ATLASSIAN

Cómo Atlassian Cloud logra seguridad y cumplimiento normativo de nivel empresarial

Análisis detallado del compromiso de Atlassian con la privacidad de los datos globales, las certificaciones, el cumplimiento normativo y mucho más.

Índice

En el cambiante panorama digital actual, la nube ha supuesto la posibilidad de escalar de forma ilimitada y de que los equipos colaboren sin importar que trabajen en lugares alejados de la oficina. Sin embargo, el aumento de los dispositivos y los canales disponibles para acceder a las aplicaciones en la nube ha supuesto un aumento del riesgo de sufrir filtraciones de datos y la necesidad de garantizar el cumplimiento de las cambiantes obligaciones con respecto a la privacidad de los datos en todo el mundo. Atlassian se compromete plenamente a ayudar a sus más de 190 000 clientes a disfrutar de todas las ventajas de escalar en la nube, así como a cumplir con los estándares más altos en materia de seguridad y privacidad de datos. En este artículo, se explica el enfoque de cinco dimensiones que sigue Atlassian a la hora de preparar sus productos Cloud para el ámbito empresarial desde el punto de vista de la seguridad y el cumplimiento.

Protección de la arquitectura en la nube de Atlassian con un enfoque de confianza cero

El enfoque de Atlassian con respecto a la seguridad en la nube parte de la arquitectura de red. Hemos implementado controles en cada capa del entorno de la nube y aplicamos un enfoque de seguridad de confianza cero para dar acceso a la red, sistemas y servicios corporativos.

Seguridad integral de datos con controles avanzados para la residencia y el cifrado

Proteger los datos de los clientes es prioritario, por lo que Atlassian cuenta con numerosas protecciones a fin de ofrecer total tranquilidad. Todos los datos de los clientes se alojan en Amazon Web Services, la plataforma líder del sector, con una redundancia de varios niveles. Para proporcionar un control adicional, Atlassian ofrece residencia de datos, es decir, la posibilidad de anclar datos de productos a determinadas regiones geográficas. Además, cifra todos los datos de los clientes, tanto en reposo como en tránsito, y sigue invirtiendo en controles avanzados, como el cifrado “Bring-Your-Own-Key” (BYOK, uso de claves de cifrado propias).

Inversión continua en el cumplimiento de las obligaciones globales de privacidad de datos

Todos los productos de Atlassian llevan incorporadas funciones de privacidad de datos. El equipo de Riesgo y Cumplimiento de Atlassian trabaja continuamente en tu nombre para garantizar que todos los productos Cloud cumplan con los estándares globales, incluidos el SOC, la ISO, el RGPD y las normativas específicas del sector.

Controles integrados para la gestión de accesos e identidades

Los controles integrados de Atlassian permiten a los administradores de TI aplicar protocolos de autenticación de nivel empresarial, incluidos el inicio de sesión único de SAML o la autenticación en varias fases, entre otros. Asimismo, los administradores pueden adaptar las políticas de autenticación a diferentes subconjuntos de usuarios, automatizar el aprovisionamiento y el desaprovisionamiento de los usuarios a fin de reducir el riesgo de que se produzcan accesos no autorizados, y aplicar controles de seguridad para el uso móvil con compatibilidad con la gestión de dispositivos y aplicaciones móviles (MDM/MAM).

Supervisión y protección proactivas de amenazas

Con el objetivo de evitar amenazas, Atlassian proporciona pruebas exhaustivas de seguridad y programas de gestión de vulnerabilidades para todos sus productos Cloud. Además, con Atlassian Access, los clientes obtienen registros de auditoría de la organización, que ofrecen información completa sobre su actividad administrativa, como los cambios en los usuarios, grupos y permisos, y permiten clasificar las actividades sospechosas.

Analicemos cada uno de estos elementos de seguridad de forma detallada.

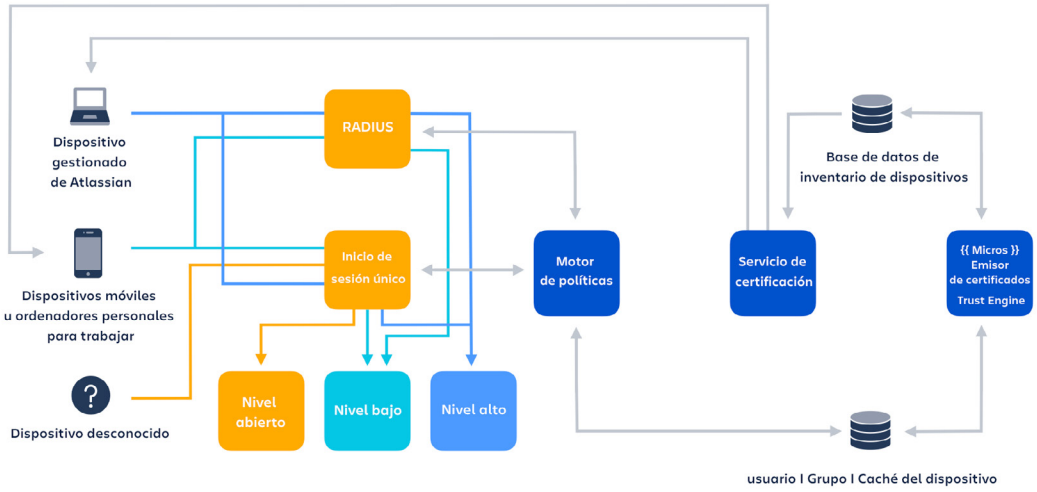
Protección de la arquitectura en la nube

Atlassian adopta **un enfoque por capas** para la seguridad, que consiste en dividir su infraestructura de nube en zonas, entornos y servicios, e implementar controles en cada una de estas capas. Este proceso limita el tráfico de red del personal, los datos de los clientes, la integración e implementación continuas (CI/CD) y la zona desmilitarizada (DMZ) que puede fluir a través de cada zona. También se utilizan listas de permitidos de autenticación para controlar y autorizar explícitamente los servicios que pueden interactuar entre sí.

