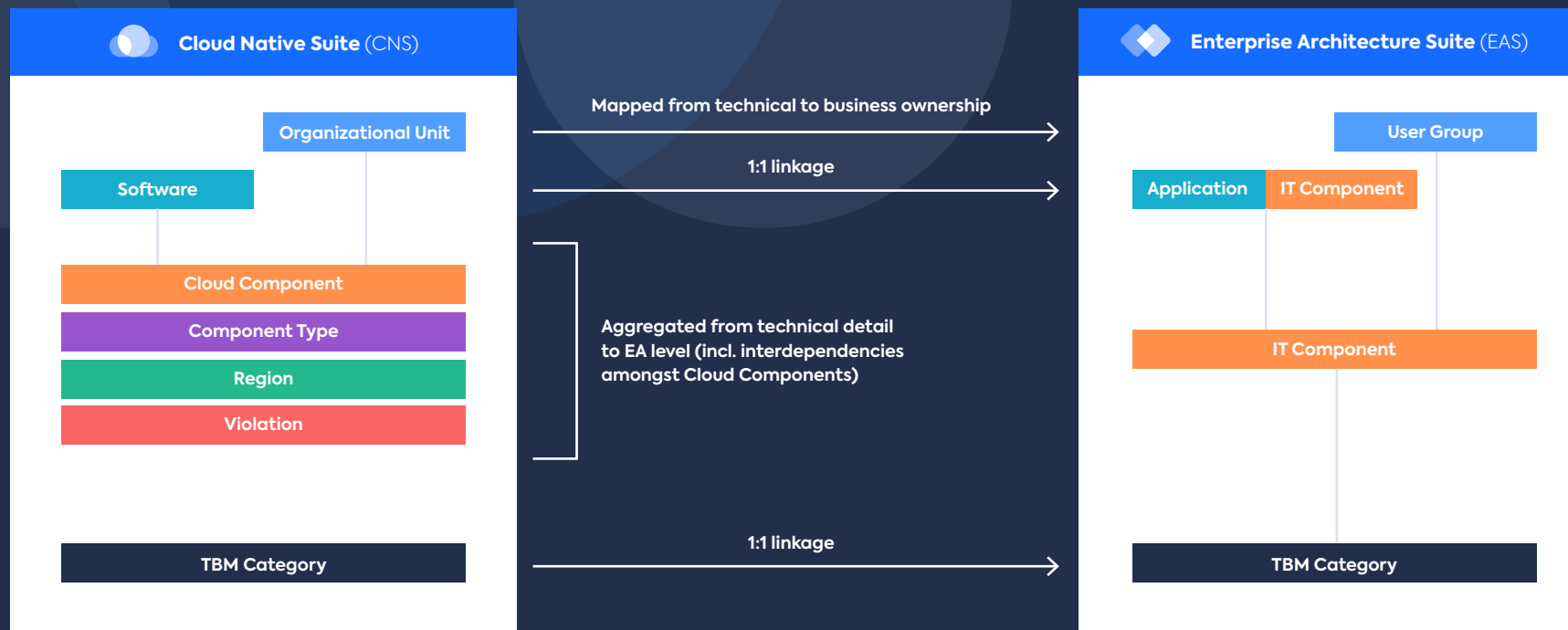
STEP 5

AWS tags, Azure tags and GCP labels are auto-discovered and directly linked to their business context

Tags and labels used to classify cloud metadata in software deployments are recognized by LeanIX Cloud Intelligence. These marked cloud resources are instantly discovered by the tool and then sorted to their respective business capabilities.

- Filter inventory by tag and label group
- Categories include Framework, Integrated Application, Microservice, Runtime Environment, and User Interface
- Run detailed reports on cloud software billing

Technical details on cloud components held in LeanIX Cloud Intelligence can be aggregated and then viewed from within the LeanIX Enterprise Architecture Suite (EAS). The integration offers complementary analysis of cloud native landscapes via reports and terminology relevant to users of both products.

