

The Forrester Wave™: Identidad del cliente y gestión del acceso, Q4 2020

Los 13 proveedores que más importan y cómo se calculan

Por Andras Cser

8 de Octubre, 2020

¿Porque leer este artículo?

En nuestra evaluación de 32 criterios de la identidad del cliente y los proveedores de gestión de acceso (CIAM), identificamos a los 13 proveedores más significativos - Akamai, Auth0, ForgeRock, IBM, LoginRadius, Microsoft, Okta, OpenText, Optimal IdM, Ping Identity, Salesforce, SAP, y WSO2 - e investigado, analizando, y las anotando. Este informe muestra cómo cada proveedor da la talla y ayuda a los profesionales de la seguridad y el riesgo (S&R) a seleccionar el más adecuado para sus necesidades.

Conclusiones clave

ForgeRock, IBM y SAP lideran el paquete la investigación de Forrester descubrió un mercado en qué ForgeRock, IBM y SAP son líderes; Ping Identity, WSO2, Okta, Salesforce y Auth0 son de alto rendimiento; y LoginRadius, Microsoft, Akamai, OpenText y Optimal IdM son contendientes.

Gestión de consentimiento, verificación de identidad, y la escalabilidad son diferenciadores clave

A medida que las soluciones CIAM más antiguas se vuelven menos efectivas para cumplir con la seguridad y la privacidad de la rápida evolución, requisitos de adquisición de clientes digitales y procesos de retención, proveedores que pueden proporcionar una gestión integral del consentimiento, integración productiva con verificación de identidad, y la escalabilidad se posicionan para ofrecer gestión de usuarios agradable, sin fricciones, tiempo de generación de valor acelerado para los clientes y triunfar en este mercado.

The Forrester Wave™: Identidad del cliente y gestión del acceso, Q4 2020

Los 13 proveedores que más importan y cómo se calculan



Por [Andras Cser](#)
Con [Merritt Maxim](#) y Benjamin Corey
8 de Octubre del 2020

Tabla de contenido

- 2 CIAM Converge seguridad y usuario de administración
- 3 Resumen de evaluación
- 9 ofertas de proveedores
- 9 perfiles de proveedores
- Lideres
- Fuertes artistas
- Contendientes
- 15 Resumen de la evaluación
- Criterios de inclusión de proveedores
- 16 Material suplementario

Documentos de investigación relacionados

[The forrester Customer-Obsessed identity And Access Management Operating Model](#)

[The forrester Wave™: risk-Based Authentication, Q2 2020](#)

[Transform your iAM strategy To succeed in The Post-Pandemic era](#)



Comparta informes con sus colegas. Mejore su membresía con cuota de investigación.

CIAM Converte seguridad y administración de usuarios

El mercado CIAM ha experimentado cambios importantes en los últimos dos años, CIAM ya no es solo una extensión de las capacidades generales de IAM, y la mayoría de los proveedores de IAM empresariales ahora ofrecen CIAM dedicando soluciones. Los proveedores con experiencia en IAM, como IBM, Okta y Ping Identity, se han integrado a plataformas para sistemas comerciales como CRM, análisis web y gestión de privacidad en soluciones CIAM. Al mismo tiempo, proveedores como Akamai y SAP con más gestión de usuarios de clientes antecedentes han expandido las integraciones de sistemas empresariales y han agregado capacidades de seguridad como aprovisionamiento, autenticación y autorización para sus soluciones.

Como resultado de estas tendencias, los clientes de CIAM deben buscar proveedores que:

› **Habilite la gestión del consentimiento y la privacidad del cliente sin problemas y sin problemas.**

Como regional y las regulaciones de privacidad globales se multiplican, la tarea de los profesionales de S&R es administrar la privacidad y el consentimiento del usuario a los términos y condiciones (TyC) mientras se mantienen experiencias de seguridad agradables para el cliente, se obtienen de manera más compleja. Como resultado, los clientes de Forrester demandan cada vez más soluciones CIAM con sistemas nativos e integrados. gestión de consentimiento. La gestión del consentimiento debe ir más allá del uso de un usuario, cliente, arbitrario Atributo de tienda para indicar qué versión de un acuerdo de usuario aceptó el cliente, en su lugar proporcionando la capacidad de administrar múltiples versiones de acuerdos y generar informes granulares sobre aceptación del usuario de los TyC.

› **Integre con soluciones de verificación de identidad (IDV).** En tiempos (post) pandémicos, el cliente digital, la adquisición, incorporación y retención son más críticas que nunca. Para apoyar sin rostro en línea enfoques, las soluciones CIAM deben ofrecer una integración productiva con documentos físicos soluciones de verificación como Onfido y Mitek; Soluciones IDV como Equifax, Experian, GBG, LexisNexis y TransUnion según los encabezados de los archivos de crédito; y soluciones de IDV sociales como código e id.me. Extraer datos de fuentes de inteligencia de amenazas internas o de terceros para suministrar contexto y refinar aún más la evaluación de riesgos del cliente durante la incorporación también reduce la fricción del cliente y del trabajo de investigación.

› **Escale a un gran número de usuarios tanto en tecnología como en precio.** Incluso las pequeñas empresas tienen enormes poblaciones de usuarios de clientes que requieren gestión y autenticación digital; empresas de medios son un gran ejemplo. Los clientes buscan un proveedor CIAM con un historial probado de servicio a decenas de millones de clientes con su solución CIAM; también quieren que los proveedores proporcionen guías de tamaño y Garantías de rendimiento bajo cargas máximas, incluidos tiempos de respuesta documentados para nuevos usuarios. procedimientos de registro, autoservicio de usuario e inicio de sesión. Los proveedores de CIAM deben ofrecer precios basados en volúmenes de transacciones, número de usuarios activos y número total de usuarios (activos e inactivos).¹

Resumen de la evaluación

La evaluación de Forrester Wave™ destaca a los líderes, los artistas fuertes, los contendientes y los retadores. es una evaluación de los principales proveedores del mercado y no representa todo el panorama de proveedores. encontrará más información sobre este mercado en nuestros informes sobre CIAM.

Pretendemos que esta evaluación sea solo un punto de partida y alentamos a los clientes a ver las evaluaciones de productos y adaptar las ponderaciones de los criterios utilizando la herramienta de comparación de proveedores basada en Excel (ver figura 1 y ver figura 2). Haga clic en el enlace al comienzo de este informe en forrester.com para descargar la herramienta.