Enfoque de confianza cero

En cuanto al acceso a la red, Atlassian adopta un enfoque más granular mediante un sistema llamado **Confianza cero**: “No te fíes nunca, compruébalo siempre”. Este enfoque no solo tiene en cuenta las credenciales de autenticación, sino también la confidencialidad de los recursos a la hora de determinar cómo se puede acceder a ellos en las redes de Atlassian. En función de la confidencialidad de un recurso, este se ofrece con una seguridad de nivel abierto, bajo o alto.

- Se puede acceder a los recursos de nivel abierto con la autenticación de usuario de la red de Atlassian adecuada.
- Para los recursos de nivel bajo se requiere tanto la autenticación de usuario como el uso de un dispositivo corporativo de confianza (facilitado por Atlassian o inscrito en el programa de gestión de dispositivos móviles).
- Los recursos de nivel alto requieren la autenticación de usuario y pueden acceder a ellos usuarios con un dispositivo corporativo facilitado por Atlassian.



Recuperación ante desastres y continuidad empresarial

Por último, como todos sabemos, pueden producirse interrupciones; Atlassian las planifica activamente mediante la creación de planes de recuperación ante desastres y continuidad empresarial en todos sus procesos. Para satisfacer las necesidades de recuperación ante desastres y continuidad empresarial, se incorporan en todos los productos medidas de redundancia, que prueban periódicamente los ingenieros de fiabilidad del sitio a fin de detectar cualquier carencia. Todos los equipos de Atlassian trabajan con un líder en recuperación ante desastres que garantiza que esta se integre en todos los proyectos producidos por el equipo; además, se llevan a cabo pruebas de recuperación ante desastres de forma frecuente con el fin de mejorar los procesos y la tecnología de Atlassian.

Seguridad integral de los datos

Según IBM, una empresa que sufra una filtración de datos deberá invertir de media unos 3,86 millones de dólares por filtración en detección y escalación, pérdidas empresariales, esfuerzos de notificación y respuesta ex post. A cualquier líder de seguridad se le pone la piel de gallina con solo imaginar esta situación. Por ello, la seguridad de los datos es una parte esencial de todos los productos de Atlassian Cloud, en los que los datos se almacenan, se cifran y se mantienen privados de forma segura. Además, Atlassian garantiza que los clientes tengan el control de sus datos en la mayor medida posible.

Infraestructura de alojamiento líder del sector

Los productos y los datos de Atlassian se alojan en Amazon Web Services (AWS), un proveedor de alojamiento en la nube líder del sector. En la red de AWS, los datos de los clientes se alojan en varias regiones geográficas diferentes, incluidas las ciudades de la costa este y oeste de Estados Unidos, la Unión Europea y la región Asia-Pacífico. Los datos se replican siempre en otros centros de datos aislados geográficamente (conocidos como zonas de disponibilidad), de modo que, en caso de fallo de una zona de disponibilidad, los clientes de Atlassian no se ven afectados.

> CHG Healthcare ha conseguido ahorrar casi 120 000 dólares hasta la fecha y más de 30 horas por semana, que puede dedicar a la innovación en lugar de a la administración, aligerando la infraestructura y reduciendo el mantenimiento que esta precisa. Además, ahora que Atlassian gestiona los parches y las actualizaciones de seguridad, CHG no tiene que preocuparse de las vulnerabilidades.

Controles de residencia de datos

Dada la aplicación de normativas de datos geográficos, como el Reglamento general de protección de datos (RGPD) de la Unión Europea, Atlassian permite que sus clientes elijan el lugar en el que se almacenan sus datos del modo más sencillo posible. Con la función de residencia de datos (disponible en todos los planes de pago), ahora los administradores de TI pueden anclar los datos de productos que generan los usuarios, como páginas de Confluence y tickets o comentarios de Jira, a determinados ámbitos de datos.

Las opciones de residencia de datos de Atlassian permiten que los clientes tengan un mayor control de estos. Por ejemplo, si hace falta anclar una parte determinada de los datos de una empresa a una región, los administradores de TI pueden optar por aislar dichos datos en una **única instancia de producto** para garantizar el aislamiento de los datos y el cumplimiento de las normativas relativas a estos.

Por el momento, la residencia de datos está disponible en la Unión Europea y Estados Unidos, pero Atlassian tiene planeado **ofrecerla en otras regiones**, como Australia, Reino Unido, Canadá y Japón a mediados de 2022. Además, como parte del compromiso de Atlassian de mejorar continuamente los productos Cloud, a finales de 2021 se lanzará la **residencia de datos para aplicaciones de terceros**.

Con el fin de satisfacer los requisitos de rendimiento de usuarios de todo el mundo, los datos de la información de las cuentas de usuario se replican a nivel global, por lo que, la residencia de datos no se aplica actualmente a estos datos. Ni el RGPD ni la Schrems II lo exigen; en cambio, se centran en la necesidad de proporcionar la protección adecuada a los datos europeos cuando salen de Europa. Por ello, Atlassian se adhiere a las cláusulas contractuales tipo para garantizar que todos los datos de los usuarios se protejan adecuadamente, tal y como exige el Reglamento general de protección de datos. Para obtener más información sobre el lugar y la forma en que se almacenan los datos de usuario, accede a **Atlassian Trust Center**.

