

▲ ATlassian

in Seoul '22



▲ ATlassian

in Seoul '22

Atlassian 제품은 어떤 방식으로 보안을 통제하고 규정을 준수하나? ATLASSIAN TRUST & SECURITY

Trust in Cloud

KwangSeob Jeong
Solution Engineer,
Atlassian



The background is a light blue gradient. It features several stylized, semi-transparent illustrations. At the top, there are soft, pastel-colored clouds. In the middle ground, there are two cranes, one on the left and one on the right, each lifting a rectangular object. At the bottom, there are stacks of server racks or data center equipment, also in a semi-transparent style. The overall aesthetic is clean and modern, typical of tech-related presentations.

왜 **CLOUD** 에서 신뢰가 중요할까요?

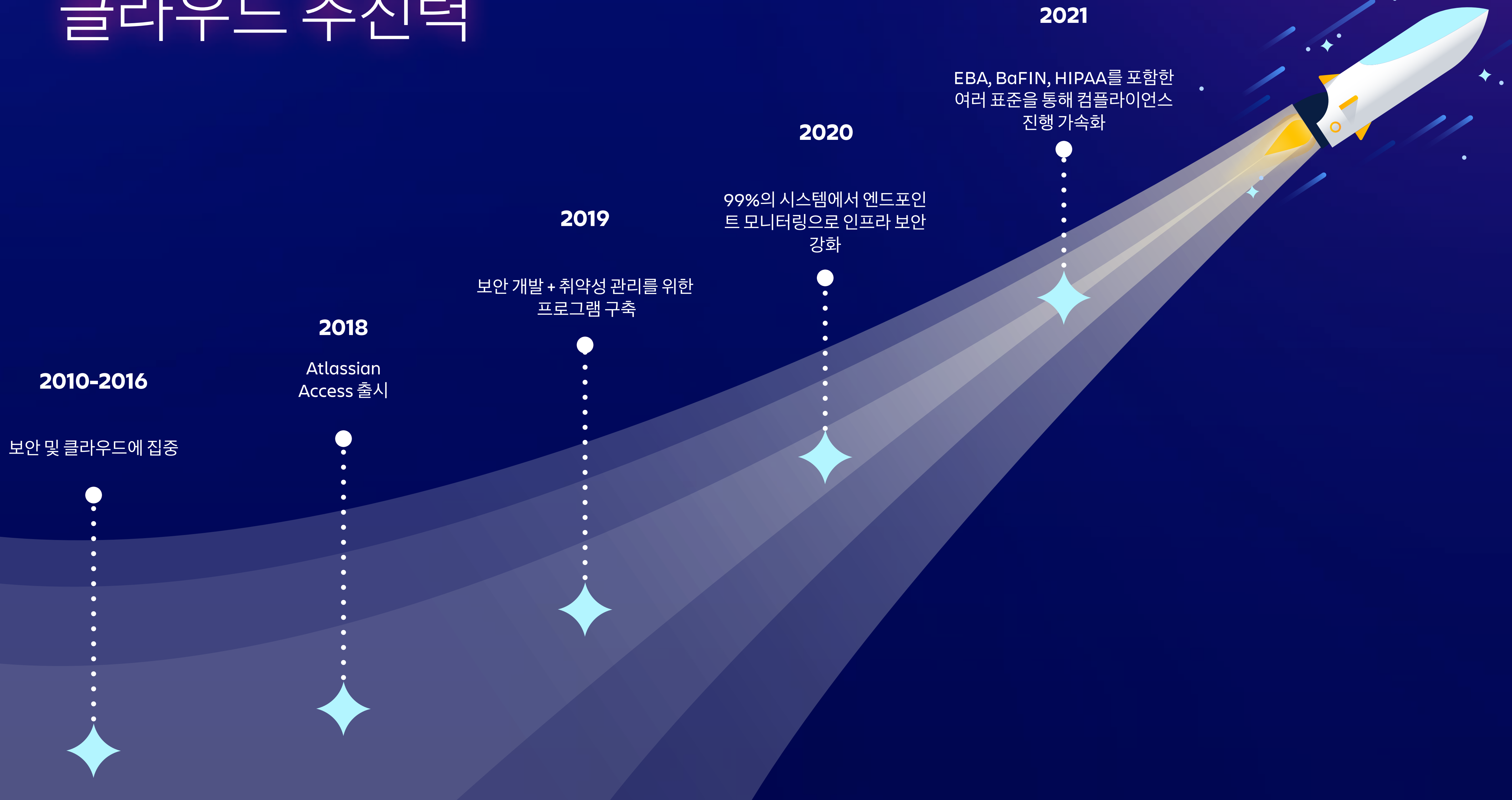
security, compliance, privacy, reliability, 그 외

신뢰는 Atlassian의 최우선 순위

Atlassian은 고객의 Cloud로 여정을 도울 파트너입니다.



클라우드 추진력



신뢰를 얻기 위한 Atlassian 의 3가지 접근 방식



COMPLIANCE



보안을 고려한 설계

Cloud 제품은 보안 및 데이터 개인 정보 보호를 기반으로 구축되어 있습니다.

