



The content described herein is intended to outline our general product direction for informational purposes only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions.

The development, release, and timing of any features or functionality described herein remain at the sole discretion of Atlassian and is subject to change.



Enterprise-grade cloud

How Atlassian is enabling secure collaboration



ETHAN HARRY – ASHWINI RATTIHALLI – BEN MAGRO

Cloud means best-in-breed,

but is it secure?



Server/data center



Customer



Atlassian



Cloud

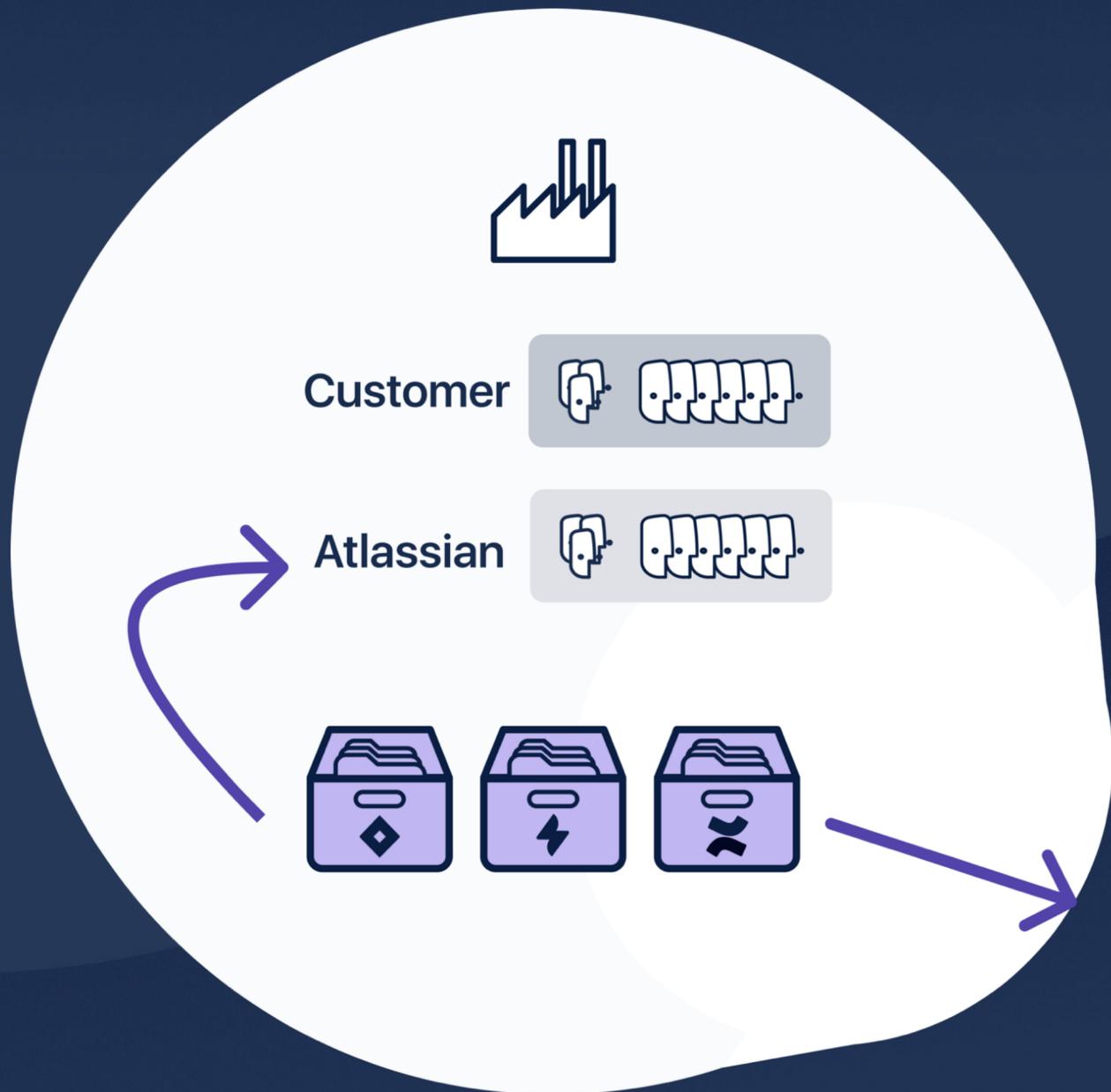


Customer



Atlassian





Data handling concerns



Data access and sharing