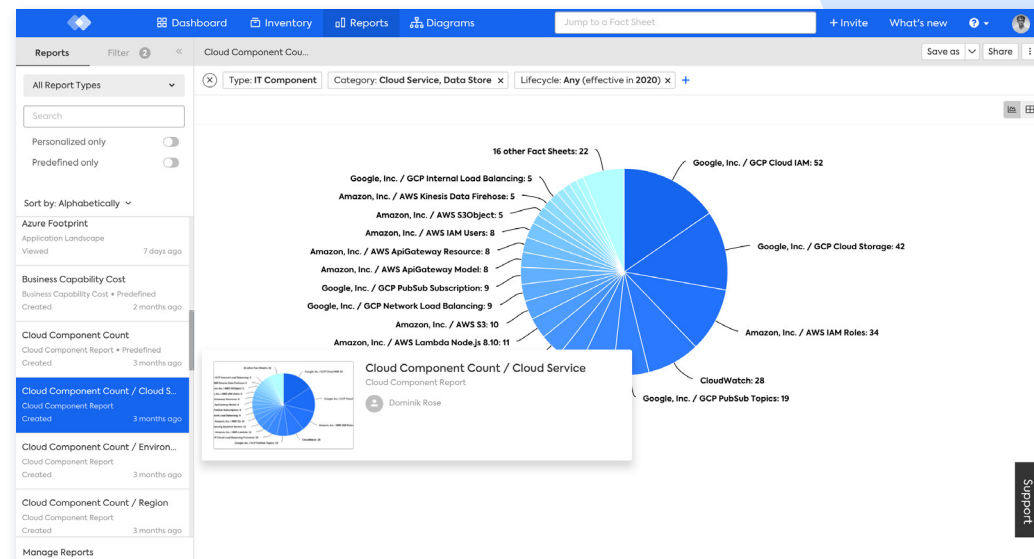
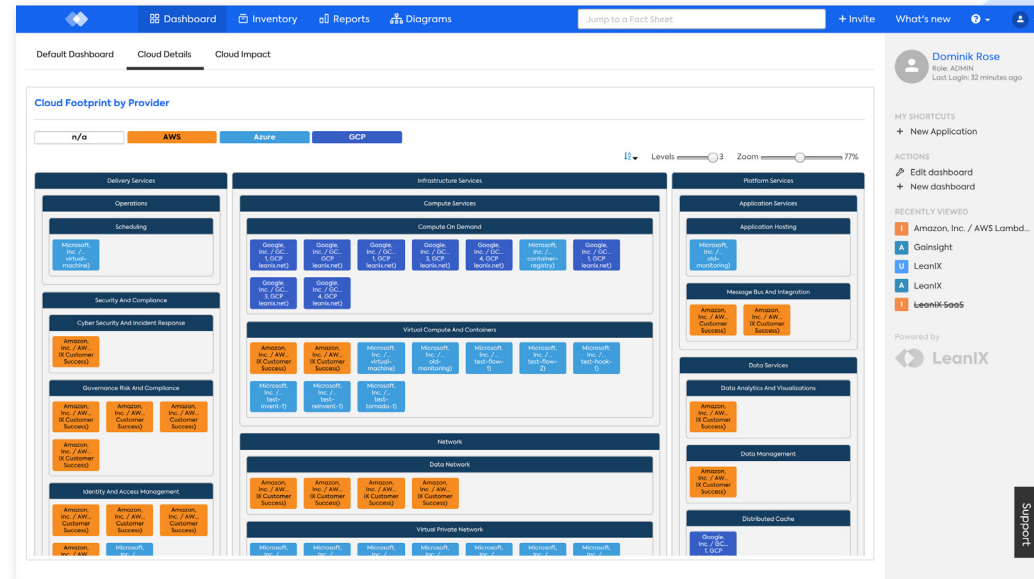


STEP 6

Cloud components are synchronously linked to services in LeanIX Enterprise Architecture Suite

A view into all cloud services and associated cloud strategies, or a “Cloud Footprint”, is auto-imported from LeanIX Cloud Intelligence into the EA workspace. Footprints from AWS, Azure and GCP arrive pre-detailed to TBM framework categories. Of note, cloud components from every provider can be seen alongside their associated business capabilities.