Figura 1 Forrester Wave™: Identidad del cliente y gestión del acceso, Q4 2020

THE FORRESTER WAVE™

Identidad del cliente y gestión del acceso

Q4 2020

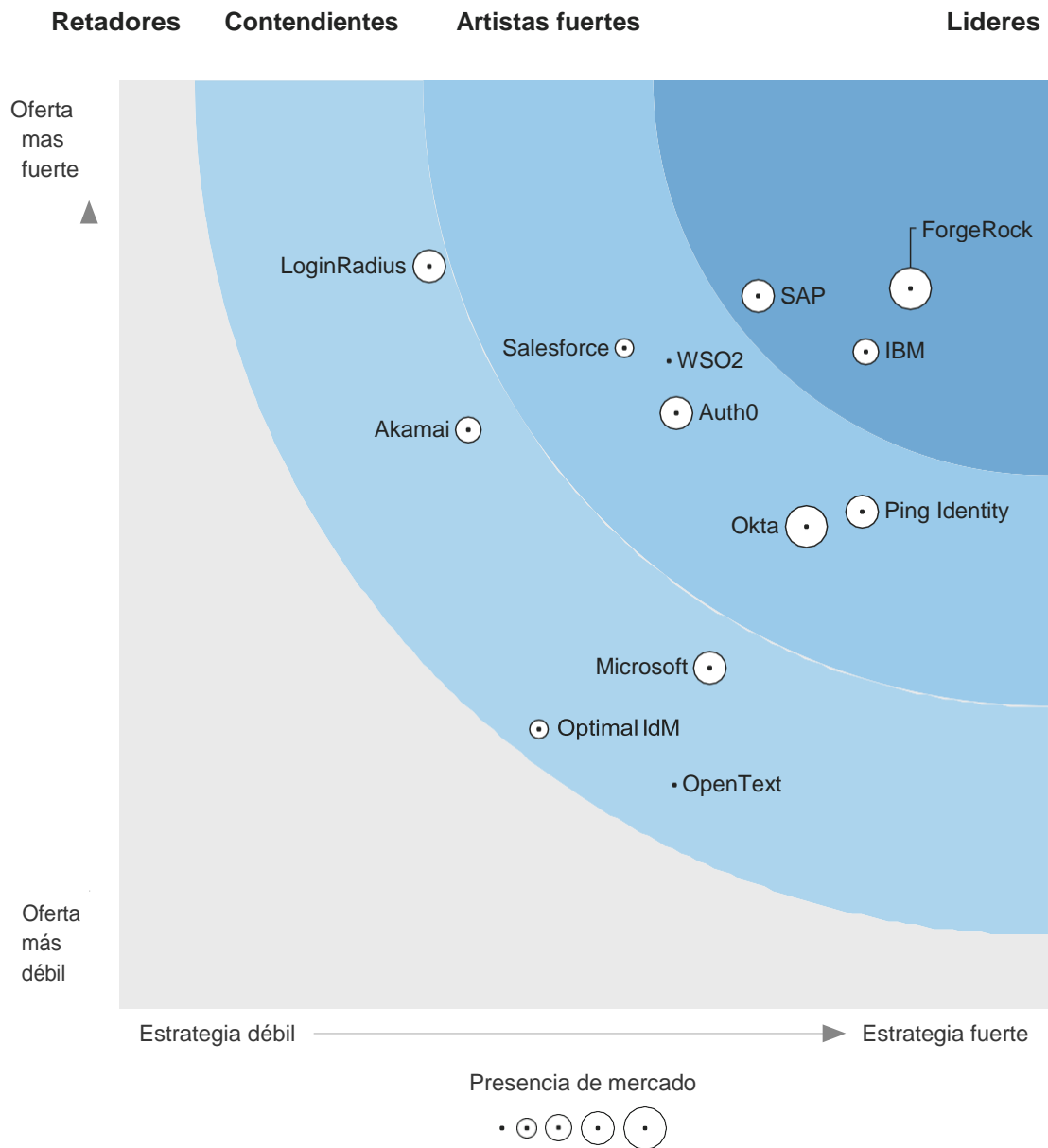


Figura 2 Forrester Wave™: Identidad del cliente y gestión del acceso, Q4 2020

	Forrester ponderación	Akamai	Auth0	ForgeRock	IBM	LoginRadius	Microsoft	Okta
Oferta actual	50%	3.12	3.21	3.88	3.54	4.00	1.84	2.60
Orquestación de datos y gestión de usuarios	8%	1.00	3.00	5.00	3.00	5.00	1.00	3.00
Verificación de la identidad del cliente y registro	8%	3.00	3.00	5.00	1.00	3.00	1.00	5.00
Privacidad, gestión de consentimiento y perfilado	7%	5.00	3.00	3.00	3.00	5.00	1.00	1.00
Autenticación del cliente	7%	1.00	1.00	3.00	5.00	3.00	1.00	5.00
Autoservicio al cliente	7%	3.00	1.00	5.00	1.00	3.00	1.00	1.00
Integración de sistemas empresariales	7%	1.00	5.00	5.00	3.00	3.00	3.00	3.00
Sistemas de gestión de IDV y fraude de integración	7%	3.00	3.00	5.00	5.00	1.00	3.00	1.00
Informes y paneles	7%	5.00	0.00	3.00	5.00	3.00	1.00	1.00
Usuarios activos	7%	5.00	5.00	1.00	3.00	5.00	3.00	3.00
Número de marcas	7%	5.00	3.00	5.00	3.00	5.00	1.00	1.00
Intentos de autenticación por hora	7%	5.00	5.00	5.00	3.00	5.00	1.00	1.00
Conformidad	7%	3.00	5.00	3.00	5.00	5.00	5.00	5.00
Navegación y entorno integrado	7%	3.00	3.00	5.00	5.00	5.00	3.00	3.00
Documentación estática y contextual	7%	1.00	5.00	1.00	5.00	5.00	1.00	3.00

Todos los puntajes se basan en una escala de 0 (débil) a 5 (fuerte).

The Forrester Wave™: Identidad del cliente y gestión del acceso, Q4 2020

Los 13 proveedores que más importan y como se calculan

FIGURE 2 forrester Wave™: Customer identity And Access Management scorecard, Q4 2020 (Cont.)