보안 관행

강력한 보안 정책 및 관행을 기반으로 팀을 운영합니다.

보안 기능

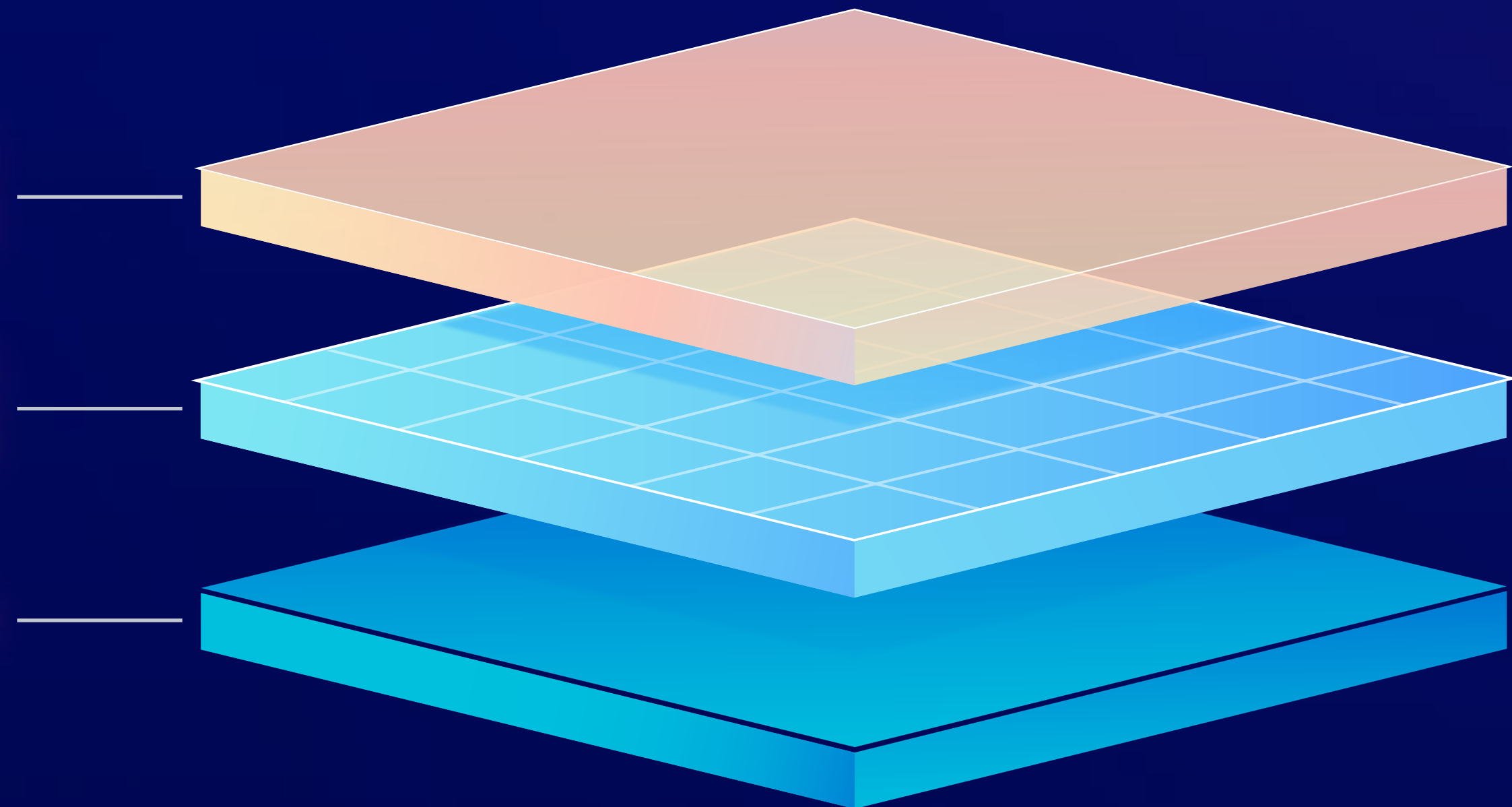
고객이 활용할 수 있는 보안 기능으로 데이터를 더 안전하게 보호합니다.