Partnership with Atlassian

Agenda



Shared responsibility

Cloud customers partner with Atlassian to secure data



Atlassian controls

Security and compliance provided by Atlassian



Customer controls

Levers provided to customers to protect access and data

SOLUTIONS

Agile &
DevOps

IT Service
Management

Work
Management

New
Solutions

EXPERIENCES



Collaboration



Automation



Analytics



Administration



EXTENSIBILITY

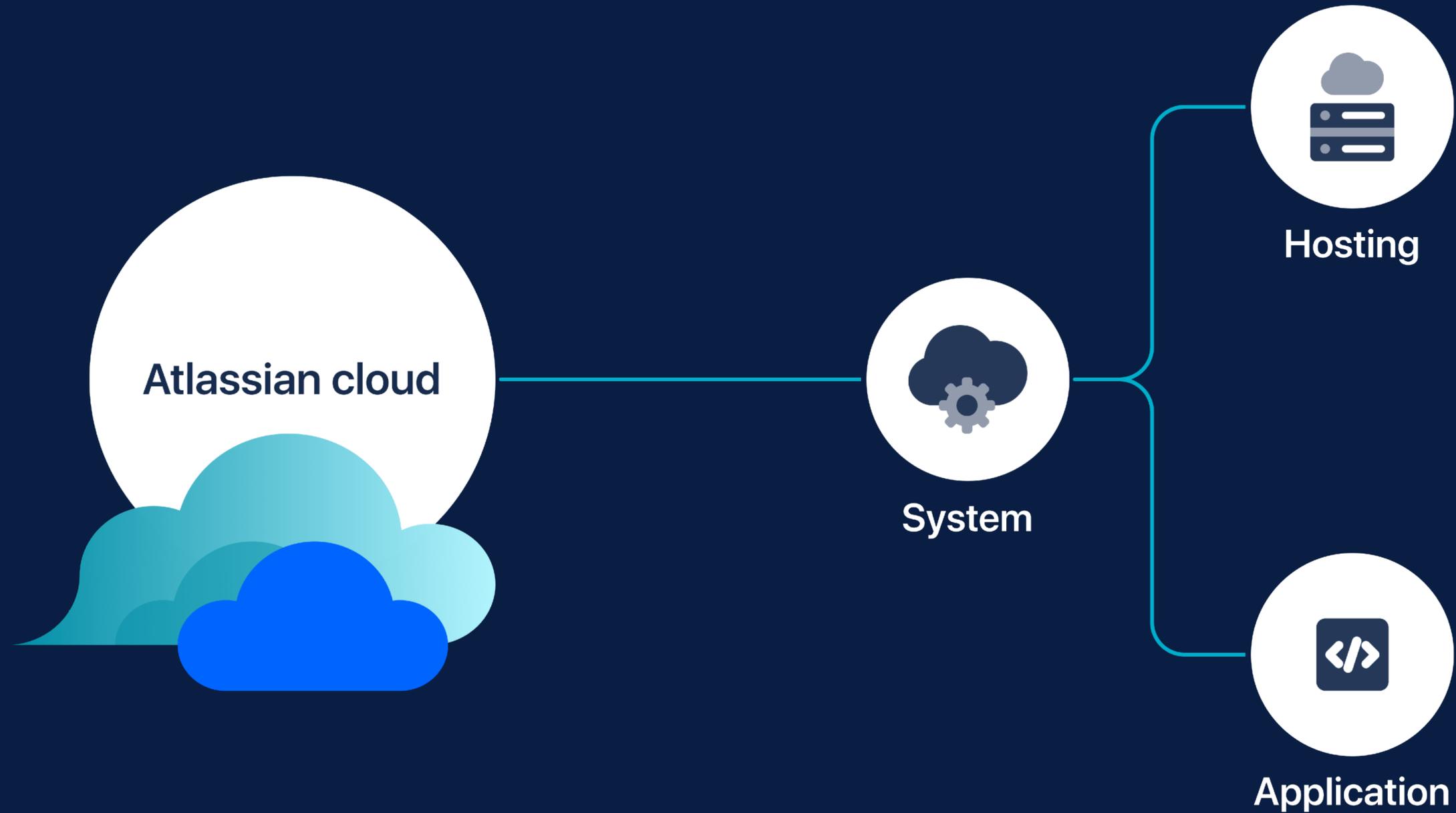


DATA MANAGEMENT



INFRASTRUCTURE

 INFRASTRUCTURE





DATA MANAGEMENT



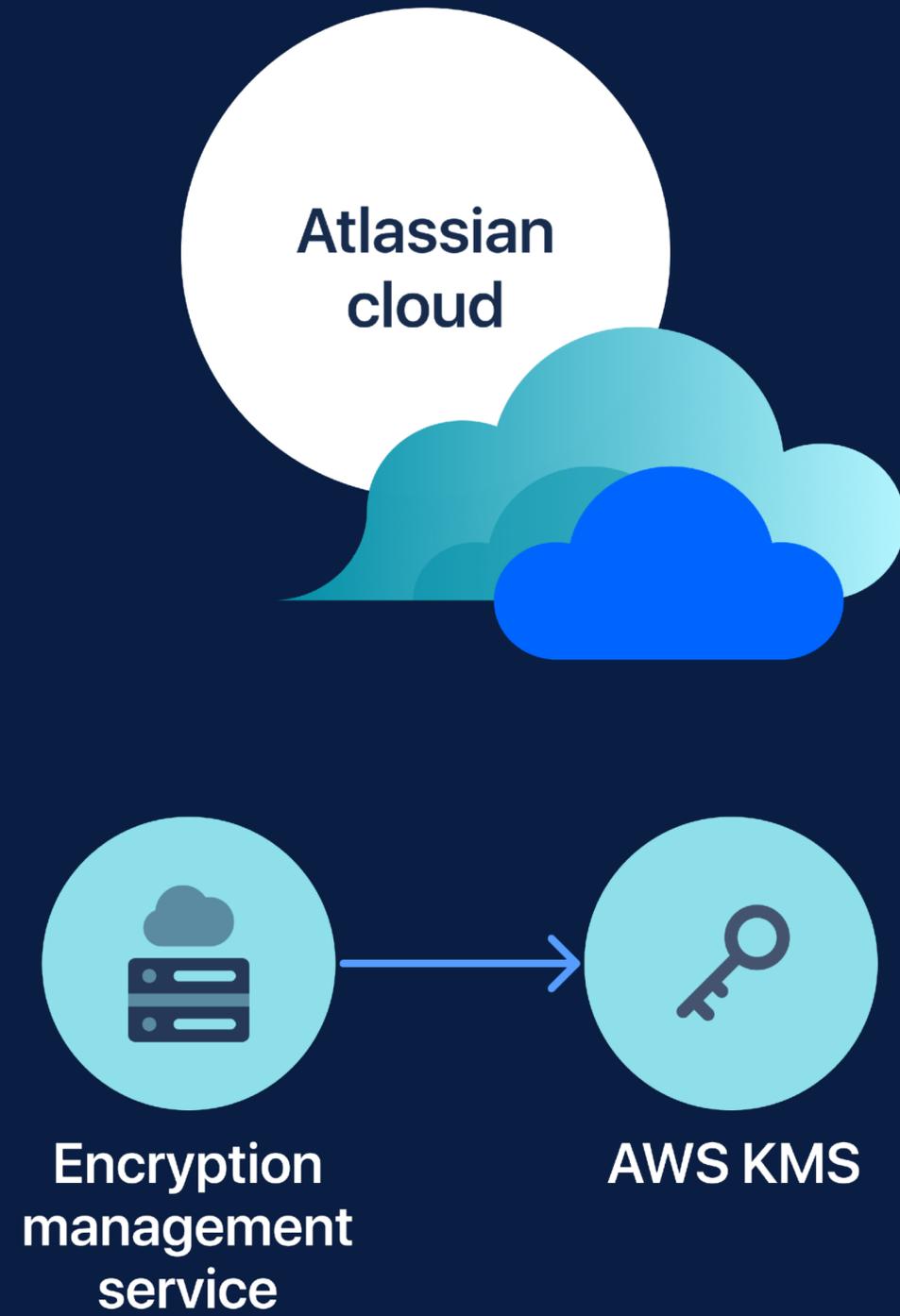


DATA MANAGEMENT

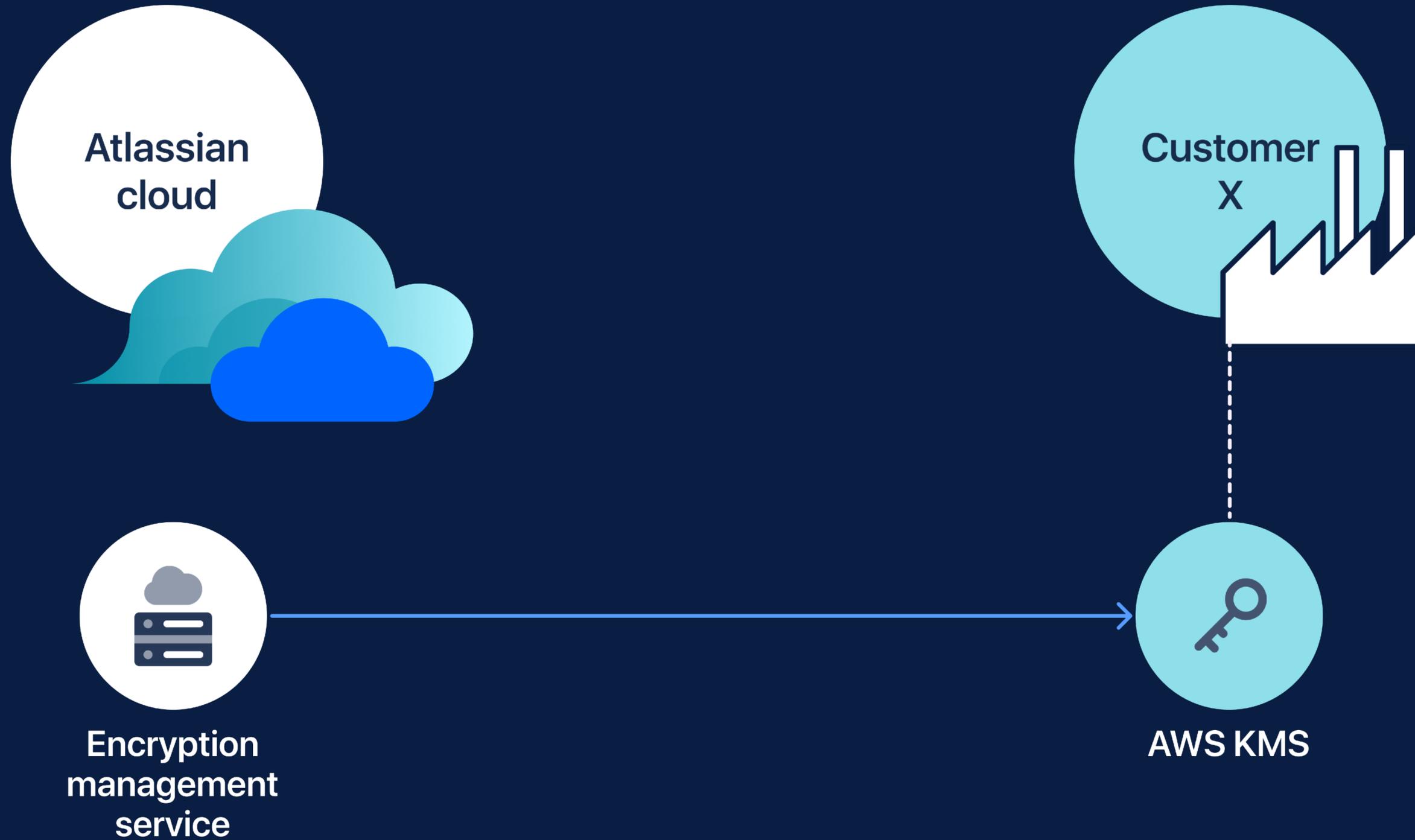




BYOK



BYOK



Agenda



Shared responsibility

Cloud customers partner with Atlassian to secure data



Atlassian controls

Security and Compliance provided by Atlassian



Customer controls

Levers provided to customers to protect access and data

Organization



 **ATLASSIAN** Access

Organization



 **ATLASSIAN** Enterprise

AUTHENTICATION PROTECTIONS

Securing user access

Authentication protections



Authentication policies

Allows organization to configure SSO, 2SV, and idle session durations



IP allowlisting

Allows organization to control which networks have access to your content



External user security

Allows organizations the ability to ensure non-managed users have gone through a second factors authentication