- Sort applications by IaaS, on-premise, PaaS, or SaaS
- Inspect trends in cloud component volume
- Clear measurements of total cloud spend
- See the business criticality of cloud components
- Assess IT portfolios via the functional and technical fit of cloud components



Reports

Filter

Security Violations by Account

Type: Cloud Component

View: Violations: Warning criticality

Enable Editing

Settings

Expand

Collapse

All Report Types

violation

Personalized only

Predefined only

Sort by: Alphabetically

Cloudcikt integration violations mo...

Cloud Component Landscape

Created

7 days ago

Infrastructure Components with Viol...

Cloud Component Landscape

Created

7 months ago

Security Violations by Account

Cloud Component Matrix

Created

7 days ago

Violations by Org Unit

Cloud Component Landscape

Created

3 months ago

Violations by region

Cloud Component Landscape

Created

3 months ago

Violations from Cloudcikt Rules Eng...

Cloud Component Matrix

Created

7 days ago

Manage Reports

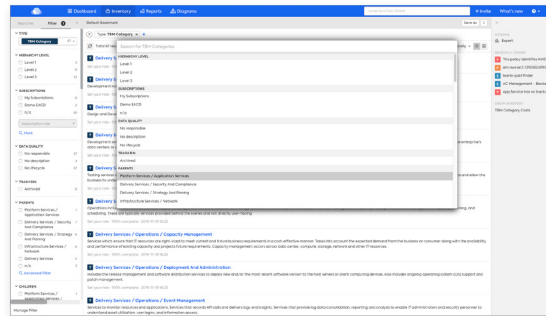
Amazon AWS	AWS IAM Customer Access	Access should be restricted for permissive Network Security Groups with Internet-facing VPCs	Access to App Services should be restricted	Access to storage accounts with firewall and virtual network configurations should be restricted (Preview)	App Service has no SSL Binding	Checks buckets in Amazon Simple Storage Service (Amazon S3) that have open access permissions or allow access to any unauthenticated AWS user	Checks security groups for rules that allow unrestricted access to a resource	Ensures EC2 instances are using an IAM role instead of hard-coded AWS credentials	Ensures EC2 associated IAM roles are not password-protected	
						arn:aws:x3:gainsight-in...				
						arn:aws:x3:gainsight-in...				
						arn:aws:x3:gainsight-in...				
						arn:aws:x3:leanix-gains...				
	Microsoft Azure	Azure container-registry							/subscriptions/7b6eccc2-b...	
		Azure key-vault						/subscriptions/7856ecc2-b...		
		Azure iot-hub-west-europe-sub-monitoring	/subscriptions/95e3fca8-4...	/subscriptions/95e3fca8-4...	/subscriptions/95e3fca8-4...	/subscriptions/95e3fca8-4...				
		Azure iot-hub-west-europe-test-flow-1	/subscriptions/95e3fca8-4...							
		Azure iot-hub-west-europe-test-flow-2	/subscriptions/95e3fca8-4...							
Azure iot-hub-west-europe-test-hook-1		/subscriptions/95e3fca8-4...								
Azure iot-hub-west-europe-test-invent-1		/subscriptions/95e3fca8-4...								
Azure iot-hub-west-europe-test-invent-2		/subscriptions/95e3fca8-4...								
Azure iot-hub-west-europe-test-invent-3		/subscriptions/95e3fca8-4...								
Azure iot-hub-west-europe-test-invent-4		/subscriptions/95e3fca8-4...							/subscriptions/...	