Cifrado de datos en tránsito y en reposo

En lo que respecta a la seguridad en la nube, **cifrar los datos confidenciales** debería ser la apuesta inicial de cualquiera persona que trabaje en este sector. Por ello, Atlassian se compromete a aplicar capas a la seguridad de toda su arquitectura de nube y a proporcionar cifrado de datos en reposo para todos los datos y adjuntos de los clientes en Jira Software Cloud, Jira Service Desk Cloud, Jira Work Management, Confluence Cloud, Statuspage, Opsgenie y Trello.

Todos los datos inactivos que se almacenan en los servidores se cifran

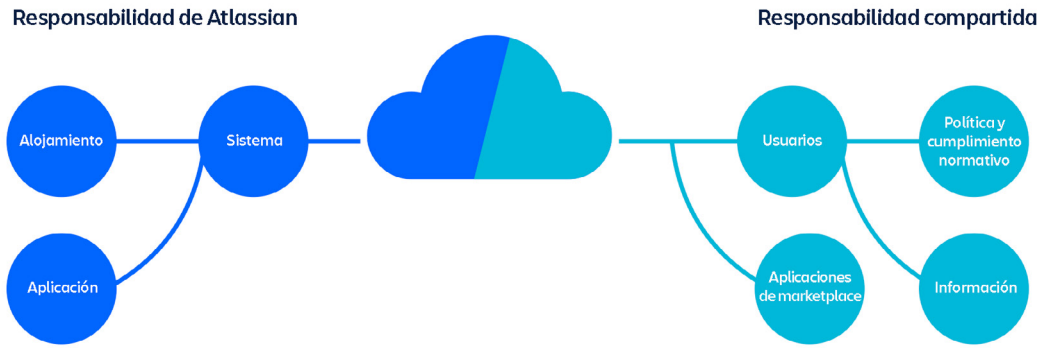
en reposo de acuerdo con el estándar del sector Advanced Encryption Standard 256. Se cifran todos los datos de los clientes durante el tránsito por las redes públicas mediante el protocolo de Seguridad de la capa de transporte 1.2+ con confidencialidad directa total (PFS), que garantiza un cifrado con códigos y longitudes de clave seguros. Estas medidas contribuyen a proteger los datos contra cualquier revelación o modificación no autorizada durante el tránsito.

Cifrado Bring Your Own Key (BYOK) próximamente disponible para Atlassian Cloud Enterprise

A principios de 2023, se implementará la función de **cifrado Bring Your Own Key (BYOK)** para Jira y Confluence, destinada para empresas que quieran tener un control adicional. Con ella, las empresas podrán gestionar sus propias claves criptográficas a través del Key Management Service de Amazon Web Services. Además de poder conceder o revocar el acceso, BYOK también ofrece un control de compensación para satisfacer las necesidades de cumplimiento de las normativas referentes a la seguridad de los datos.

Colaboración para la protección de los datos

Atlassian asume enteramente la responsabilidad de la seguridad, el rendimiento y la disponibilidad de sus sistemas, pero también requiere la plena participación de los clientes para la protección de todos sus datos.



Existen cuatro responsabilidades compartidas de las que los usuarios deben tomar nota:

Política y cumplimiento
La **política de privacidad** de Atlassian está disponible públicamente, al igual que **las distintas normativas** a las que hace referencia. Sin embargo, en última instancia, corresponde al usuario garantizar que el sistema Atlassian satisfaga sus necesidades empresariales y de cumplimiento normativo.

Usuarios
Los productos de Atlassian están diseñados para permitir tanto una colaboración abierta como una privada, según sea necesario. Por tanto, los usuarios deben asegurarse de otorgar a los empleados y los usuarios externos los permisos adecuados a sus aplicaciones y datos de Atlassian.

Información
Los usuarios y las aplicaciones que cuenten con los permisos adecuados podrán acceder a cualquier contenido que almacenen en Confluence Cloud, Jira Cloud, Trello y Bitbucket Cloud. Asegúrate de que tus productos e instancias de Atlassian estén configurados según la accesibilidad a la información que requiera el contenido.

Aplicaciones de Marketplace
Los desarrolladores de las aplicaciones de terceros de Atlassian Marketplace, que se verifican de forma independiente, **supervisan periódicamente las aplicaciones para detectar posibles vulnerabilidades**. Además, ahora cuentan con **Forge** , una plataforma en la nube que les permite crear aplicaciones empresariales con la misma seguridad excepcional que Atlassian ofrece para sus productos. Sin embargo, también te corresponde a ti evaluar los servicios de terceros con los que decidas trabajar, ya que deberás conceder a esas aplicaciones acceso a la información almacenada en tus productos de Atlassian.

Cumplimiento de las obligaciones globales de privacidad de datos

Al elegir utilizar una plataforma en la nube como Atlassian Cloud Enterprise, los administradores de TI pueden simplificar la tarea de supervisar y garantizar el cumplimiento normativo en toda tu pila de recursos tecnológicos.

Programa de privacidad

El programa de privacidad de Atlassian está diseñado para ofrecer a los clientes los estándares más estrictos de protección. Esto implica ir más allá de lo que exige la ley e incorporar la privacidad por diseño a todos los productos.

Los productos de Atlassian Cloud se ajustan a los estándares y las certificaciones de privacidad ampliamente aceptados. El personal de Atlassian que gestiona los datos de los clientes recibe formación periódica sobre protocolos de confidencialidad y seguridad para dar tranquilidad a los clientes de Atlassian mediante el control. Los administradores de la organización de los equipos de los clientes pueden gestionar con facilidad los perfiles de usuario final e, incluso, **facilitar la eliminación de las cuentas** de los usuarios que gestionan desde la consola de administración. Así, se eliminan sus datos personales de todas las organizaciones y sitios utilizados para acceder a Jira Cloud, Confluence Cloud, Bitbucket Cloud y Trello. Los usuarios finales no gestionados también pueden solicitar que se eliminen sus datos personales **iniciando una solicitud de eliminación de cuenta**.