GOVERNANCE PROTECTIONS

Implement your governance standards

Audit logs

Track user actions across your suite of Atlassian products

The screenshot shows the Atlassian Administration interface for 'Vortex + Vogue'. The 'Security' tab is active, displaying the 'Audit log' page. The page includes a navigation sidebar on the left with categories like 'USER SECURITY', 'DATA PROTECTION', and 'MONITORING'. The main content area features a breadcrumb 'Admin / Vortex + Vogue', an 'Audit log' title, and an 'Export log' button. Below this is an introductory paragraph and a search filter section with a search input, 'Date' dropdown, 'Activities' dropdown, 'Apply' button, and 'Reset' button. A table titled 'Showing 30 activities' displays a list of audit events with columns for Date, Location, Actor, and Activity.

Admin / Vortex + Vogue

Audit log

Your organization's audit log tracks activities that occurred from your organization and across your sites within the past 180 days. For product-specific activity, visit the product's audit log. [Learn more about your organization's audit log](#)

To save activities before they pass 180 days, regularly export the log or use the organization REST API to store activities to another location. [Learn more about the organization REST API](#)

Search by name, group, Date Activities Apply Reset

Showing 30 activities ↕

Date	Location	Actor	Activity
Mar 24, 2023 09:00 GMT+11	San Francisco 4.16.192.66	Melody Qiao mqiao@atlassian.com	Granted Product Admin role to mqiao@atlassian.com for Trello
Mar 24, 2023 07:17 GMT+11	San Francisco 4.16.192.66	Melody Qiao mqiao@atlassian.com	Exported managed accounts
Mar 24, 2023 04:36 GMT+11	San Francisco 4.16.192.66	Melody Qiao mqiao@atlassian.com	Exported user list for organization
Mar 23, 2023 10:23 GMT+11	Sydney 123.103.201.174	Anthony Stonehouse astonehouse@atlassian.com	Added prichardson@atlassian.com to administrators group
Mar 23, 2023 10:22 GMT+11	Sydney 123.103.201.174	Anthony Stonehouse astonehouse@atlassian.com	Invited prichardson@atlassian.com to organization https://rhejthaseuoguhastd.jira-dev.com
Mar 23, 2023 09:56 GMT+11	San Francisco 4.16.192.66	Melody Qiao mqiao@atlassian.com	Invited mqiao+03@melqrules.usersinbuckets.com to organization
Mar 23, 2023 09:41 GMT+11	San Francisco 4.16.192.66	mel q1 mqiao@melqrules.usersinbuckets.com	Logged in to account successfully
Mar 23, 2023 09:26 GMT+11	Unavailable	Atlassian Internal System Atlassian Internal System	Changed mqiao+01@melqrules.usersinbuckets.com 's authentication policy to Applies to all users
Mar 23, 2023 09:25 GMT+11	Unavailable	Atlassian Internal System Atlassian Internal System	Claimed account mqiao+01@melqrules.usersinbuckets.com for domain melqrules.usersinbuckets.com
Mar 23, 2023 09:14 GMT+11	Unavailable	Melody Qiao mqiao@atlassian.com	Granted Trello access to mqiao+02@melqrules.usersinbuckets.com
Mar 23, 2023 08:55 GMT+11	San Francisco 4.16.192.66	mel q1 mqiao@melqrules.usersinbuckets.com	Logged in to account successfully
Mar 23, 2023 08:53 GMT+11	San Francisco 4.16.192.66	Melody Qiao mqiao@atlassian.com	Granted Product Admin role to mqiao@melqrules.usersinbuckets.com for Trello

Beacon

Track user actions across your suite of Atlassian products

The screenshot shows the Beacon dashboard for Acme Company. The main section is titled "Alerts" and features a donut chart for "Alerts by status" showing 58 total alerts: 42 Open, 12 Acknowledged, and 4 Closed. To the right, a bar chart shows "Data protection alerts" for Jira and Confluence across categories: Crawling, Exports, and Suspicious searches. Further right, a line chart shows "Average minutes per alert" over time, with a value of 27. Below these charts is a search bar and filters for "From date", "To date", "Alert type", and "Actor". At the bottom, a table lists recent alerts.

Time	Alert	Actor	Product
Dec 14, 2022 12:15 PM	Unusual page views activity	Grace Harris	ADMIN
Dec 14, 2022 12:15 PM	Suspicious search terms in Confluence	Grace Harris	ADMIN
Dec 14, 2022 12:15 PM	An admin logged in as another user	Omar Darboe	ADMIN
Dec 14, 2022 12:15 PM	Application tunnel created	Jie Yan Song	ADMIN

DATA PROTECTIONS

Add controls to your most sensitive content

Data protections

Allows admins to create policies that add controls to groups of content

The screenshot displays the Atlassian Admin interface for 'Acme Inc.' with the 'Security' tab selected. The main content area is titled 'Data security policies' and includes a 'Create policy' button. Below the title, there is a search bar and a list of four policies: 'Finance department policy' (ACTIVE), 'IT and support' (ACTIVE), 'People and culture' (ACTIVE), and 'Test policy' (INACTIVE). The interface also shows a sidebar with navigation options and a footer with pagination and results per page information.