Atlassian 클라우드 플랫폼

Authentication/authorization
of micro services

Multi-tenant micro
service architecture

AWS Infrastructure



안전한 마이크로 서비스 아키텍처

테넌트의 논리적 분리

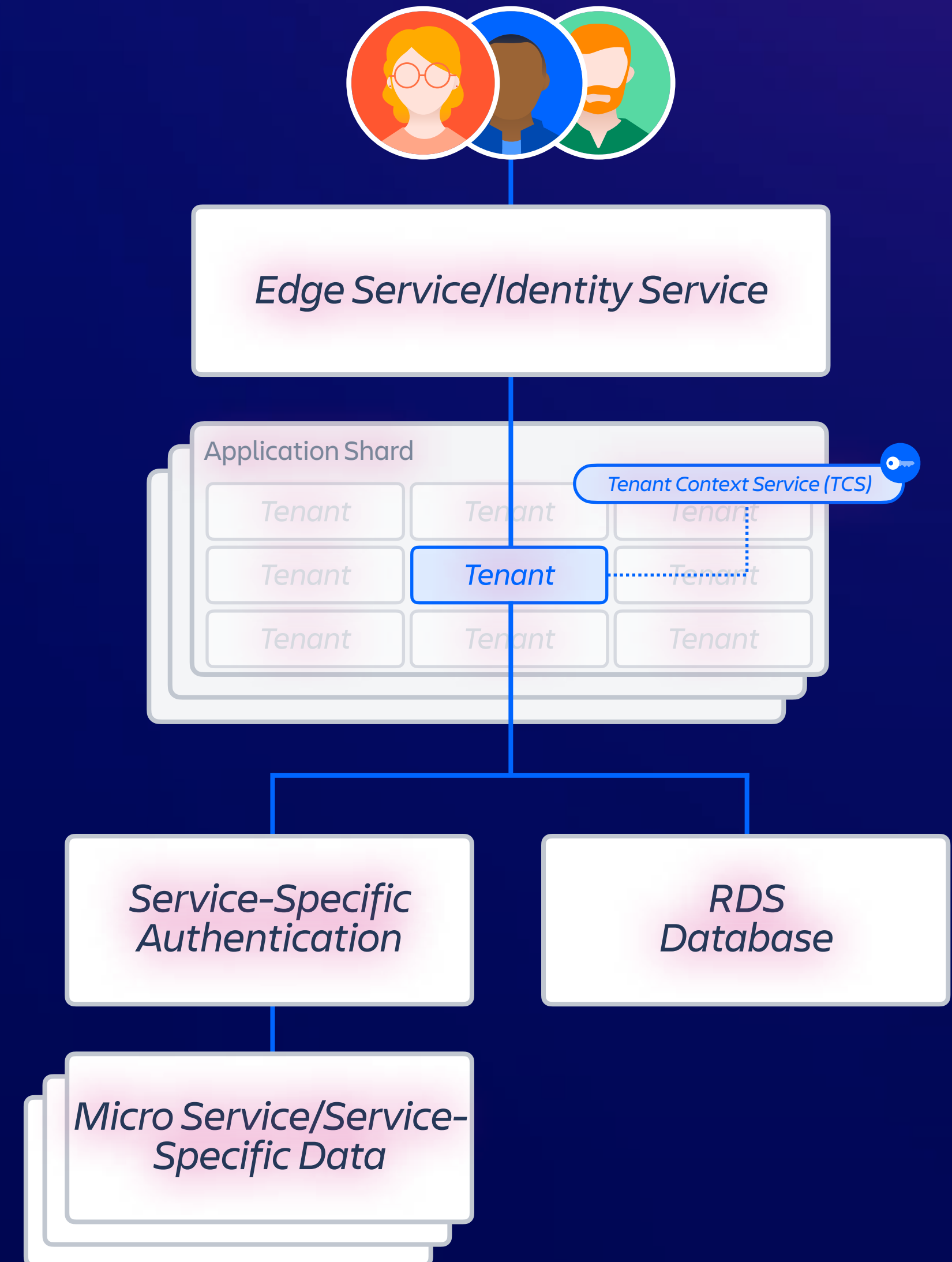
TCS는 같은 shard 내 테넌트를 다른 테넌트와 분리해서 관리

마이크로서비스마다 자체 데이터 저장소 보유

보안을 위해 각 마이크로서비스는 자체 RDS 를 갖고 있고 다른 테넌트의 Data 에 접근할 수 없음

저장 및 전송시 데이터 암호화

데이터를 저장할 때 AES256 으로 암호화(KMS), 전송할 때 TLS 1.2+ 이상 및 PFS 사용



보안 정책과 관행

1

보안 위협 방지 + 관리

보안 태세를 극대화하기 위한 관행

- 고객 데이터 접근 통제
- 상시 보안 테스트
- 모든 임직원에 보안 최우선 문화 구축



보안관행 기반 철저한 내부 통제

Jira

Your work

▼

Projects

▼

Filters

▼

Dashboards

▼

People

▼

Plans

▼

Insight

▼

Apps

▼

Create

Q Search

Prevent UGC on Local

Service project

Queues

Raise a request

Slack integration

KNOWLEDGE

Knowledge base

Reports

CHANNELS & PEOPLE

Channels

Customers

SHORTCUTS

Give feedback

Projects / Prevent UGC on Local / PUOL-167476

Internal Audit - Atlassian customer data on your laptop

Link issue

▼

1

ipaas-jira-bot raised this request via Jira

Description

Hello KwangSeob Jeong,

Ticket [PSD-28969](#) has been closed.

We have identified that you have downloaded/previewed attachments from this ticket. As required by Atlassian, all support data **must be removed** from the engineer's computer after the support is provided.

Action Needed:

Please review the files below and remove any customer data not required for an active ticket.

Files identified as potential non-compliance

Filename	Downloaded
EULA_RED_LINES.doc	04/26/2022 11:00:33PM UTC

Please let us know once the files are removed, if the files aren't related to support tickets, or are still being used.