STEP 7

Application filters extend to evaluate cloud hosting risks via IT components

The reliability of cloud-based applications can be gauged based on the lifecycles and violations of services in use from a provider. Version updates and phase-outs (current and approaching) from vendors are shown in color-coded detail. The level of impact a license expiration has on the overall IT landscape is prominently displayed.

- Applications filterable by primary deployment type (IaaS, PaaS, SaaS, on-premise)
- Cloud risks mapped to business capabilities
- Cloud violations impacting performance, availability, security and best practices are aggregated
- Additional sorting by functional and technical fit



Shareable reports

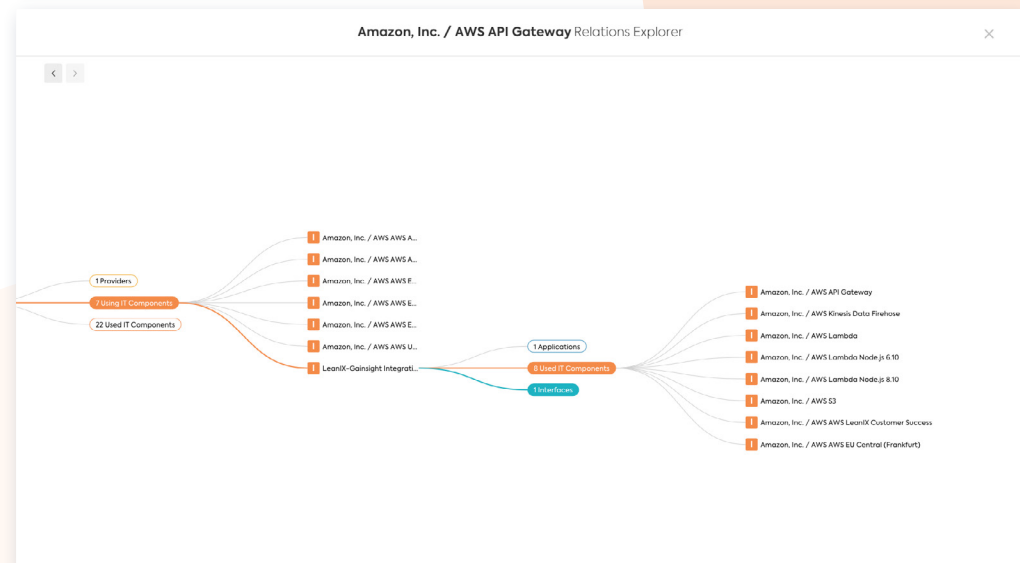
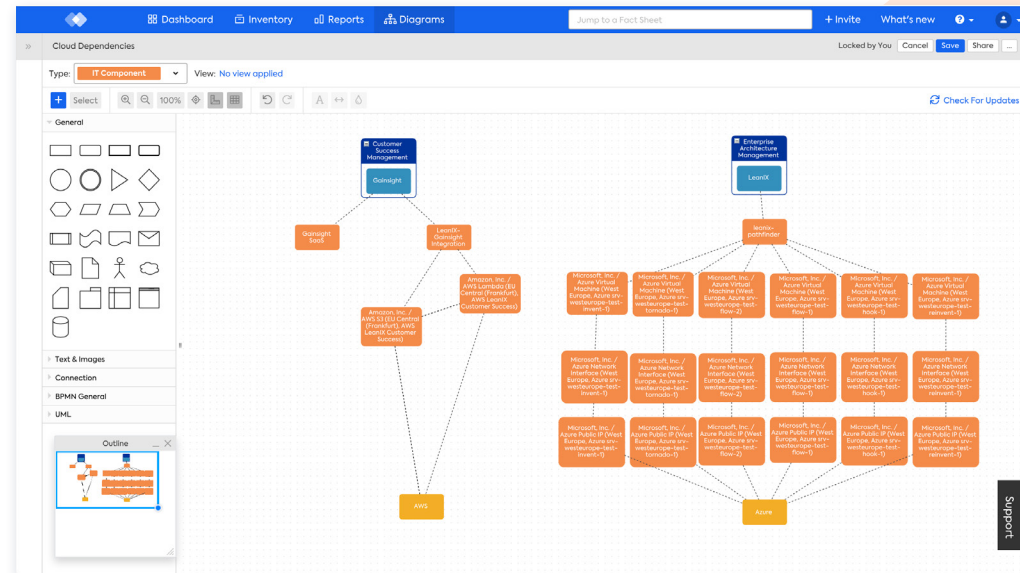
LeanIX reports can be annotated, saved, and then shared to fellow users. All user-made documents appear at the top of personalized lists.