Estrategia	Forrester Ponderación	Proveedores						
		Akamai	Auth0	ForgeRock	IBM	LoginRadius	Microsoft	Okta
	50%	1.88	3.00	4.26	4.02	1.67	3.18	3.70
Hoja de ruta de ejecución Empleados	7%	3.00	3.00	5.00	3.00	1.00	5.00	3.00
Empleados	1%	3.00	3.00	1.00	5.00	1.00	5.00	3.00
Desarrolladores	7%	1.00	5.00	5.00	3.00	3.00	3.00	5.00
Ventas	7%	5.00	3.00	3.00	3.00	1.00	5.00	5.00
Inversión en R&D	7%	1.00	5.00	5.00	5.00	5.00	3.00	3.00
Orquestación de datos, flujos de trabajo y usuario de administración	7%	1.00	3.00	5.00	1.00	1.00	1.00	5.00
Verificación y riesgo de identidad	7%	1.00	3.00	5.00	3.00	0.00	1.00	3.00
Identidad descentralizada/autónoma	7%	1.00	1.00	3.00	5.00	1.00	5.00	1.00
Privacidad, gestión de consentimiento y perfilado	7%	3.00	3.00	5.00	5.00	0.00	1.00	3.00
Planes de autenticación	7%	3.00	3.00	5.00	3.00	1.00	1.00	5.00
Análisis de identidad y fuentes de amenazas	7%	1.00	3.00	5.00	5.00	0.00	3.00	5.00
Integración de sistemas empresariales	7%	3.00	3.00	1.00	5.00	3.00	3.00	5.00
Ingenieros de soporte	7%	1.00	3.00	5.00	5.00	1.00	5.00	5.00
Servicios profesionales	7%	1.00	1.00	5.00	5.00	1.00	5.00	3.00
Ecosistema de socios	1%	3.00	3.00	5.00	5.00	5.00	5.00	3.00
Modelo de socios	7%	1.00	3.00	3.00	5.00	5.00	3.00	1.00
Presencia del mercado	0%	3.00	3.50	4.50	3.00	3.50	3.50	5.00
CIAM Ingresos por suscripción	50%	3.00	3.00	4.00	5.00	2.00	3.00	5.00
CIAM Crecimiento de ingresos	50%	3.00	4.00	5.00	1.00	5.00	4.00	5.00

Todos los puntajes se basan en una escala de 0 (débil) a 5 (fuerte).

The Forrester Wave™: Identidad del cliente y gestión del acceso, Q4 2020

Los 13 proveedores que más importan y como se calculan

FIGURE 2 forrester Wave™: Customer identity And Access Management scorecard, Q4 2020 (Cont.)

		Forrester ponderación	OpenText	Optimal IdM	Ping Identity	Salesforce	SAP	WSO2
Oferta actual		50%	1.21	1.51	2.68	3.56	3.84	3.49
Orquestación de datos y gestión de usuarios	8%	1.00	3.00	1.00	3.00	3.00	5.00	
Verificación de la identidad del cliente y registro	8%	1.00	1.00	1.00	3.00	3.00	1.00	
Privacidad, gestión de consentimiento y perfilado	7%	1.00	0.00	1.00	5.00	5.00	5.00	
Autenticación de clientes	7%	1.00	3.00	5.00	1.00	3.00	5.00	
Autoservicio al cliente	7%	1.00	5.00	3.00	3.00	5.00	5.00	
Integración de sistemas empresariales	7%	0.00	1.00	1.00	5.00	3.00	5.00	
Sistemas de gestión IDV y fraude	7%	0.00	0.00	5.00	5.00	3.00	1.00	
Sistemas de gestión IDV y fraude integración	7%	1.00	1.00	1.00	5.00	3.00	5.00	
Informes y paneles	7%	1.00	1.00	5.00	3.00	5.00	0.00	
Usuarios activos	7%	5.00	0.00	5.00	3.00	5.00	5.00	
Número de marcas	7%	1.00	1.00	5.00	3.00	5.00	3.00	
Intentos de autenticación por hora	7%	1.00	1.00	1.00	5.00	3.00	1.00	
Conformidad	7%	3.00	3.00	1.00	3.00	5.00	3.00	
Navegación y entorno integrado	7%	0.00	1.00	3.00	3.00	3.00	5.00	

Todos los puntajes se basan en una escala de 0 (débil) a 5 (fuerte).

The Forrester Wave™: Identidad del cliente y gestión del acceso, Q4 2020

Los 13 proveedores que más importan y como se calculan

FIGURE 2 forrester Wave™: Customer identity And Access Management scorecard, Q4 2020 (Cont.)

		Forrester Ponderación	OpenText	Optimal IdM	Ping Identity	Salesforce	SAP	WSO2
Estrategia		50%	2.99	2.26	4.00	2.72	3.44	2.96
Hoja de ruta de ejecución Empleados	7%	5.00	5.00	5.00	5.00	3.00	3.00	
Empleados	1%	5.00	1.00	3.00	5.00	5.00	1.00	
Desarrolladores	7%	3.00	1.00	5.00	1.00	5.00	1.00	
Ventas	7%	3.00	1.00	5.00	1.00	5.00	1.00	
Inversión en R&D	7%	1.00	5.00	3.00	1.00	1.00	3.00	
Orquestación de datos, flujos de trabajo y usuario de administración	7%	3.00	5.00	5.00	3.00	5.00	5.00	
Verificación y riesgo de identidad	7%	1.00	3.00	5.00	1.00	3.00	3.00	
Identidad descentralizada/autónoma	7%	3.00	1.00	5.00	3.00	5.00	3.00	
Privacidad, gestión de consentimiento y perfilado	7%	5.00	3.00	1.00	3.00	5.00	3.00	
Planes de autenticación	7%	1.00	1.00	3.00	3.00	3.00	5.00	
Análisis de identidad y fuentes de amenazas	7%	1.00	1.00	3.00	3.00	5.00	3.00	
Integración de sistemas empresariales	7%	5.00	1.00	3.00	3.00	1.00	3.00	
Ingenieros de soporte	7%	5.00	1.00	5.00	3.00	3.00	3.00	
Servicios profesionales	1%	0.00	1.00	5.00	1.00	3.00	1.00	
Ecosistema de socios	7%	1.00	3.00	3.00	5.00	1.00	5.00	
Modelo de socios	7%	1.00	3.00	3.00	5.00	1.00	5.00	
Presencia del mercado	0%	1.00	1.50	3.50	2.00	4.00	1.00	
CIAM Ingresos por suscripción	50%	1.00	1.00	4.00	2.00	5.00	1.00	
CIAM Crecimiento de ingresos	50%	1.00	2.00	3.00	2.00	3.00	1.00	

Todos los puntajes se basan en una escala de 0 (débil) a 5 (fuerte).