GSAC ticket

None

Add internal note

/

Reply to customer

Pro tip: press **M** to comment

Done

▼

✓ Done

SLAs

18 May 10:22 AM

✗

 Time to reminder within 168h

18 May 10:22 AM

✗

 Time to Resolution within 168h

Details

Assignee

KwangSeob Jeong

Reporter

1

ipaas-jira-bot

Service Desk Origin

None

Knowledge base

1 related article

Due date

None

Priority

Minor

Labels

[gsac-production](#)

Leader / Manager

Scott Goh-Davis

Who's Looking?

Open Who's Looking?

Automation

Rule executions

My Reminders

Open My Reminders

More fields

Request participants, Approvers, Organizati...

▼

Spaces

People

Apps

Templates

Create

Q

Search

Solutions Engineering - Trust Scorecard - 2022-05-16

S

Created by sec-scorecards-bot

May 17, 2022

10 min read

5 people viewed

No updates

What's New in Trust Scorecards

2022-Apr-01: Q4 Trust Scorecard changes are here!

If you need help or have feedback, please contact us in [#trust-scorecards](#)

Product	Solutions Engineering
Owner	@Sean Muranjan
Cost Center	Sales:Solutions Engineers
Assessment Date	2022-05-16
Partner Security Engineers	Solutions Engineering currently has no Partner Security Engineers assigned to it. See go/securitypartners to learn about Security's Partnership program and how your product can engage with it.
Overall Score	<div> 115 / 120 (95%) - How is this scored? <div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> </div> </div> <div> <div>Compare with other products</div> <div>Solutions Engineering's scores over time</div> </div>
About This Scorecard	This scorecard was uploaded automatically. Products without Partner Security Engineers have scorecards uploaded automatically every 2 weeks.

Scored

보안 정책과 관행

1

보안 위협 방지 + 관리

보안 태세를 극대화하기 위한 관행

2

사고 감지 + 대응

보안 위협을 감지하고 대응하기 위한 프로세스 구축

- “보안 침해는 발생한다”라는 마인드셋
- 의심스러운 활동에 대해 선제적 예방 활동
- 보안 침해 지표를 조기에 발견
- 보안 사고 유형에 대한 대응 플레이북



보안 정책과 관행

1

보안 위협 방지 + 관리

보안 태세를 극대화하기 위한 관행

2

사고 감지 + 대응

보안 위협을 감지하고 대응하기 위한 프로세스 구축

3

비즈니스 연속성 + 재해 복구

사고로 부터 빠르게 복구하기 위한 지속적인 백업 및 복구 훈련

- 복구를 위한 4 티어 시스템
- 분기별 백업 테스트
- 중단에 대비한 계획

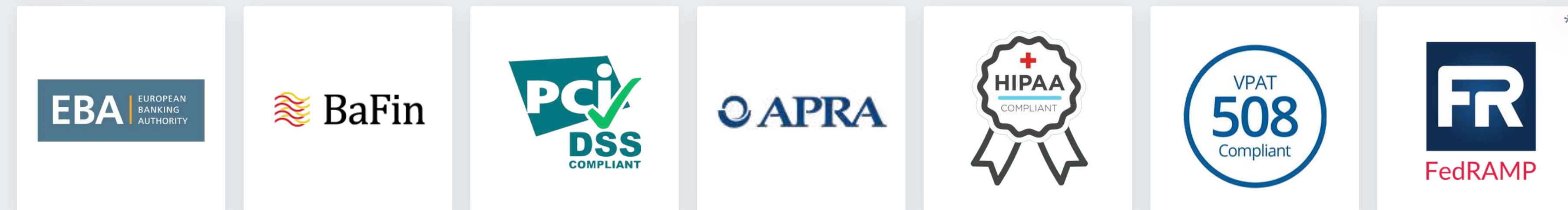


규제 + 컴플라이언스 표준 획득

Core / Foundational



산업별



재무

의료

정부

* 제공 예정

And this list continues to grow! Visit [Compliance at Atlassian](#) →

Atlassian 의 2명의 CTO

Atlassian 의 CTO를 소개합니다.



“

As I looked at my next step, the set of learnings and experiences I wanted to have and where I could be most helpful, the CTO role at Atlassian offered a lot of what I was looking for.

Rajeev Rajan
Chief Technology Officer



“

Atlassian은 고객에서 더 높은 수준의 서비스를 제공하기 위해 노력합니다.

Atlassian은 투명하며 독립적으로 검증할 수 있도록

Atlassian의 관행을 공개적으로 문서화합니다.