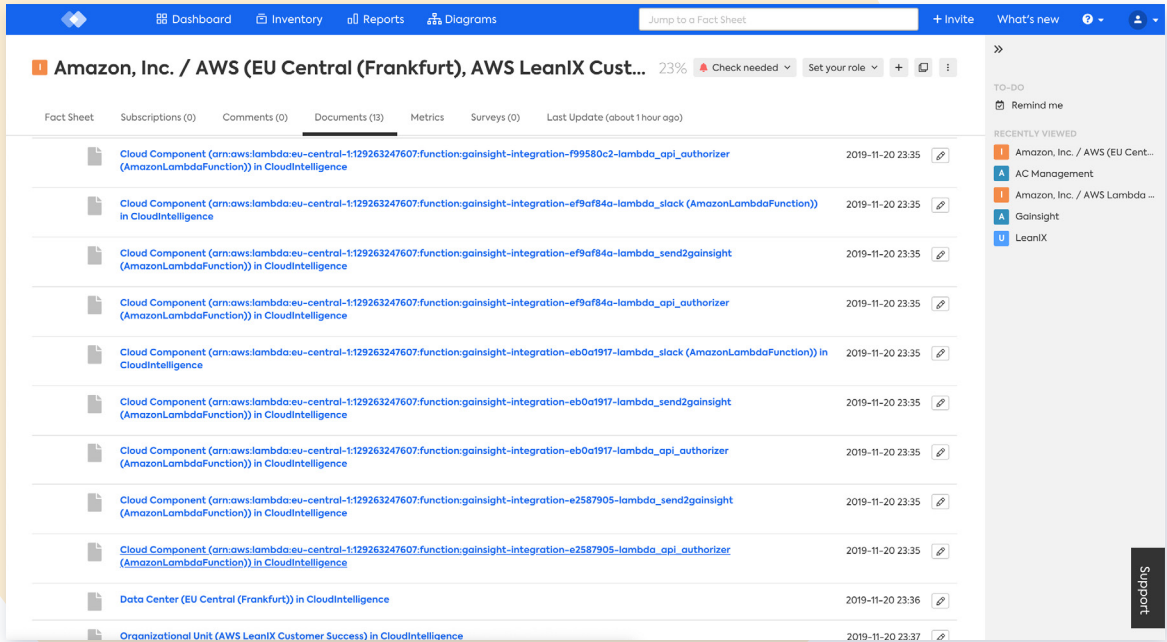
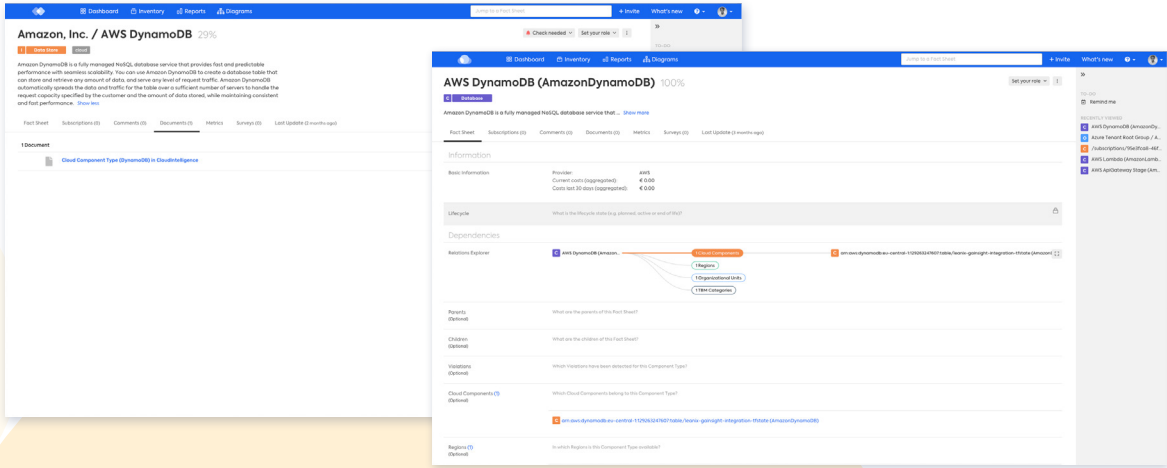
STEP 8