Ofertas de proveedores

Forrester incluyó a los 13 proveedores en esta evaluación: Akamai, Auth0, ForgeRock, IBM, LogonRadius, Microsoft, Okta, OpenText, Optimal IdM, Ping Identity, Salesforce, SAP y WSO2.

Perfiles de proveedores

Nuestro análisis descubrió las siguientes fortalezas y debilidades de los proveedores individuales.

Lideres:

- › **ForgeRock aprovecha nuevos fondos para reenfocarse en CIAM:** Tradicionalmente un IAM local plataforma de software, ForgeRock ha abandonado en gran medida el modelo de negocio de código abierto relacionado con el soporte y ahora genera ingresos a partir de ofertas de IAM comerciales basadas en suscripción, como su nube Plataforma CIAM. Forrester estima que la empresa genera dos tercios de sus ingresos anuales de su solución CIAM. ForgeRock planea mejorar la personalización del usuario mediante el autoservicio de árboles de flujo de trabajo, simplificación de la autenticación al extender FIDO2 Web Authn al inicio de sesión sin nombre de usuario, y introducir análisis de comportamiento para autenticación y autorización.

La solución tiene un potente flujo de trabajo y una abstracción de políticas denominada Árboles que permite a los administradores crear flujos de trabajo modulares, personalizados, sin código o con código bajo para todos los casos de uso de CIAM, incluidos registro, autenticación y autoservicio. Asignación de datos de almacenes de usuarios existentes a la solución es fácil. Admite registros sin contraseña en una etapa temprana, listos para usar; inicio de sesión único (SSO) y los flujos de validación son muy amplios y flexibles. Sin embargo, la gestión del consentimiento de la solución y el control de versiones son más complejos de configurar que los de otros proveedores. La solución incluye integraciones seleccionables de autenticación multifactorial (MFA) de terceros; los clientes informan que escribiendo Los informes personalizados ad hoc requieren la creación de consultas SQL.2 No admite listas de control de acceso para definir quién puede ver qué informe. La solución es ideal para empresas que tienen muchas aplicaciones orientadas al cliente con requisitos complejos de autenticación y flujo de trabajo y para aquellas con habilidades establecidas de IAM o CIAM

- › **IBM tiene un compromiso renovado con CIAM.** El liderazgo intelectual de IBM en IAM ha disminuido y fluyó en los últimos años, pero la empresa ha renovado su cartera CIAM y ha creado una oferta de CIAM denominada IBM Security Verify. IBM integró con éxito su Trusteer basado en riesgos de solución de autenticación y gestión de fraude web con su cartera CIAM para crear Security Verify. El proveedor planea implementar una evaluación de riesgos continua para aplicaciones móviles y web nativas, Implementar un proceso de gestión de flujo de trabajo de confianza progresivo y brindar soporte al desarrollador y a la privacidad de experiencias en la plataforma.

La solución admite una amplia gama de protocolos de autenticación, FIDO2 y datos biométricos y se integra con la solución de inteligencia empresarial Tableau. Integración con Trusteer y terceros Las soluciones de verificación de identidad y gestión de fraudes están por delante de la competencia, al igual que los informes y tablero. Sin embargo, los clientes informan sobre desafíos con los flujos de trabajo de integración de datos y el control de acceso basado en roles para administradores; las invitaciones para el registro también se retrasan. Gestión de consentimiento y la elaboración de perfiles progresivos son rudimentarios.³ Autoservicio de cliente listo para usar (identificación de usuario olvidada recuperación, cancelación de registro de usuario y actualizaciones de perfil) y registro de gestión de datos maestros (MDM) también se quedan atrás. La solución es ideal para empresas que necesitan combinar la autenticación basada en riesgos con CIAM o renovar una cartera de gestión de fraude web o IAM existente de IBM.

- › **SAP eleva las funciones de seguridad de Gigya a una solución CIAM completa.** Después de adquirir Gigya en septiembre de 2017, SAP debatió si tratar la tecnología de Gigya como seguridad o como cliente de administración. SAP decidió incluirlo en la gestión de datos de clientes; como resultado, SAP es agregar constantemente funciones de seguridad: mejoras de SSO, autenticación push y autenticación: a las capacidades tradicionales de gestión de usuarios de la solución. SAP planea lanzar CIAM del lado del servidor para mejorar la prevención de apropiación de cuentas, implementar el soporte de FIDO2 WebAuthn, e introducir conjuntos de pantallas nativas que ofrecen flujos de trabajo prediseñados e integración de aplicaciones más rápidamente.

La solución ofrece una excelente gestión del consentimiento, un amplio autoservicio para el cliente y un muy bien pensado a través de la interfaz de administración CIAM. Herramientas de marketing líderes como Adobe Campaign y Constant Contact y portales de comercio electrónico como Magento y SAP Commerce están pre integrados. Sin embargo, carece de compatibilidad con FIDO2 WebAuthn; no hay puntuaciones de riesgo reales para autenticación; y los clientes se quejan de la falta de soporte productivo para empresas gestión de fraudes, MDM o soluciones de prueba alternativas A / B. La solución no está disponible en las instalaciones, solo como una solución de identidad como servicio (IDaaS) basada en la nube. Es ideal para empresas. requiriendo una gestión de consentimiento extensa y compleja para usuarios con diferencias en los requisitos en múltiples geografías.

Fuertes artistas

- › **WSO2 ensambla piezas de código abierto y patentadas en una plataforma CIAM versátil.** La solución CIAM de WSO2 proviene de su plataforma de gestión y gobierno de identidad. Tiene siempre enfocado en IAM basado en API y estándares y viene con una referencia completa de arquitectura. Más de la mitad de los empleados de WSO2 trabajan en el desarrollo de productos. El vendedor planea lanzar una nube CIAM de software como servicio (SaaS) centrada en el desarrollador, introducir una nube híbrida, oferta en la nube para clientes que no pueden mover la información de sus clientes a la nube y utilizar aprendizaje automático (ML) y análisis de comportamiento para permitir que la solución CIAM ayude a los clientes A / B esfuerzos de prueba.