A finales de cada año, Atlassian publica **un Informe de transparencia anual**, en el que se divulga abiertamente información sobre las solicitudes gubernamentales recibidas a lo largo de ese año y las respuestas ofrecidas a dichas solicitudes. Atlassian ofrece **transparencia** respecto a las solicitudes gubernamentales relacionadas con datos de usuarios, la eliminación de contenido o la suspensión de cuentas de usuarios. A la hora de ofrecer una respuesta a estas solicitudes, se siguen estrictos **procedimientos y políticas**. Para que Atlassian facilite información de los clientes, las autoridades legales deben seguir la diligencia judicial adecuada para el tipo de información solicitada, como una citación, una orden judicial o una orden de registro. Puedes obtener más información en el **Trust Center.**

CERTIFICACIONES ACTUALES

Los clientes de Atlassian presentan diversas necesidades de cumplimiento, por lo que sus productos se desarrollan de acuerdo con **las variadas normativas y regulaciones principales del sector**. En la actualidad, los productos de Atlassian cumplen con las siguientes normativas:

- Controles de sistemas y organizaciones (SOC) 2, SOC 3
- ISO/IEC 27001, ISO/IEC 27018
- Estándar de seguridad de datos en los sectores de tarjetas de pago (PCI DSS)
- Plantilla voluntaria de accesibilidad de productos (VPAT 508)
- RGPD

Compromiso con el RGPD

Los productos de Atlassian Cloud se diseñan de acuerdo con muchos estándares de seguridad y privacidad, que cumplen los requisitos del RGPD. Vamos a profundizar en el compromiso de Atlassian de ser líder en términos de privacidad y seguridad de los datos y, en consecuencia, en cómo sus productos cumplen los estándares del RGPD.

Transferencias internacionales de datos

En vista de la reciente resolución de la sentencia Schrems II, Atlassian proporciona un **Anexo sobre el tratamiento de datos** (DPA, por sus siglas en inglés) previamente firmado, que incluye una copia completa de las cláusulas contractuales tipo (SCC) y sirve como mecanismo válido para la transferencia legal de datos personales a productos de Atlassian Cloud fuera del Espacio Económico Europeo. Este anexo contiene disposiciones específicas para ayudar a los clientes a cumplir con el RGPD. Además, de acuerdo con **las directrices del RGPD**, Atlassian seguirá invirtiendo en funciones de cifrado avanzadas como BYOK para proteger los datos personales.

Consentimiento y derechos de privacidad individuales

Con el fin de cumplir las estipulaciones del RGPD relativas al derecho al olvido de las personas, Atlassian facilita a los administradores el proceso de eliminar los datos personales de los usuarios de los productos de Atlassian Cloud. Tanto los usuarios finales gestionados como los no gestionados pueden solicitar que se eliminen sus datos personales y los administradores de la organización pueden **facilitar la eliminación de las cuentas** a través del portal de administración de Atlassian.

Elección y consentimiento

A los usuarios finales de la UE se les ofrece transparencia y posibilidad de elección respecto al uso que Atlassian hace de su información, mostrando el consentimiento para las cookies y los mensajes de marketing en todos los puntos de recopilación. Esto permite a los usuarios comprender exactamente la forma en que se recopila y utiliza su información, lo que les da la posibilidad de elegir cómo compartirla con Atlassian.

Datos de clientes y terceros

Atlassian trabaja con subcontratistas externos para proporcionar sitios web, desarrollo de aplicaciones, alojamiento, mantenimiento, copias de seguridad, almacenamiento, infraestructura virtual, procesamiento de pagos, análisis y otros servicios. Con el fin de proporcionar dichos servicios, estos proveedores pueden tener acceso a la información de identificación personal (PII) o procesarla.

Atlassian pone en conocimiento de sus clientes cualquier uso o procesamiento que haga cualquier subcontratista de su información de identificación personal, mediante notificación y antes de que se produzca dicho procesamiento. En la página **Encargados del tratamiento de los datos personales subcontratados de Atlassian, se proporciona una lista de los subcontratistas con los que trabaja Atlassian. Puedes suscribirte a una fuente RSS para recibir una notificación cada vez que se añada un encargado del tratamiento de los datos personales subcontratados de Atlassian nuevo.**