Interactive mapping of technical dependencies between cloud-based applications

Labelled as IT components, networks of interdependent cloud services can be picked apart to reduce technical overlap and optimize configurations. Relations can be seen from within a series of customizable reports and further detailed using combinations of pre-configured views.

- Vulnerability and data flow analysis
- Instant contextualization (e.g., business capabilities, processes, TBM framework, providers, etc.)
- Incorporate cloud spend (current and historic) into total cost of ownership





STEP 9

Alternate freely between LeanIX Enterprise Architecture Suite and LeanIX Cloud Intelligence for layered analysis cloud components

Attached to every cloud service fact sheet in LeanIX EAS are links to the corresponding information in LeanIX Cloud Intelligence. Here users can switch between the two LeanIX suites for preferential views on IT components.

CONCLUSION

The challenges of operating cloud native environments—lack of IT visibility, cost management, increased security and compliance vulnerabilities—represent a clear and present need for tools that deliver data-driven certainty.

LeanIX Cloud Intelligence and the wider Cloud Native and Enterprise Architecture Suite are designed to help large-scale enterprises sustain accelerated rates of innovation. Backed by a team of dedicated implementation agents and on-call support technicians, LeanIX customers are never stranded on their cloud native journey.

If there's anything in this eBook that you'd like to discuss in detail, please reach out at info@leanix.net

If you're ready
for the next step
in your cloud native
transformation,
contact us for a
free trial of LeanIX
Cloud Intelligence.

FREE DEMO

This document is current at the time of its initial publication.
LeanIX GmbH reserves the right to alter it at any time.
THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED
AS IS, WITH NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLICIT.

2020v1.0

LeanIX offers a Software-as-a-Service (SaaS) application for driving Enterprise Architecture and Cloud Governance, enabling companies to accelerate their IT transformation. From on-premises to cloud native and microservices, architecture teams using LeanIX have the power to strategically support their business and take decisions faster. More than 250 global brands including Volkswagen, Adidas, Bosch, DHL, Santander, Atlassian, and Zalando rely on LeanIX to improve transparency, visibility, and drive real-time efficiencies. LeanIX addresses IT's critical need to ensure high-quality, real-time data is accessible to stakeholders whenever needed. Use cases include Cloud Governance, Application Portfolio Management, and Technology Risk Management. LeanIX was founded in 2012 by Jörg Beyer and André Christ. The company is headquartered in Bonn, Germany, with U.S. headquarters in Boston, Massachusetts.

Copyright© LeanIX GmbH. All rights reserved. LeanIX and the LeanIX logo are trademarks or registered trademarks of LeanIX GmbH in Germany and/or other countries. All other products or services are trademarks of their respective companies