Policy name	Status
Finance department policy	ACTIVE
IT and support	ACTIVE
People and culture	ACTIVE
Test policy	INACTIVE

Data protections

Creating a policy

The screenshot displays the Atlassian Admin interface for configuring a data security policy. The browser address bar shows the URL `https://admin.atlassian.com/data-security-policies/policy/MA-policy`. The navigation menu includes 'Administration', 'Acme Inc.', 'Overview', 'Directory', 'Products', 'Security', 'Billing', and 'Settings'. The left sidebar lists various security and data protection options, with 'Data security policies' highlighted as a new feature. The main content area shows the 'Finance dept policy' configuration page, which is currently inactive. The policy description is 'Restricting app access and protecting sensitive financial data'. It was created by Amar Sundaram just now. The 'Policy coverage' section is currently empty, with a prompt to select data. The 'Policy rules' section includes options for 'App access', 'Data export', 'Public links (Confluence only)', and 'Anonymous access', each with a brief description and a right-pointing arrow for further configuration.

Administration
https://admin.atlassian.com/data-security-policies/policy/MA-policy

ATLASSIAN Admin Acme Inc. | Overview Directory Products Security Billing Settings

Security guide

USER SECURITY

Authentication policies

External user policies

Identity providers

DATA PROTECTION

Data security policies **NEW**

Data residency

Encryption

MONITORING

Audit log

Discovered products

Insights

[Back to Data security policies](#)

Finance dept policy

Restricting app access and protecting sensitive financial data

Activate policy

Created by: Amar Sundaram (Just now) | Policy status: **INACTIVE**

Policy coverage

Select data to define the policy coverage.

Selected data >
The data you select will define the policy coverage

Policy rules

Manage rules to protect the data covered by this policy. [Learn more about data security policy rules](#)

MARKETPLACE APPS

App access >
Control how apps access data

DATA SHARING

Data export >
Block data exports from products like Jira and Confluence

Public links (Confluence only) >
Disable page links that can be viewed by the public

Anonymous access >
Restrict unlicensed users from accessing data

Data protections

Set the coverage

Administration

https://admin.atlassian.com/data-security-policies/policy/MA-policy

Select method **Select data** Review data

Select data to cover

Select the data you want to cover with this policy. You can cover up to 30 items in one policy.

PRODUCTS 20

Search Product ▼

- alpha-inc.com/wiki** Confluence ✓ 3
- alpha-inc-developers.com/wiki Confluence
- alpha-inc-public.com/wiki Confluence
- alpha-inc-restricted.com/wiki Confluence
- alpha-inc.com Jira Software
- alpha-inc.com Jira Service Management
- beta-inc.com/wiki Confluence
- delta-inc.com/wiki** Confluence ✓ 2
- delta-inc.com** Jira Service Management ✓ 1
- kappa-inc.com/wiki Confluence

Select spaces

If you can't find a space, it may have been moved or deleted.

Search by name

Showing 500 spaces

<input type="checkbox"/>	Space name	Space key
<input checked="" type="checkbox"/>	Alpha M&A	AMA
<input type="checkbox"/>	Alpha Operations	ACMEops
<input type="checkbox"/>	Alpha People & Culture	APC
<input type="checkbox"/>	Admin Space	ADMINsp
<input type="checkbox"/>	Advisory Services Engineering	ADVSE
<input type="checkbox"/>	Advocacy Design Requests	ADR
<input type="checkbox"/>	Amars Test Space	AMAR
<input type="checkbox"/>	Analytics	ANALYT
<input type="checkbox"/>	Analytics Data Flows	ANADAF
<input type="checkbox"/>	Analytics Test	ANALYT2
<input type="checkbox"/>	APAC Events Space	APACevent

6 items selected

Back Next

Data protections

Choose a control

The screenshot displays the Atlassian Admin interface for configuring a data security policy. The browser address bar shows the URL `https://admin.atlassian.com/data-security-policies/policy/MA-policy`. The navigation menu includes 'Overview', 'Directory', 'Products', 'Security', 'Billing', and 'Settings'. The left sidebar lists various security and data protection options, with 'Data security policies' highlighted as a new feature. The main content area shows the 'Finance dept policy' configuration page, which is currently inactive. The policy description is 'Restricting app access and protecting sensitive financial data'. It was created by Amar Sundaram just now. The 'Policy coverage' section shows that 20 Confluence spaces are selected. The 'Policy rules' section includes 'App access', 'Data export', 'Public links (Confluence only)', and 'Anonymous access', each with a brief description and a right-pointing arrow for further configuration.

Administration
https://admin.atlassian.com/data-security-policies/policy/MA-policy

ATLASSIAN Admin Acme Inc. Overview Directory Products Security Billing Settings

Security guide

USER SECURITY

Authentication policies

External user policies

Identity providers

DATA PROTECTION

Data security policies **NEW**

Data residency

Encryption

MONITORING

Audit log

Discovered products

Insights

[← Back to Data security policies](#)

Finance dept policy [Activate policy](#) [⋮](#)

Restricting app access and protecting sensitive financial data

Created by **Amar Sundaram** Just now Policy status **INACTIVE**

Policy coverage
Select data to define the policy coverage.

Selected data [>](#)
✓ 20 Confluence spaces

Policy rules
Manage rules to protect the data covered by this policy. [Learn more about data security policy rules](#)

MARKETPLACE APPS

App access [>](#)
Control how apps access data

DATA SHARING

Data export [>](#)
Block data exports from products like Jira and Confluence

Public links (Confluence only) [>](#)
Disable page links that can be viewed by the public

Anonymous access [>](#)
Restrict unlicensed users from accessing data

Data protections

Restrict app access

Administration

https://admin.atlassian.com/data-security-policies/policy/block-app-access

App access Review

App access

Protect your data by preventing selected apps from accessing information in your products and preventing future app installs. [Learn more about app access](#)

Prevent future app installs

Apps not yet installed in the selected coverage will be prevented from accessing data.