Adrian Ludwig

Chief Trust Officer(최고 신뢰 책임자)



신뢰와 보안을 위한 조직 구성

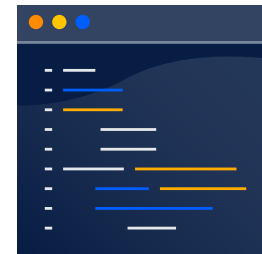
Trust Organization



SECURITY



**RISK +
COMPLIANCE**



**TRUST
ENGINEERING**



**TRUST CULTURE
+ TRAINING**



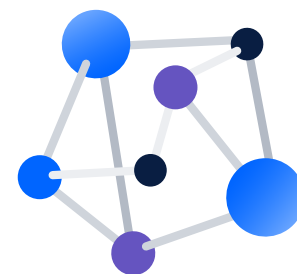
**SECURITY
INTELLIGENCE**



**PRODUCT
SECURITY**



**RED
TEAM**



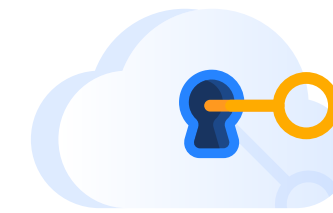
**TRUST
ENGAGEMENT**

보안을 고려한 설계 + 보안 관행

Enterprise Trust (R&D Teams)



**TRUST
FOUNDATION**



**CLOUD
SECURITY**



**CLOUD
ADMIN**

보안기능



ID 관리 및 접근 통제

인증 제어로 접근 통제



정보 보호

민감한 비즈니스 데이터 보호

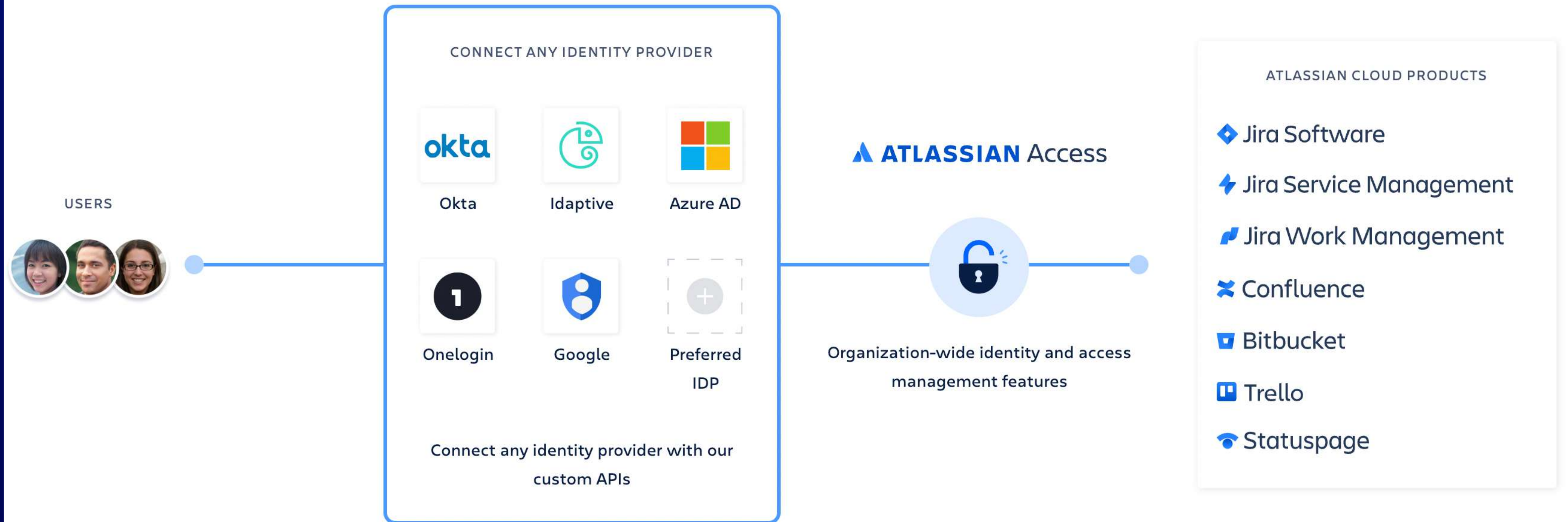


위협 탐지

위협 감지 및 조사

ATLASSIAN ACCESS + CLOUD ENTERPRISE

쉬운 SSO 연동 + 2 Factor 인증





ID 관리 및 접근 통제



인증 제어로 접근 통제



정보 보호



민감한 비즈니스 데이터 보호



위협 탐지



위협 감지 및 조사

ATLASSIAN ACCESS + CLOUD ENTERPRISE

Audit log

ATLASSIAN

Admin

wiswedel

Overview

Directory

Products

Security

Billing

Settings

?

Security guide

Insights

Audit log

Data residency

IP allowlists

Discovered products

Mobile app policy

Authentication policies

SAML single sign-on

Admin / wiswedel

Audit log

Use the audit log to monitor key activities across your organization and in your products. The log tracks activities within the past 180 days.
[Learn more about the audit log](#)

Search by name, group, or site

e.g. YYYY/MM/DD

to

e.g. YYYY/MM/DD

All activities

Apply

Date	Location	Actor	Activity
Jun 29, 2022 09:21 GMT+9	Unavailable	Atlassia Atlassia	Edited CDEN Setting custom
Jun 29, 2022 04:13 GMT+9	Unavailable	Sascha swiswed	Edited Jira issue SCM1-5
Jun 29, 2022 04:13 GMT+9	Unavailable	Sascha swiswed	Viewed Jira issue SCM1-5
Jun 29, 2022 04:13 GMT+9	Unavailable	Sascha swiswed	Created Jira issue SCM1-5
Jun 29, 2022 04:11 GMT+9	Unavailable	Sascha swiswed	Viewed Jira issue SCM1-1
Jun 28, 2022 19:42 GMT+9	Frankfurt am Main 18.159.201.171	Lazar Ideretic	Exported managed accounts
Jun 28, 2022 09:21 GMT+9	Unavailable	Atlassia Atlassia	Edited CDEN Setting custom domain
Jun 27, 2022 23:39 GMT+9	Frankfurt am Main 18.159.201.171	user1 user1@sascha-wiswedel.de	Logged in to account successfully