La solución es compatible con FIDO2 y ofrece soporte completo de API REST para la integración que los clientes dijeron fue bastante fácil de usar. Administración de usuarios, gestión de consentimiento, autenticación, autoservicio, y la integración del sistema empresarial es sólida. Control de acceso basado en roles para administradores, sin contraseña la autenticación, la recuperación de ID de usuario olvidada y la gestión de notificaciones y el panel de control son también fuerte. Sin embargo, la solución no tiene una oferta real de SaaS / IDaaS y gestiona múltiples marcas. o las propiedades en línea son engorrosas. Carece de biometría de comportamiento incorporada y postura del dispositivo detección o integración de la gestión; la salida de informes tabulares basada en texto requiere una solicitud. Las certificaciones de cumplimiento del proveedor son más limitadas que otras. La solución es un ideal para empresas que buscan una solución rentable que operen por sí mismas o tengan un proveedor de servicios de seguridad gestionada.

- › **Ping Identity se duplica en CIAM con PingOne para clientes.** Ping Identity para los clientes, una oferta de IDaaS dedicada a CIAM, ofrece MFA que los desarrolladores pueden integrar en las aplicaciones, administración de perfiles y administración de políticas CIAM basada en API REST. Forrester espera que CIAM comprenda finalmente casi la mitad de los ingresos totales de Ping Identity. El proveedor planea agregar fuentes de amenazas integradas para acceder a las definiciones de políticas, lanzar Ping Portal para proporcionar acceso unificado a todas las consolas de administración de Ping y crear un nuevo servicio IDaaS para la privacidad y gestión del consentimiento.

A los clientes les encanta el amplio conjunto de estándares de autenticación admitidos de la solución, fáciles de usar integración y recuperación biométrica, integración productiva con servicios de verificación de identidad, buena creación de perfiles progresiva y amplia gestión de usuarios de los dispositivos registrados. Sin embargo, PingOne para los clientes carece de soporte FIDO2 y no hay control de acceso basado en roles (RBAC) para ver informes y soporte de pruebas A / B listo para usar. Gran parte de la funcionalidad que evaluamos en este Forrester Wave, incluida la integración de MFA, sistemas de gestión de fraude y soluciones de autenticación: requieren que las empresas que utilizan PingOne para los clientes instalen y configuren Ping Federate y Ping Access como componentes independientes y probablemente locales. La solución es buena apto para empresas con requisitos complejos de gestión de acceso de clientes y muchas locales aplicaciones que deben integrar en el régimen SSO.

- › **Okta se centra en la escalabilidad y la gestión del rendimiento.** En 2019, Okta lanzó DynamicScale para responder a las tendencias de la industria, las expectativas de los consumidores y el CIAM del cliente problemas de rendimiento y hacer que el rendimiento sea más predecible. Proporciona un IDaaS basado en células / unidad de alta disponibilidad refactorizado que puede manejar cargas de tráfico elevadas sostenidas. Mientras que los clientes pagarán más por cargas más altas que antes de la introducción de DynamicScale, el servicio garantiza altos disponibilidad de la oferta CIAM de Okta. El proveedor planea lanzar servicios de plataforma para modularizar su oferta, mejorar su Okta Identity Engine para aceptar información de amenazas de terceros y lanzar un meta directorio universal para conectar repositorios de usuarios.

La solución ofrece buenas opciones de verificación de identidad del cliente, admite un amplio conjunto de estándares de autenticación y tiene una extensa lista de certificaciones de cumplimiento normativo a nivel mundial. El propio servicio Threat Insight integrado de Okta proporciona contexto sobre los usuarios y sus sesiones para impulsar las políticas de acceso. El soporte productivo para autenticadores de terceros para MFA también es bueno. Sin embargo, la gestión de consentimiento y el panel de control de la solución van por detrás de la competencia. La solución carece de biometría de comportamiento, un constructor de UI para la gestión de perfiles y gestión de la postura del dispositivo. Integraciones productivas y listas para usar con análisis web, marketing y gestión de consentimiento las soluciones también se quedan atrás. La solución es adecuada para empresas que buscan SaaS CIAM puro con componentes mínimos en las instalaciones

- › **Auth0 mejora CIAM con detección de amenazas y anomalías.** Auth0 lanzó su detección de anomalías motor para proporcionar sus propias herramientas de inteligencia de amenazas y fuentes de datos, como dirección IP, dominio y reputación de contraseña. También lanzó recientemente el registro social, la autenticación sin contraseña y una función de migración de usuarios que maneja los hashes de las contraseñas de los usuarios con elegancia. Auth0 tiene 660 empleados a nivel mundial, con un alto enfoque en la ejecución de ventas. El proveedor planea invertir en la plataforma CIAM capacidades, automatizar la prevención de ataques utilizando su motor de detección de anomalías y mejorar el usuario conocimiento del contexto y extensibilidad mediante la incorporación de socios en su mercado de integración.

La solución proporciona excelentes servicios de migración de usuarios y gestión de invitaciones de registro. Cuenta vinculación, prevención de relleno de credenciales y reemplazo de token MFA perdido están por delante de la competencia. Los clientes dijeron que las integraciones con soluciones CRM y MDM y análisis web, las plataformas son particularmente fuertes. Sin embargo, la solución carece de soporte FIDO2; atributos de mapeo de fuentes de datos de usuario LDAP es engorroso y requiere más secuencias de comandos que la competencia. Agregar administradores de sistema de forma explícita es más complicado que con otros proveedores, y La solución ofrece un soporte mínimo para registros de clientes ligeros y solo por correo electrónico.⁵ Consentimiento La biometría de gestión y del comportamiento también está detrás de la competencia. La solución es buena apto para empresas que están pasando de la autenticación en silos desarrollada internamente y específica de la aplicación a Servicios CIAM centralizados y orquestados.

- › **Salesforce fortalece su CIAM con sus plataformas de gestión de datos de clientes.** Sobre la base de más de 150.000 organizaciones de clientes que utilizan sus soluciones empresariales no relacionadas con la seguridad, Salesforce ha realizado ventas cruzadas de su solución CIAM desarrollada orgánicamente a su base instalada.⁶ Los planes del proveedor para integrar Data Manager con su cartera CIAM para una vista de 360 grados del cliente, lanzamiento un conjunto de herramientas de privacidad del usuario e integrar su plataforma de gestión de datos (a través de su adquisición de 2017 de of Krux) y la plataforma de datos del cliente con su solución CIAM para ayudar a los clientes a rastrear y promover conversión de cliente no registrado.