Allow future app installs

Don't allow future app installs

Prevent installed apps

Select the installed apps you would like to prevent from accessing data. Use the links under Egress and Permissions to see whether an app can send data out of the Atlassian cloud and information about the data an app has access to. [Learn more about app egress and permissions](#)

<input type="checkbox"/> App	Egress	Permissions
<input type="checkbox"/>  Figma for Confluence LITE By Collabsoft	Yes	3
<input type="checkbox"/>  Miro for Confluence By Miro	No	3
<input type="checkbox"/>  Viewtracker for Confluence By Bitvoodoo	Yes	6

FUTURE PROTECTIONS

Investments we are making in DLP

Data classifications

The practice of organizing and categorizing data according to predefined criteria

HIGHLY CONFIDENTIAL



Master key



Stocks/Money

CONFIDENTIAL



CC information



HR records

PROTECTED



Strategy



Compliance

INTERNAL



Internal docs

PUBLIC



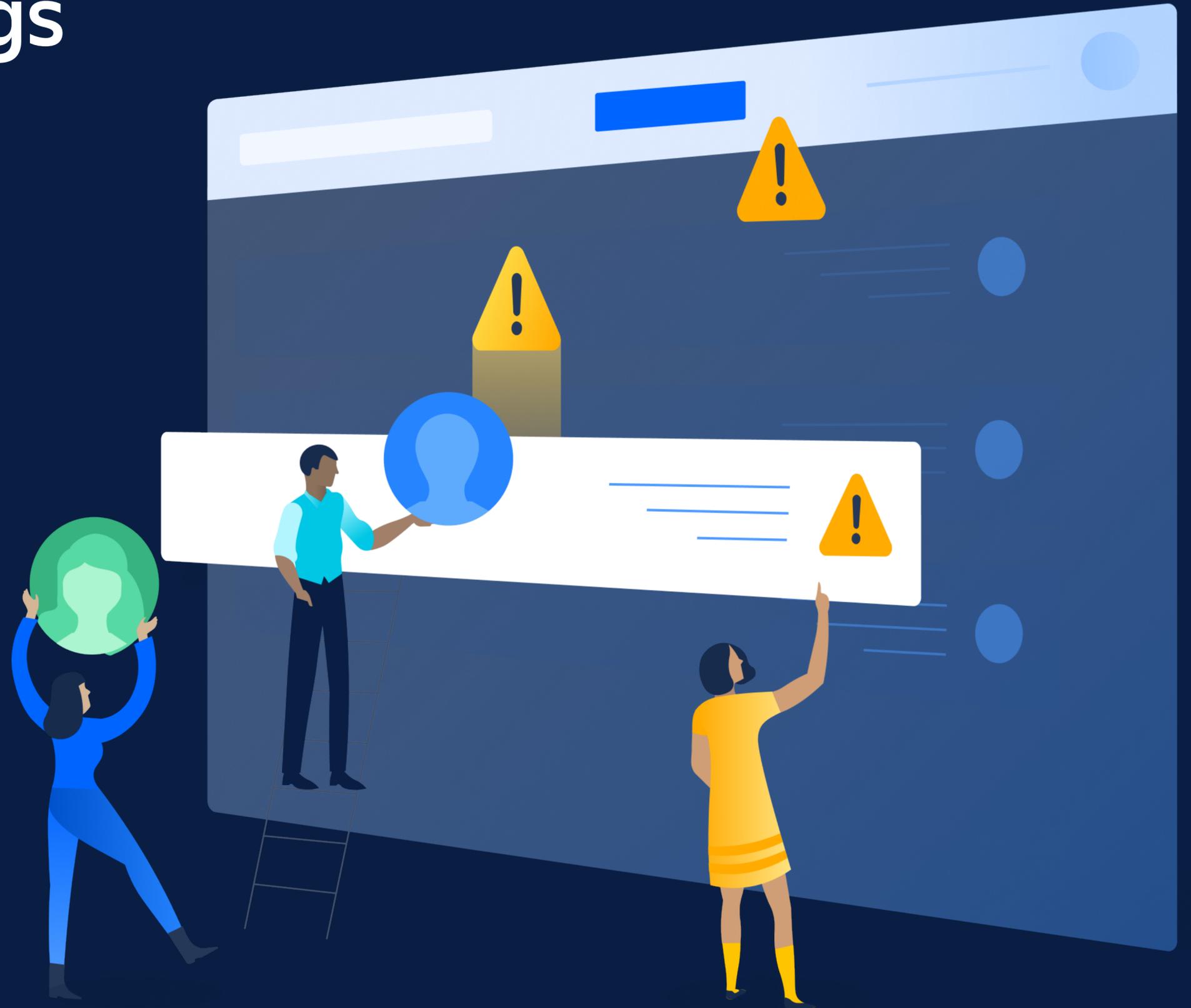
Website



Announcements