Added user to group

Resent invite to user

Resent site invitation to user

Removed user from organization

Suggested changes to details for user

Revoked role from user for product

Granted product access to group

Remove default access from group

Removed product admin access from group

Removed role from group

Mobile Policy

Create your mobile policy

These policy settings apply to supported cloud mobile apps for both Android and iOS (unless indicated otherwise). [Learn how these settings work](#)

Apply this policy to

- ☒ All users with access to your organization's products
- ☐ Specific users

App data protection

- ☒ Disable sharing, saving, or backing up data to devices
- ☒ Disable screenshots (Android only) and screen recording
- ☐ Prevent cutting or copying data from within the app

App access requirements

- ☒ Require data encryption
- ☒ Require biometric authentication or a device passcode
- ☒ Set a minimum OS version

Android

Android 11



iOS / iPadOS

iOS / iPadOS 15



Cancel

Create policy

IP allowlist

Create allowlist

Name *

Work from Home

Applies to *

Confluence x Jira x Confluence x



Available for products with a Premium plan

IP addresses *

112.161.132.37 x



Enter IPv4 and IPv6 addresses and ranges separated by commas. Use CIDR notation.

Enable?

- ☒ Do this later
- ☐ Apply immediately

Cancel

Create



ID 관리 및 접근 통제



인증 제어로 접근 통제



정보 보호



민감한 비즈니스 데이터 보호



위협 탐지



위협 감지 및 조사

ATLASSIAN ACCESS + CLOUD ENTERPRISE

CASB 로 데이터 유출 방지



Bringing advanced security and threat protection capabilities to Atlassian cloud customers.

[Try Atlassian Access](#)

[Learn more: McAfee MVISION Cloud →](#)

Key benefits



Centralized visibility

Gain full visibility into activities performed by users and administrators on Atlassian cloud products and your other cloud applications in one place.



Advanced data security

Protect important Atlassian cloud data wherever it lives. With advanced data loss prevention capabilities, you can reduce the risk of breaches, information loss, and more.