Cumplimiento normativo en los trabajos

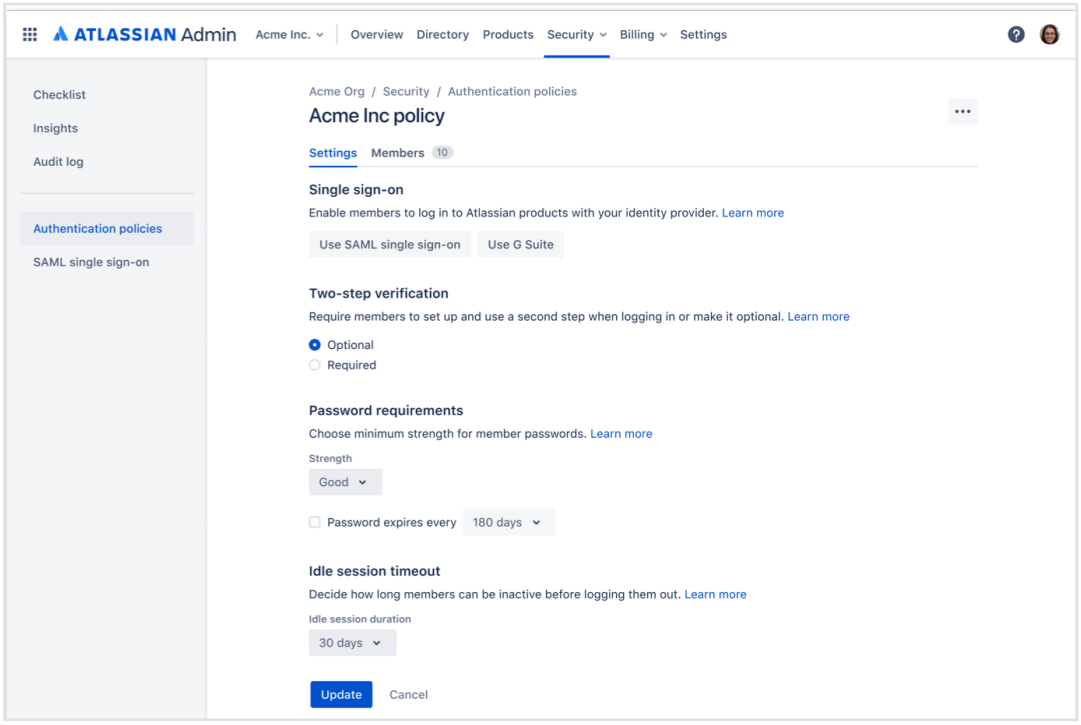
Para ofrecer mejor atención a los clientes de sectores regulados, Atlassian sigue invirtiendo en satisfacer las necesidades de cumplimiento específicas del sector. A mediados de 2022, se espera que Atlassian Cloud Enterprise cumpla con las **normativas del sector de servicios financieros** de Estados Unidos, Alemania (Autoridad Federal de Supervisión Financiera o BaFin, por sus siglas en alemán) y Australia (Autoridad Australiana de Regulación Prudencial). Respecto a las empresas sanitarias estadounidenses, nuestro objetivo es cumplir la **Ley de portabilidad y responsabilidad del seguro de salud (HIPAA, por sus siglas en inglés)** en Jira Software Cloud y Confluence Cloud también a mediados de 2022.

Gestión integrada de accesos e identidades

Aunque tu organización cumpla con las normativas del sector y te hayas asegurado de que todos los datos de los clientes estén cifrados, la seguridad de tu empresa estará en manos del empleado más vulnerable. Según **Kaspersky**, el 52 % de las filtraciones de datos empresariales en 2019 se debieron al mal uso de los recursos de TI por parte de los empleados. Por eso, Atlassian proporciona a tus administradores un amplio conjunto de controles integrados para garantizar un acceso seguro en toda la organización mientras se utilizan sus productos de Cloud.

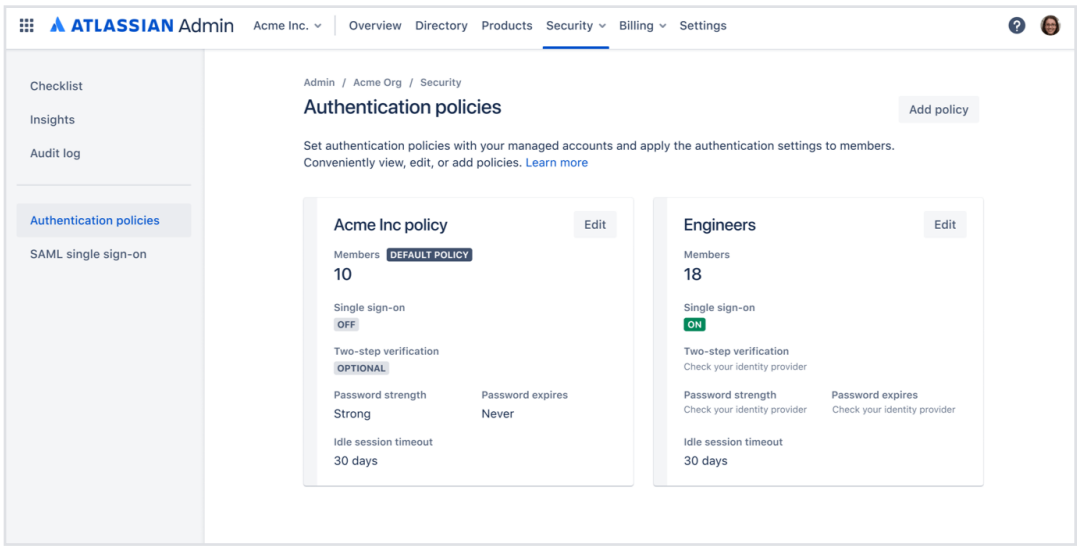
Protocolos de autenticación de nivel empresarial

Atlassian permite a las organizaciones reducir sus riesgos de seguridad mediante la implementación de protocolos de autenticación de nivel empresarial en sus productos de Atlassian. Con Atlassian Access, el centro de seguridad y administración que se incluye con el plan Enterprise de Cloud sin ningún coste adicional, los administradores pueden configurar el inicio de sesión único de SAML utilizando el proveedor de identidades con el que cuente su empresa, lo que permite a los empleados acceder a varios productos e instancias de Atlassian con un único conjunto de credenciales seguro. Los administradores también pueden **aplicar la autenticación en dos pasos** para obtener una capa adicional de seguridad solicitando a los usuarios que introduzcan un código de seis dígitos que se envía a su teléfono al iniciar sesión. Entre los controles adicionales se incluyen exigir un mínimo de seguridad en las contraseñas de los usuarios, forzar la caducidad de las contraseñas después de un tiempo determinado y cerrar automáticamente las sesiones inactivas de los usuarios después de cierto tiempo.