Como era de esperar, la solución tiene sólidas integraciones con CRM, MDM, marketing y análisis. Las soluciones, principalmente soluciones propias de Salesforce. Los informes y los paneles son visualmente agradables y muy versátil; Los administradores de CIAM pueden usar carpetas de informes para personalizar quién tiene acceso a qué informes. Salesforce CIAM admite cuentas de clientes de solo correo electrónico en etapa inicial; configurar el envío de invitaciones de registro clásicas a los clientes es muy flexible y fácil de usar. Sin embargo, la solución carece de soporte para FIDO2 y WebAuthn. La elaboración de perfiles progresivos no está del todo productiva; para muchos clientes, es muy complejo y difícil de configurar. Configurar el registro de una sola vez tokens de contraseña es más elaborado que la competencia, y no hay soporte enlatado para integraciones biométricas o pruebas A / B.7 La solución es ideal para las empresas que planean expandir sus Salesforce CRM o inversiones en herramientas de marketing a un sistema CIAM completo.

Contenedores

- › **LoginRadius ofrece una solución CIAM técnicamente sólida y versátil.** No es de extrañar que se centra en CIAM: 73 de sus 170 empleados desarrollan su solución CIAM. Teniendo en cuenta su tamaño relativamente pequeño, el proveedor tiene una extensa red de implementación socios con un historial probado de acuerdos. La solución está disponible tanto como instalado localmente software y un servicio basado en la nube, aunque LoginRadius no reveló los precios de la nube Servicio. El proveedor planea implementar el monitoreo de la web oscura en tiempo real, agregar clientes continuos autenticación para realizar biometría de comportamiento en las acciones de los usuarios para identificar potencialmente fraudulentos o actividad dañina, e implementar AI y ML para la protección de la cuenta y el enriquecimiento de datos.

La solución proporciona las capacidades técnicas más amplias de las que revisamos en esta Wave. evaluación: los servicios de migración de usuarios son buenos, y la gestión de consentimiento versátil y especialmente diseñada el sistema viene con control de versiones por consentimiento. Soporte para registros de correo electrónico y múltiples marcas y las propiedades son extensas. La variedad de certificaciones de cumplimiento es impresionante. Sin embargo, RABC para los administradores de CIAM se queda atrás, y la configuración de SSO simple requiere mucho más scripting que la competencia. El soporte de token MFA de terceros, listo para usar, se queda atrás y la solución carece Soporte FIDO2. Los clientes dijeron que los planes estratégicos del proveedor van a la zaga de otros proveedores en identidad verificación, gestión de la privacidad y el consentimiento, y análisis de identidad y fuentes de amenazas. La solución es una buena opción para empresas con habilidades considerables de marketing y desarrollo, pero que carecen de habilidades CIAM.

- › **Microsoft agrega Identity Experience Framework a su solución CIAM para la orquestación.** Gracias a la contratación de gestión estratégica de productos, Microsoft está duplicando CIAM al admitir estándares, como proveedores de OpenID Connect, compatibilidad con ID de Google y acceso a proveedores de identidad, paso de token - e introduciendo el Identity Experience Framework (IEF), que permite orquestación. Junto con otros proveedores, Microsoft también está experimentando con sistemas basados en usuarios activos. modelos de precios.

Planea integrar las capacidades de CIAM en Azure Active Directory; invertir en usuario y análisis de comportamiento de entidad (UEBA) para respaldar la gestión de acceso basada en riesgos; y mejorar la experiencia de administrador y proporciona automatización para ensamblar, probar e informar sobre flujos de trabajo.

La solución tiene el conjunto más extenso de certificaciones de cumplimiento y puede servir a millones de solicitudes de autenticación por hora. Las regiones de usuario mantienen la residencia de datos y el cumplimiento de diversas normativas de privacidad. La solución tiene una notable integración inmediata con Microsoft Dinámica usando SAML / OIDC. El control de acceso a los informes y la configuración del panel de control son muy útiles. Sin embargo, la solución es solo en la nube; no hay una versión local. Carece de soporte para FIDO2 / Compatibilidad con WebAuthn y una gran variedad de funciones, como registros de solo correo electrónico, y requiere que los administradores usen y codifiquen en la relativamente compleja IEF o REST Graph API. No hay flujo de trabajo visual diseñador. La asignación de atributos del directorio de usuarios externos y la gestión de consentimiento requieren personalización utilizando la programación IEF. Los clientes informan que cambiar el registro de usuarios fluye para admitir dinámicas. Las pruebas A / B son difíciles. La solución se adapta bien a las grandes multinacionales con datos que varían según la región con requisitos de privacidad.

- › **Akamai ofrece inicio de sesión alojado y un generador de registro actualizado.** La adquisición de Janrain en 2019 catapultó a Akamai, que tenía una experiencia limitada en IAM, al espacio CIAM. Akamai continuó agregando funciones a la solución CIAM, incluidos webhooks, inicio de sesión alojado y actualizaciones del constructor de registros. Planea implementar la autenticación adaptativa con señales de riesgo, implementar autenticación de borde utilizando su infraestructura de red de entrega de contenido para bloquear a los piratas informáticos tan pronto como posible y ampliar el ecosistema de integraciones de datos a plataformas de inteligencia empresarial.

La solución tiene buenas capacidades de generación de informes, paneles y gestiona grandes cantidades de identidades y marcas. Ofrece flujos de verificación de identidad para los registrantes y consentimiento flexible de servicios de revocación. Un servidor de autorización incorporado puede administrar derechos comerciales en portales. El alcance de los administradores de CIAM y la gestión de acceso a informes son granulares. Sin embargo, la solución carece de Soporte FIDO2 / WebAuthn. La adición de tiendas de usuarios LDAP requiere servicios profesionales; la migración de usuarios requiere una integración y un middleware complejos. En nuestra evaluación, la solución y la mayoría de sus integraciones con sistemas comerciales como MDM, análisis web y enfoque de marketing empresarial sobre la privacidad por diseño y no están elaborados ni expuestos al mismo grado que la competencia.