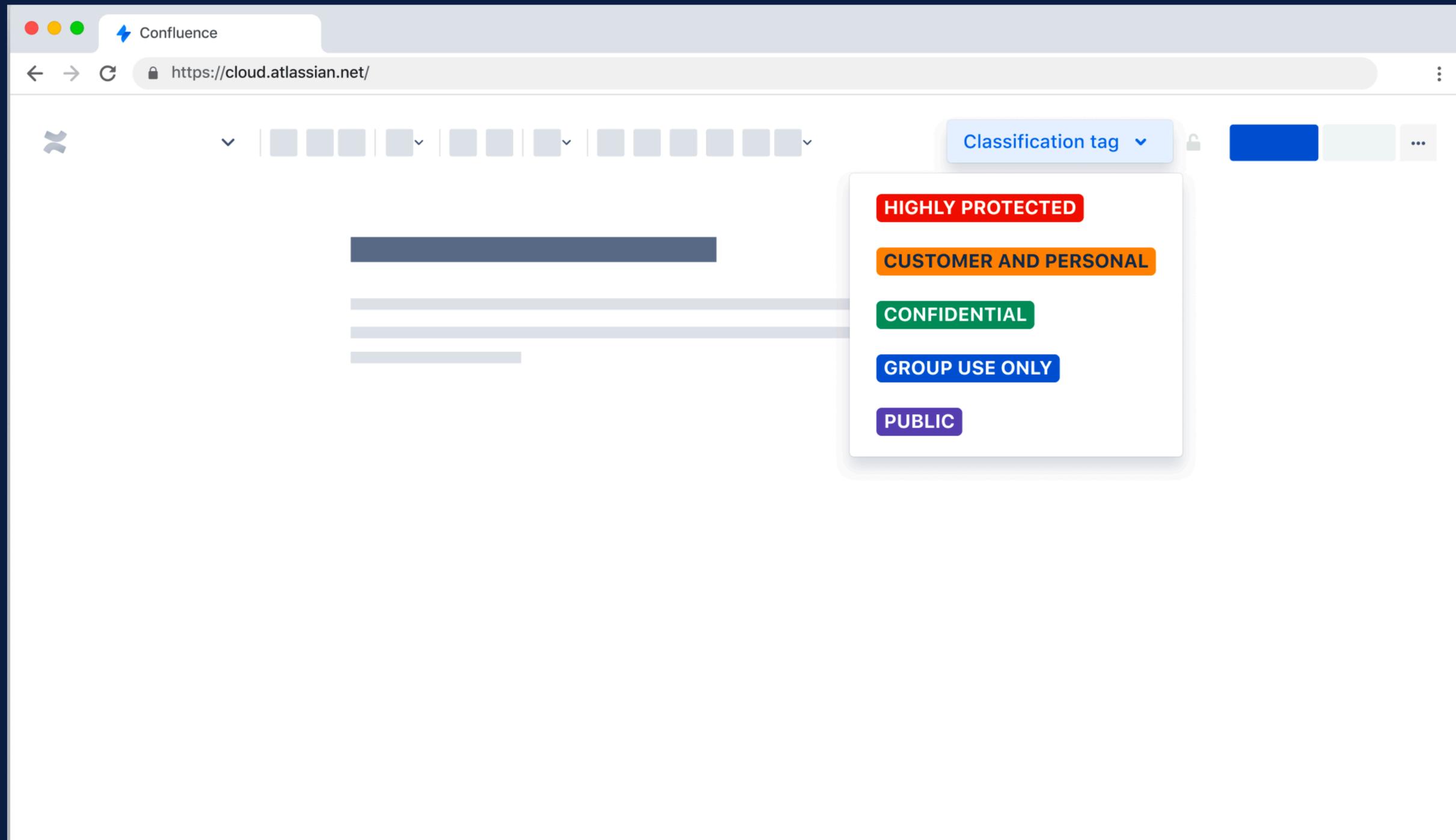
Administering tags

Setting and creating tags



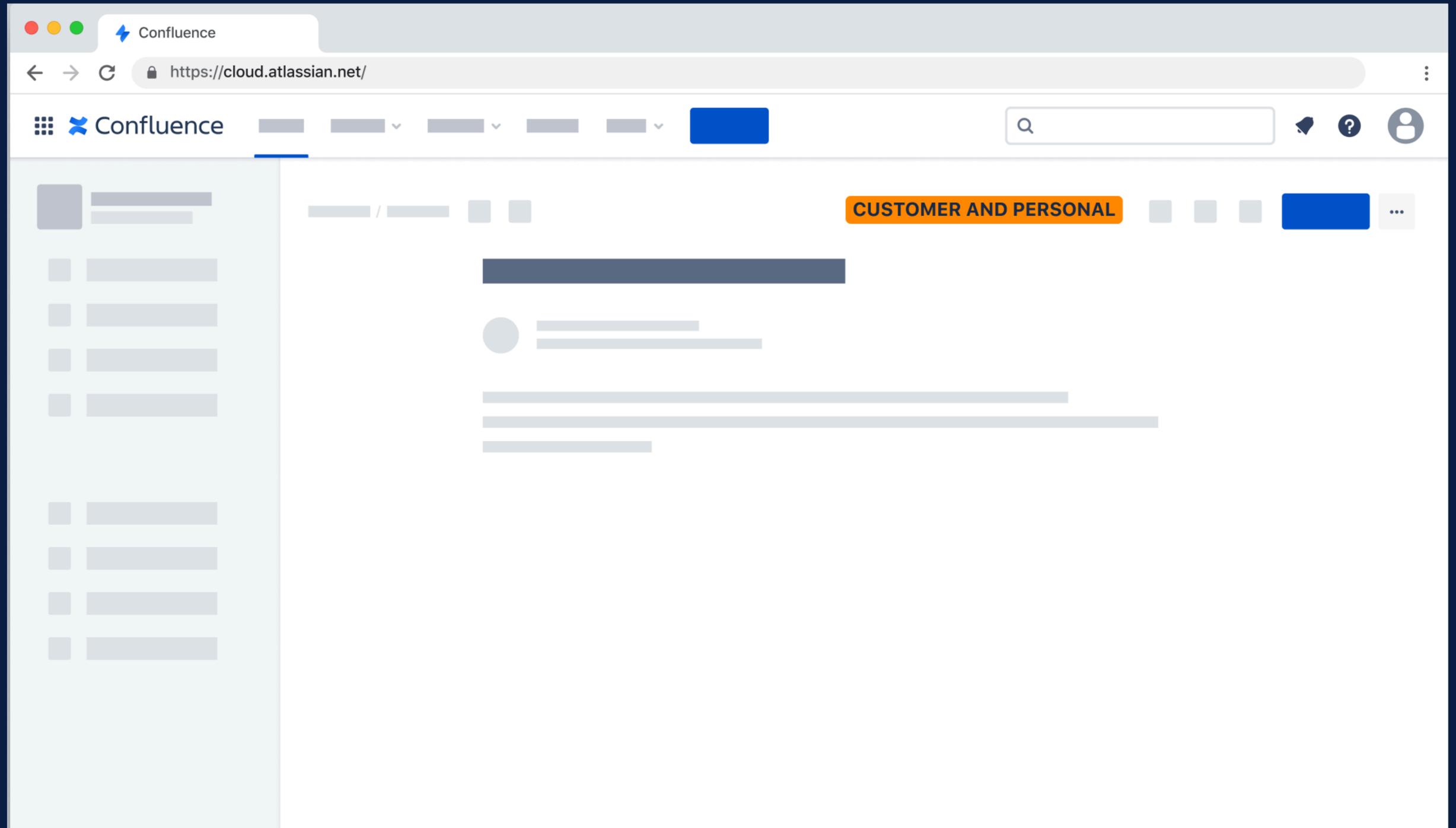
Product experience

Classifying your content



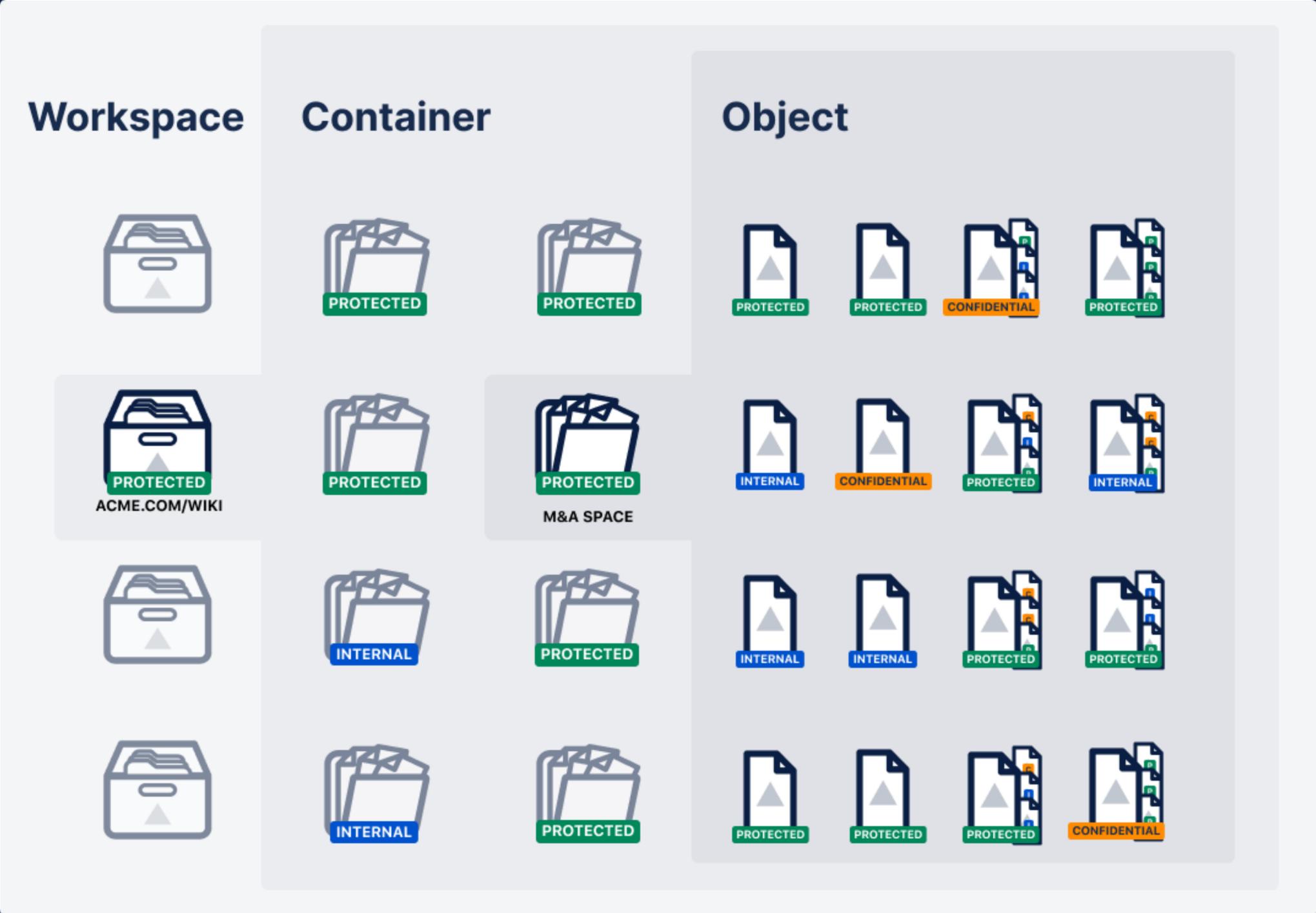
Product experience

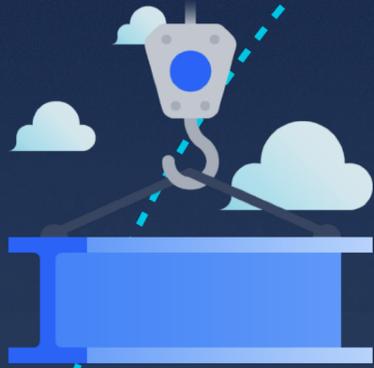
Viewing and interacting with classified content



Data protections

Protect your content based on it's classification





Customer



Atlassian



Resources



Trust whitepaper



Compliance center



Cloud roadmap