Políticas de autenticación personalizables

En lugar de aplicar un enfoque único, los administradores pueden personalizar las políticas de autenticación según se requiera para ajustarlas a diferentes subconjuntos de usuarios. Por ejemplo, pueden configurar una política de contraseñas predeterminada para todos los usuarios, pero hacer que la autenticación en varias fases sea obligatoria para un subconjunto de usuarios que acceda a una instancia de producto con datos extremadamente confidenciales.



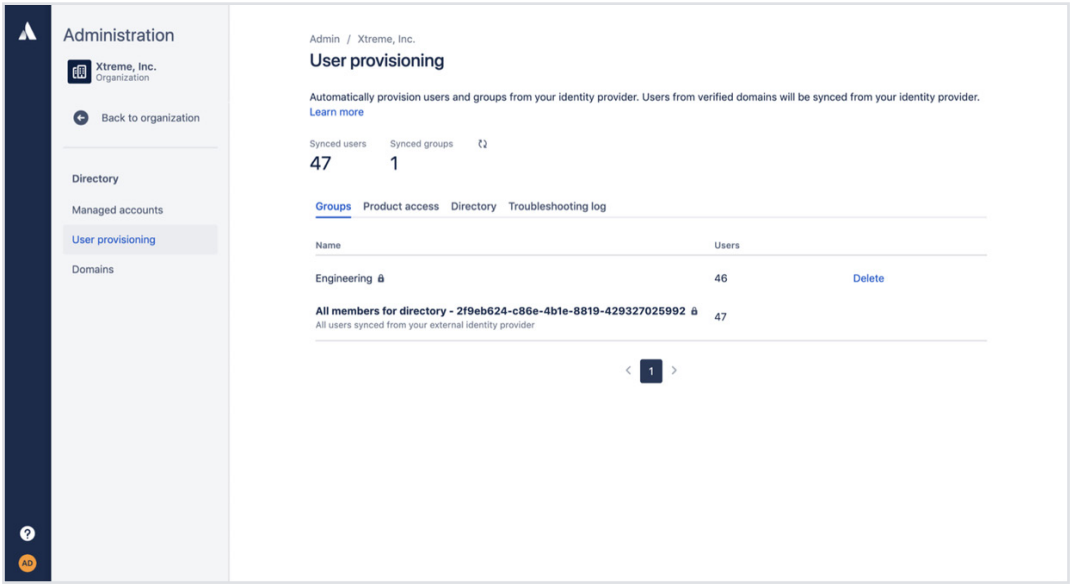
Gestión de dispositivos y aplicaciones móviles

Con el aumento de las prácticas de teletrabajo y de la política de usar dispositivos personales para trabajar (Bring-Your-Own-Device, BYOD), muchos usuarios acceden a los productos de Atlassian a través de aplicaciones móviles. Para evitar filtraciones de datos o accesos no autorizados de aplicaciones móviles, ahora los administradores pueden aplicar protocolos de seguridad específicos, como restringir las funciones de copiar y pegar, bloquear las capturas de pantalla o requerir autenticación biométrica, FaceID o TouchID al iniciar sesión. Atlassian admite actualmente la integración incorporada con el software líder de gestión de dispositivos móviles (MDM) para aplicar los protocolos de seguridad para la familia de productos Jira, Confluence y las aplicaciones móviles de Trello utilizadas en dispositivos gestionados por la empresa. Hacia julio de 2021, Atlassian planea ampliar la compatibilidad con la gestión de aplicaciones móviles, que permitirá a los administradores configurar políticas de seguridad móvil a través de la **consola de administración de la organización** tanto para dispositivos gestionados como para BYOD.

Aprovisionamiento y desaprovisionamiento automático de usuarios

Según **Osterman Research**, un 89 % de los antiguos empleados todavía pueden acceder, como mínimo, a una aplicación de su antiguo trabajo después de haberlo dejado. De hecho, casi un tercio de estos antiguos empleados ha utilizado su acceso para ver la información de la empresa, y uno de cada 16 ha compartido dicha información de manera externa. En el caso de las grandes empresas, no es de extrañar que se pasen por alto las bajas de algunos empleados, pero esto no deja de ser un aspecto importante para garantizar la seguridad de la nube.

Para resolver este problema, Atlassian Access ofrece la capacidad de automatizar el proceso de aprovisionamiento y desaprovisionamiento de usuarios. Access puede sincronizarse con el **directorio de usuarios de la empresa** , bien a través de las integraciones actuales de Atlassian con los principales proveedores de identidades, bien a través de la API del sistema de gestión de identidades entre dominios (SCIM) para integraciones personalizadas, de modo que se conceda automáticamente acceso a los usuarios cuando se unen al equipo. En función del grupo de tu directorio de usuarios al que se añada un empleado (ya sea ingeniería, recursos humanos o marketing), se le concederá automáticamente acceso al conjunto de herramientas de Atlassian que precisa su equipo. Así, si cambia de equipo, sus permisos también cambiarán y, si deja la empresa, se le revocará el acceso a todas las herramientas.



Cómo Canva ha sacado partido de las funciones de seguridad de Atlassian para satisfacer sus necesidades

La plataforma de diseño Canva ha ampliado su plantilla hasta llegar a contar con más de 1000 empleados en todo el mundo, para lo que ha confiado en las funciones de Atlassian Cloud a fin de garantizar la seguridad de sus aplicaciones en la nube y, al mismo tiempo, proporcionar a los empleados la flexibilidad que necesitan. Todos los empleados de la organización utilizan tanto Jira Software como Confluence para llevar a cabo su trabajo, así como las funciones de Atlassian Access, que han permitido a Canva restringir fácilmente el acceso a diferentes instancias de productos (como la instancia del equipo de RR. HH. de Jira Service Management) y gestionar la configuración de seguridad de los empleados.