Nuestra impresión de las conversaciones con los clientes fue que Akamai pasó tiempo tratando de recuperar su el impulso de desarrollo de CIAM después de la adquisición de Janrain, lo que provocó retrasos en el mantenimiento de la competencia. La solución es una buena opción para las empresas globales preocupadas por la seguridad que buscan proteger propiedades que utilizan informática sin servidor, protecciones distribuidas contra ataques de denegación de servicio y gestión CIAM de frente.

- › **OpenText se basa en los activos CIAM de Covisint.** OpenText amplió su portafolio CIAM para permitir interoperabilidad en toda su cartera de productos no relacionados con la seguridad. Durante el período de 12 meses que finaliza la fecha límite, el proveedor también ha implementado un sistema para la gestión de identidad entre dominios (SCIM) y U2F y se realizaron varias mejoras en el flujo de trabajo de CIAM y la migración de usuarios. El proveedor planea crear un entorno de desarrollo de código bajo para permitir a los desarrolladores automatizar la construcción de entornos CIAM, integrar el centro de privacidad OpenText con su solución CIAM, e introducir una interfaz productiva para OpenText Experience para habilitar CIAM omnicanal, A / B testing y optimización CIAM de las llamadas.

La solución CIAM de OpenText capitaliza su experiencia en la federación de identidades y la confianza en B2B2C IAM y tiene un buen conjunto de funciones de IAM para Internet de las cosas (IoT). La solución tiene útil autenticación basada en riesgos y funciones integrales para reemplazar tokens MFA perdidos. Multi Alquiler la administración de jerarquías de inquilinos, es muy buena y, en general, adoptado por los clientes. Controlar el acceso a los informes es funcional y flexible. sin embargo, El proveedor no tiene socios de implementación CIAM, lo que limita en gran medida su capacidad para aumentar el rendimiento de su solución. Soporte productivo para múltiples marcas o propiedades, privacidad y consentimiento de gestión, creación de perfiles progresiva, cuentas de clientes en fase inicial (no autenticadas) y La revocación del consentimiento no está expuesta a los administradores del CIAM en el mismo grado que la competencia. La solución puede ser una buena opción para las empresas que buscan una administración de dispositivos IoT IAM escalable con bloque de su estrategia CIAM.

- › **Optimal IdM tiene una solución CIAM totalmente alojada en la nube.** El vendedor mejoró su federación y Capacidades de integración LDAP y soporte multiusuario agregado a Optimal Cloud. La solución también ofrece API para una fácil integración. Optimal IdM gasta mucho en innovación; Forrester estima que gasta la mitad de sus ingresos del CIAM en investigación y desarrollo del CIAM. Planea ampliar el CIAM API de la solución configurada para una integración más sencilla en los clientes y socios usuarios finales, implemente UEBA real para analizar los datos que la solución Optimal Cloud del proveedor almacena en Splunk y mejorar su SCIM motor de aprovisionamiento

El mapeo de atributos de la solución es bueno y tiene aprovisionamiento de usuarios administradores basado en SCIM y CSV capacidades Tiene un soporte decente para múltiples jerarquías de inquilinos. Análisis de patrones de mecanografía proporciona protección adicional contra la apropiación de cuentas y la solución admite explícitamente el autoservicio de auto des registro y actualización de perfil de usuario. Sin embargo, va por detrás de otras soluciones en gestión de consentimiento e integraciones con sistemas empresariales como CRM y MDM. IDV y fraude la integración de soluciones de gestión también se queda atrás. Los clientes y Forrester descubrieron que los informes y el tablero de instrumentos falta en gran medida. Además, el proveedor no tiene un ecosistema de integrador de sistemas. socios. La solución se adapta bien a las organizaciones que desean utilizar una solución integrada para ambos personal y gestión de identidad y acceso de clientes.

Resumen de la evaluación

Evaluamos a los proveedores según 32 criterios, que agrupamos en tres categorías de alto nivel:

- › **Oferta actual.** La posición de cada proveedor en el eje vertical del gráfico de Forrester Wave indica la fuerza de su oferta actual. Los criterios clave para estas soluciones incluyen datos orquestación y gestión de usuarios, verificación y registro de la identidad del cliente, privacidad, gestión de consentimiento y creación de perfiles, autenticación de clientes, autoservicio de clientes, negocios integración de sistemas, integración de sistemas de gestión de fraudes e IDV, informes y paneles de control, escala, cumplimiento, entorno integrado y documentación estática y contextual.
- › **Estrategia.** La ubicación en el eje horizontal indica la fuerza de la estrategia de cada proveedor, evaluamos la hoja de ruta de ejecución, enfoque de mercado, inversión CIAM en I + D, solución CIAM mejora, profundidad de los servicios profesionales de soporte y ecosistema de socios.
- › **Presencia del mercado.** Representada por el tamaño de los marcadores en el gráfico, muestra la presencia en el mercado, los puntajes reflejan los ingresos y el crecimiento anual de las suscripciones CIAM de cada proveedor.

Criterios de inclusión de proveedores

Forrester incluyó a los 13 proveedores en la evaluación: Akamai, Auth0, ForgeRock, IBM, LoginRadius, Microsoft, Okta, OpenText, Optimal IdM, Ping Identity, Salesforce, SAP y WSO2. Cada uno de estos proveedores tiene:

- › **Un portafolio de productos y servicios líder en el pensamiento.** Incluimos proveedores CIAM que demostró liderazgo intelectual y ejecución de la estrategia de solución mediante la actualización y mejorando su cartera de productos y modelos productivos. Los clientes de los proveedores tenían que informar que la solución está diseñada específicamente para la gestión de acceso e identidad de cara al cliente.
- › **Ingresos anuales de CIAM de al menos \$ 4 millones con un crecimiento de al menos 9.5%.** Incluimos proveedores que tienen al menos \$ 4 millones en ingresos combinados de la solución CIAM y al menos 9.5% de crecimiento año tras año en los ingresos CIAM.
- › **Mindshare con los clientes finales de Forrester.** Los proveedores que evaluamos son frecuentemente mencionados en las consultas de clientes de usuarios finales de Forrester, RFP de selección de proveedores, listas cortas, consultoría proyectos y estudios de caso.
- › **Mindshare con los proveedores.** Los proveedores que evaluamos son frecuentemente señalados por otros proveedores durante Las sesiones informativas de Forrester como competidores viables y formidables.