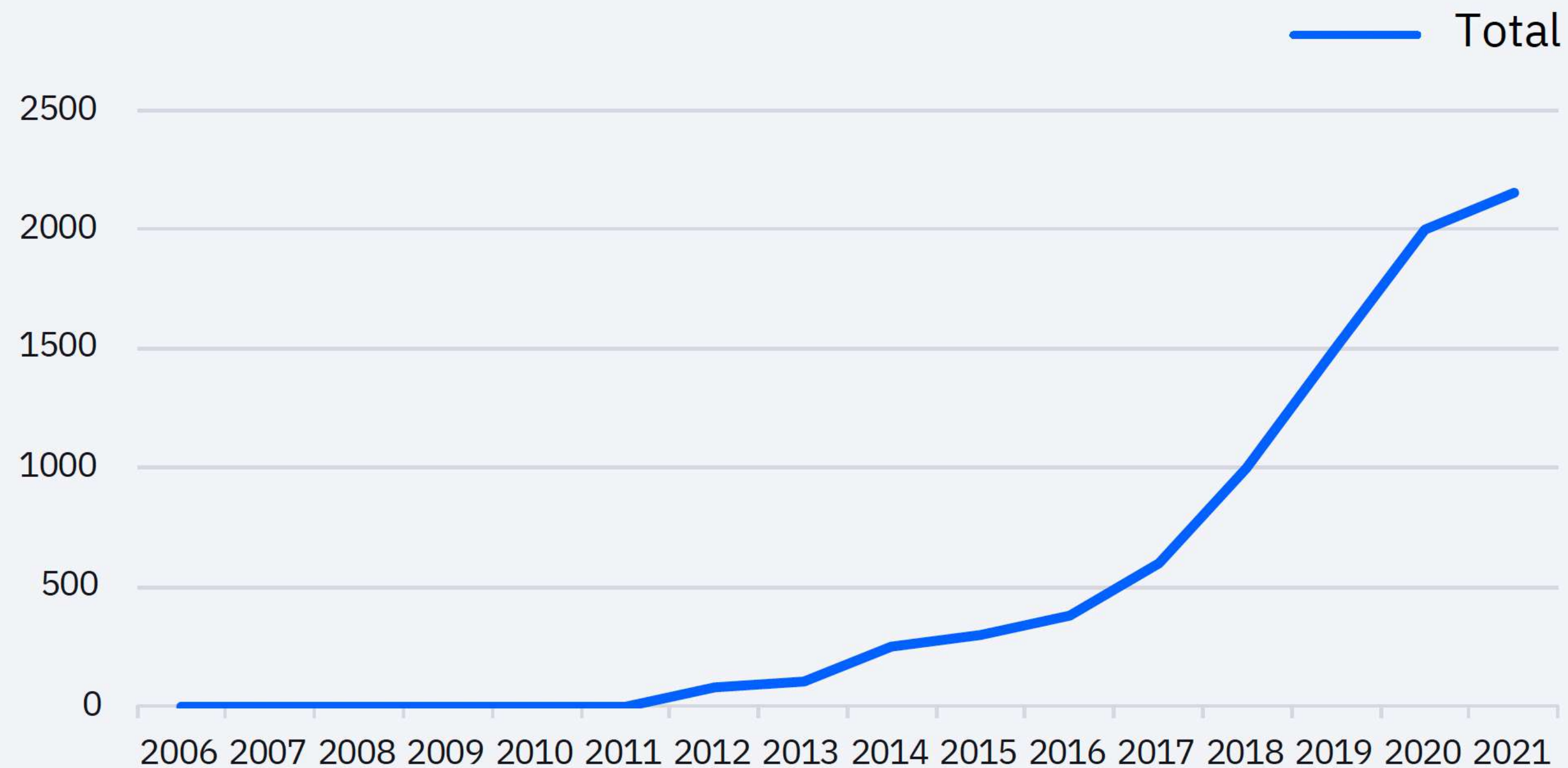


Threat protection

With automatic monitoring, you can safeguard your Atlassian cloud data from threats such as compromised accounts, insider attacks, and other malicious behavior.

클라우드 환경에서 발견된 보안 취약점 증가


Number of cloud vulnerabilities tracked by X-Force



Source: IBM x-force report

오픈소스 취약점에 대응하기 위한 Atlassian 의 노력


THE **LINUX** FOUNDATION PROJECTS



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

[About](#) [Community](#) [Training](#) [News](#) [Blog](#) [Get Involved](#) [Shop](#) [Membership Inquiries](#) [Join](#) [Search](#)

Governing Board




Adrian Ludwig
Chief Trust Officer,
Atlassian

Adrian Ludwig is the Chief Trust Officer at Atlassian. He is responsible for Atlassian's security, risk & compliance and privacy practices. Adrian joined the company in May 2018 and previously held the role of Chief Information Security Officer where he oversaw Atlassian's security team and initiatives. Prior to joining Atlassian, Adrian held a number of leadership positions where he was in charge of building out security capabilities at Nest, Macromedia, Adobe, and Android (Google).

[Read More](#)

[in](#)




Andrew Van Der Stock
Executive Director, OWASP
Foundation

Andrew is a seasoned web application security specialist and enterprise security architect. He is the Executive Director at OWASP, taking the Foundation through organizational change and taking our mission to the next level. Andrew has worked in the IT industry for over 25 years. Andrew has researched and developed the web application security and architecture fields since 1998.

[Read More](#)

[in](#)




Bob Callaway (TAC Chair)
Tech Lead & Manager,
Google Open Source
Security Team

Bob is the tech lead & manager of the supply chain integrity group in Google's Open Source Security Team. He and his team directly contribute to critical OSS secure software supply chain projects (including sigstore that he co-founded), as well as help drive adoption of best practices throughout the broader open source ecosystem.

[Read More](#)

[in](#) [Twitter](#) [GitHub](#)



Brian Fox
CTO, Sonatype

Brian is Co-founder and Chief Technology Officer at Sonatype. He has extensive open source experience as a member of the Apache Software Foundation and former Chair of the Apache Maven project. Brian was a direct contributor to the Maven ecosystem, including the maven-dependency-plugin and maven-enforcer-plugin. He has over 20 years of experience driving the vision behind, as well as developing and leading the development of software for organizations ranging from startups to large enterprises. Brian is a frequent speaker at national and regional events including Java User Groups and other development related conferences.

[Read More](#)

Vulnerability Disclosures

open source software ecosystem where the time to fix a vulnerability and deploy that fix across the ecosystem is measured in minutes, not months.

Security Tooling

to provide the best security tools for open source developers and make them universally accessible.

Identifying Security Threats

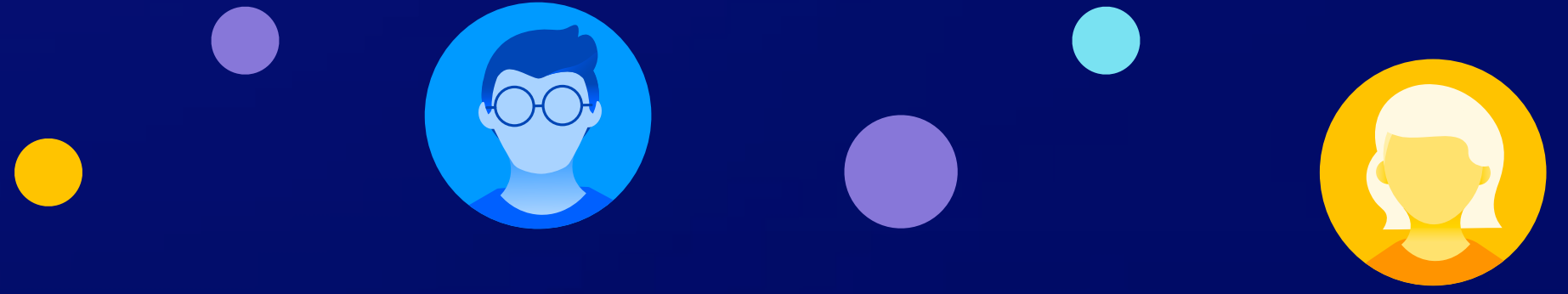
enable stakeholders to have informed confidence in the security of open source projects.