“Los que tienen acceso a la información de RR. HH. están muy controlados, y también se han implementado unas fuertes medidas de seguridad”, explica Jeff Lai, experto en infraestructura interna de Canva. “Si no fuera por ese alto nivel de seguridad, no habríamos estado dispuestos a publicar este tipo de información en Jira Service Management”, añade.

Canva también utiliza la función de aprovisionamiento y desaprovisionamiento automatizados de usuarios que ofrece Atlassian Access para conceder acceso de forma sencilla a los nuevos empleados a los sistemas y documentos de la empresa. Por otro lado, la empresa recurre el proveedor de identidades externo Okta para sincronizar datos con Access y otorga permisos a los nuevos empleados para visualizar una cantidad restringida del contenido de Canva antes de su primer día. Mediante el SSO de Access y la verificación obligatoria en dos pasos, los contratistas externos también pueden acceder a un conjunto limitado de los sistemas de Canva.

“No pueden ver nada, excepto los documentos que les enviamos, ya que el acceso está restringido y solo se permite a aquellos que están asignados a un grupo de usuarios. Todos los empleados de la empresa tienen acceso al historial de cambios, lo que supone otra capa de seguridad que permite asegurarnos de que nadie toque los documentos que no debe”, afirma Lai.

Supervisión y prevención proactivas de amenazas

Aunque se tomen fuertes medidas de seguridad, se producen amenazas, razón por la cual Atlassian ha adoptado un enfoque versátil que evoluciona constantemente respecto a la prevención de amenazas y la gestión de vulnerabilidades. Atlassian utiliza tanto procesos automatizados como manuales para buscar, supervisar y corregir vulnerabilidades en todos los productos de Cloud, lo cual se ha ampliado para dotar a los equipos de TI de los clientes de Atlassian de herramientas similares.

Programa de recompensas por errores

El programa de recompensas por errores de Atlassian alienta a más de 60 000 investigadores de ciberseguridad a realizar técnicas de “hacking ético” en los productos de Atlassian y marcar cualquier vulnerabilidad que detecten. Si se registra una vulnerabilidad, se creará un ticket y se asignará al propietario del sistema o al equipo de ingeniería responsable del producto.

Pruebas uniformes de productos

Como parte de la canalización de integración e implementación continuas (CI/CD) de Atlassian, los ingenieros deben ejecutar un proceso exhaustivo de análisis de seguridad de cualquier contenedor implementado en entornos de desarrollo, ensayo o producción.

Si se realizan cambios en el código existente, los ingenieros de Atlassian llevarán a cabo un proceso de “Revisión por compañeros, compilación correcta” para garantizar que los cambios no causen ningún problema. En el marco de este proceso, al menos un compañero debe revisar cualquier cambio de código antes de enviarlo.

Dado que muchos de los productos de Atlassian también utilizan bibliotecas de código abierto, se emplea una combinación de herramientas empresariales, creadas internamente y de código abierto para escanear e identificar automáticamente cualquier dependencia que exista dentro de dichas bibliotecas y que pueda estar vinculada a vulnerabilidades de seguridad.

Detección proactiva de seguridad

Ante la constante evolución de las amenazas de ciberseguridad, Atlassian lleva a cabo búsquedas programadas y proactivas de cualquier actividad maliciosa, para lo que emplea la plataforma de gestión de incidentes de seguridad y eventos. El equipo de inteligencia de seguridad de Atlassian realiza búsquedas de forma periódica (o, como Atlassian las denomina, "detecciones") de cualquier actividad dirigida a Atlassian o a sus clientes.

De esta forma, todas las amenazas que se detectan se registran, investigan y utilizan para mejorar la capacidad de detección de amenazas en el futuro. El equipo de inteligencia de seguridad diseña constantemente detecciones nuevas que permitan buscar de forma más eficaz amenazas nuevas y existentes, lo que ayuda a Atlassian a entender mejor el panorama actual y futuro de las amenazas.