Interactúe con un analista

Obtenga una mayor confianza en sus decisiones trabajando con los líderes de opinión de Forrester para aplicar nuestra investigación a sus iniciativas empresariales y tecnológicas específicas.

Consulta del analista

Para ayudarte a poner la investigación en la práctica, conectar con un analista para discutir sus preguntas en un Sesión telefónica de 30 minutos - u optar por una respuesta vía correo electrónico.

Aprende más vía email.

Asesor de analistas

Traducir la investigación a acción trabajando con un analista en un específico compromiso en la forma de estrategia personalizada sesiones, talleres, o discursos.

Aprende más vía email.

Webinar

Únase a nuestras sesiones en línea sobre las últimas investigaciones que afectan a su negocio. cada llamada incluye preguntas y respuestas de analistas y diapositivas y está disponible a pedido.

Aprende más vía email.



[Aplicaciones de investigación de Forrester para iOS y Android.](#)

Manténgase por delante de su competencia sin importar dónde se encuentre.

Material Suplementario

Recurso en línea

Publicamos todas nuestras puntuaciones y ponderaciones de Forrester Wave en un archivo de Excel que proporciona información detallada de la evaluación de productos y clasificaciones personalizables; descargue esta herramienta haciendo clic en el enlace al principio de este informe en Forrester.com. Tenemos la intención de que estas puntuaciones y ponderaciones predeterminadas sirvan solo como punto de partida y anime a los lectores a adaptar las ponderaciones para que se ajusten a sus necesidades individuales.

La metodología de Forrester Wave

Un Forrester Wave es una guía para compradores que consideran sus opciones de compra en una tecnología mercado. Para ofrecer un proceso equitativo para todos los participantes, Forrester sigue [The Forrester Wave™ Guía de metodología](#) para evaluar proveedores participantes.

En nuestra revisión, realizamos una investigación primaria para desarrollar una lista de proveedores a considerar para la evaluación. De ese grupo inicial de proveedores, reducimos nuestra lista final según los criterios de inclusión. Entonces nos reunimos detalles del producto y la estrategia a través de un cuestionario detallado, demostraciones / sesiones informativas y encuestas / entrevistas de referencia. Usamos esos insumos, junto con la experiencia y pericia del analista en el mercado, para calificar a los proveedores, utilizando un sistema de calificación relativa que compara a cada proveedor con los demás en la evaluación.

Incluimos la fecha de publicación de Forrester Wave (trimestre y año) claramente en el título de cada Forrester Informe Wave. Evaluamos a los proveedores que participan en este Forrester Wave utilizando materiales que nos proporcionó antes del 10 de julio de 2020 y no permitió información adicional después de ese momento. Alentamos lectores para evaluar cómo el mercado y las ofertas de los proveedores cambian con el tiempo.

De acuerdo con [la Política de revisión de proveedores de The Forrester Wave™](#), Forrester solicita a los proveedores que revisen nuestros hallazgos antes de la publicación para verificar su exactitud. Proveedores marcados como proveedores no participantes en el gráfico Forrester Wave cumplieron con los criterios de inclusión definidos, pero se negó a participar o contribuyó sólo parcialmente a la evaluación. Calificamos a estos proveedores de acuerdo con [The Forrester Wave™ Y La política de proveedores de participación incompleta y no participante de Forrester New Wave™](#) y publicar su posicionamiento junto con los de los proveedores participantes.

Política de integridad

Realizamos toda nuestra investigación, incluidas las evaluaciones de Forrester Wave, [de acuerdo con las Políticas publicadas](#) en nuestro sitio web.

Notas finales

- 1 Los precios transaccionales también se conocen como precios de pago por uso. El precio basado en la cantidad de usuarios activos significa que un cliente paga solo por aquellos usuarios que inician sesión durante un mes determinado. Precios basados en el número total de inactivos y usuarios activos significa que un cliente paga una tarifa anual fija por usuario.
- 2 Sin embargo, el proveedor proporciona guías de integración para Daon, Entrust y otros.
- 3 El proveedor planea mejorar la gestión del consentimiento en la segunda mitad de 2020.
- 4 La situación fue bastante similar en nuestra última fuerza laboral IAM IDaaS Wave. Consulte el informe de Forrester ["The Forrester Wave™: Identity-As-A-Service \(IDaaS\) para empresas, segundo trimestre de 2019"](#).
- 5 Los nuevos administradores deben ser invitados explícitamente y no pueden designarse en función de la pertenencia a grupos de Active Directory. Se planifican registros de clientes ligeros y solo por correo electrónico.
- 6 Fuente: Salesforce (<https://www.salesforce.com/campaign/worlds-number-one-CRM/>).
- 7 Los flujos de inicio de sesión brindan muchas formas de crear perfiles progresivos, desde arrastrar y soltar hasta una experiencia programática completa la integración biométrica está integrada en el SDK móvil.

The Forrester Wave™: Identidad del cliente y gestión del acceso, Q4 2020

Los 13 proveedores que más importan y como se calculan

- 8 Además, la modernización del producto CIAM del proveedor y los esfuerzos de desarrollo ciudadano le permitirán aprovechar su amplia red de socios comerciales para ofrecer soluciones.
- 9 El proveedor tiene su propia organización de servicios globales para la implementación del proyecto CIAM.

Trabajamos con líderes empresariales y tecnológicos para impulsar una visión, estrategia y ejecución personalizadas que aceleren el crecimiento.

Productos y servicios

- › Investigación de herramientas
- › Compromiso de análisis
- › Datos y análisis
- › Colaboración entre pares
- › Consultoría
- › Eventos
- › Programas de certificación

La investigación y los conocimientos de Forrester se adaptan a su papel e iniciativas comerciales críticas.

Roles que servimos

Estrategia de mercadeo profesional

CMO

Marketing B2B

Marketing B2C

Experiencia del cliente

Perspectivas del cliente

Comercio electrónico y canal estratégico

Gestión de la tecnología profesional

CIO

Desarrollo de aplicaciones y entrega

Arquitectura empresarial infraestructura y

operaciones

› **Riesgo de seguridad**

Abastecimiento y proveedor de administración

Industria de la tecnología empresarial

Relaciones con analistas

Soporte al cliente

Para obtener información sobre copias impresas o reimpressiones, comunicarse con atención al cliente en +1 866-367-7378, +1 617-613-5730, o clientsupport@forrester.com. Ofrecemos cantidad de descuentos y precios especiales para instituciones académicas y sin fines de lucro.