Security Best Practices

to provide open source developers with best practices recommendations.


Securing Critical Projects

to perform audits, assurance, response teams, improvements and hands on tactical work.



SRE팀은 Cloud 를 사용
한 후 기존 대비 서버 운영
에 드는 시간이 25% 줄어
들었습니다.

LUCID SOFTWARE



이제 보안이나 취약점때문에 걱
정하거나 리소스를 투입할 일이
없어졌습니다.

Cloud 사용후 안심할 수 있다는
것이 가장 큰 장점입니다.

EMC INSURANCE

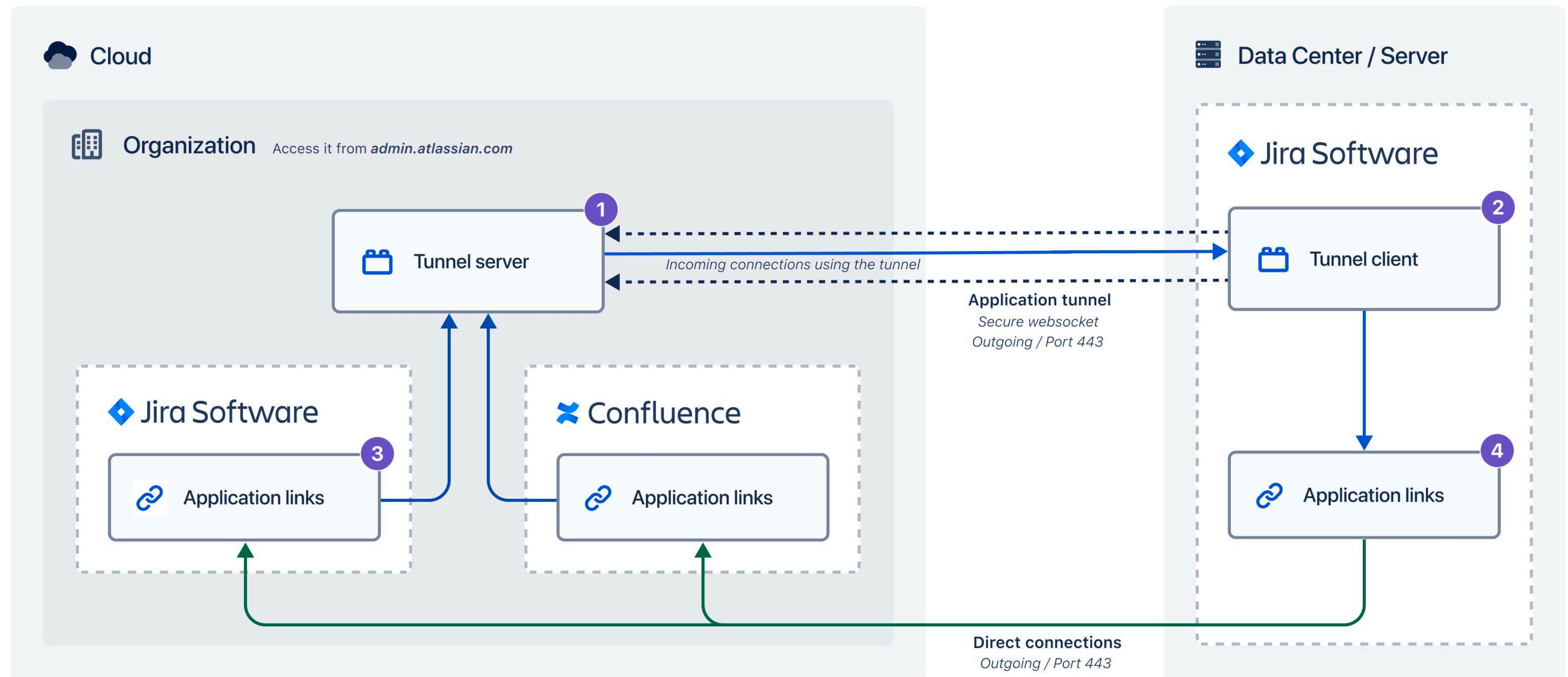


Cloud 로 migration 하는 절차와 기간은?

On-prem 에서 cloud 로 이관하기



Cloud와 On-Prem을 안전하게 연결하는 App Tunnel



The background is a light blue gradient. It features several stylized white and light blue clouds of various sizes. There are also illustrations of cranes lifting server racks, and stacks of server racks themselves, suggesting a data center or cloud infrastructure theme.

CLOUD 를 사용하면 보안팀 역할이 확장됩니다.

조직의 이니셔티브와 전략을 달성하기 위한
보안 정책/운용에 더 집중할 수 있습니다.