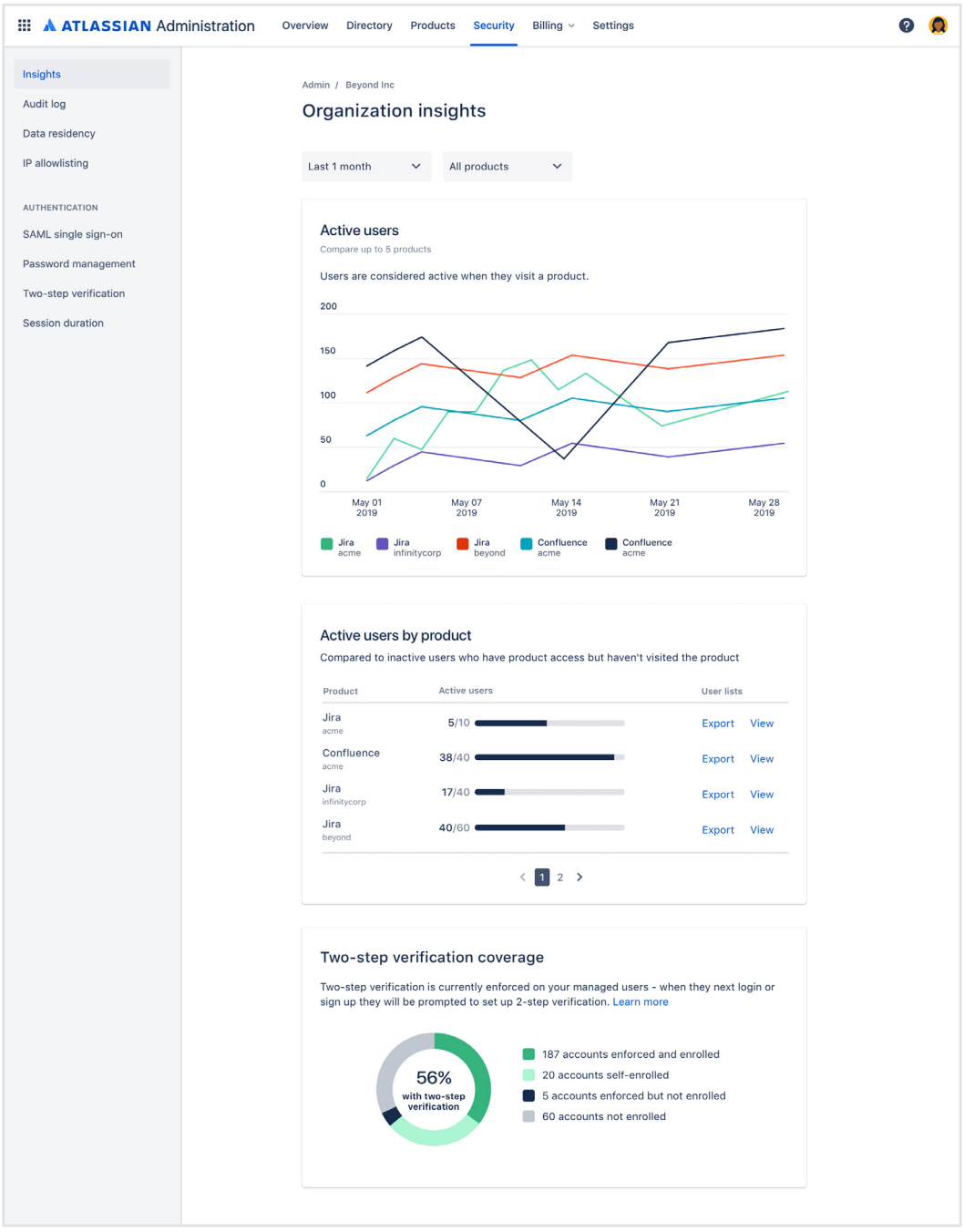
Información sobre seguridad para administradores

Atlassian ha supervisado de manera proactiva sus sistemas en busca de amenazas y vulnerabilidades, y quiere capacitar a sus clientes para que hagan lo propio, por lo que ha facilitado a los administradores el seguimiento de posibles incidencias de seguridad en sus productos de Atlassian.

El registro de auditoría de una organización de Atlassian Access funciona como un registro completo de cualquier actividad de administración que tenga lugar en la organización de Atlassian Cloud. Los administradores de la organización pueden llevar un seguimiento exacto de las instancias de productos a las que tiene acceso cada administrador del sitio, además del momento en que se le concedió dicho acceso. En caso de pérdida de datos, como la pérdida de datos sujetos a derechos de propiedad o información confidencial, los administradores pueden restringir el acceso de los usuarios según sea necesario y ver los registros de la actividad de los usuarios para identificar cualquier actividad sospechosa.

> Disponemos de mucha información extremadamente confidencial relacionada con nuestra propiedad intelectual... y nos preocupa su protección. El equipo de nuestro director de Seguridad de la Información debe saber quién tiene acceso a ella y cómo la utiliza. Atlassian Access garantiza que las personas adecuadas tengan acceso a los recursos adecuados y que las personas equivocadas no tengan acceso a los recursos equivocados.
>
> **JIM TOMPKINS**
>
> **Responsable de programas, Rockwell Automation, cliente de Atlassian Enterprise**

En Atlassian Access también se incluye la herramienta de información de la organización, que permite a los administradores obtener una visión general del nivel de seguridad con el que cuentan los usuarios en los productos de Atlassian. Mediante la información de la organización, los administradores pueden realizar un seguimiento del número de usuarios gestionados que tienen habilitado el inicio de sesión único de SAML o la verificación en dos pasos en sus cuentas. Además, pueden ver los usuarios que están activos diaria y mensualmente en un producto, de modo que pueden comprender mejor qué usuarios necesitan realmente acceso y permisos.



Escalado seguro en la nube con Atlassian

La seguridad se integra en el ADN de todos los productos de Atlassian Cloud, al igual que prácticas y procesos seguros. Atlassian Cloud Enterprise ofrece una solución de eficacia probada para empresas que requieren una plataforma segura, conforme a las normativas y centrada en la privacidad, que les permita escalar y les proporcione lo siguiente:

- Compatibilidad con residencia de los datos
- Cifrado en tránsito y en reposo
- Cumplimiento de las principales normativas del sector: SOC, ISO, RGPD y muchas más
- Todas las funciones de seguridad de Atlassian Access están incluidas sin ningún coste adicional, como el inicio de sesión único de SAML, la verificación obligatoria en dos pasos, políticas de autenticación personalizadas, aprovisionamiento y desaprovisionamiento automatizados de usuarios, registros de auditoría de la organización, información de la organización y mucho más
- SLA de 30 minutos para incidencias de seguridad críticas
- Soporte telefónico ininterrumpido con un equipo altamente especializado

Obtén más información sobre cómo puede lograr tu negocio una seguridad de nivel empresarial con Atlassian Cloud.

Ponte en contacto con tu Solution Partner hoy mismo.

ATLASSIAN