

ManageEngine



Transforme digitalmente su
organización financiera **para**
obtener un mayor valor
empresarial



Tabla de contenido

Desafíos en la industria de servicios financieros	03
La alineación entre TI-empresa	05
Casos de uso específicos de la industria BFSI	12
Caso de uso 1: Garantizar un acceso ininterrumpido y simple a las aplicaciones bancarias	12
Caso de uso 2: Optimizar las operaciones bancarias	16
Caso de uso 3: Reducir el riesgo cibernético	20
Caso de uso 4: Proteger los datos financieros críticos	24
Caso de uso 5: Aprovechar el análisis de datos para tomar decisiones informadas	28
Acerca de ManageEngine	30

Han cambiado muchas cosas en la industria de los servicios financieros

La competencia en la industria de los servicios financieros es más feroz que nunca debido a las crecientes exigencias de los clientes modernos, el aumento de las ciberamenazas y los mandatos normativos más complejos. Estos factores han contribuido a la aceleración de las iniciativas de transformación digital (DX) entre las organizaciones financieras.

Aunque algunas de las organizaciones financieras ya han iniciado este proceso, es seguro decir que la DX es un acontecimiento en curso y que las organizaciones podrían tardar algún tiempo en cosechar sus resultados reales. Sin embargo, está claro que invertir en la tecnología adecuada dará a las organizaciones BFSI una ventaja digital que puede garantizar una mejor eficiencia de los costos operativos, impulsar la innovación y fomentar el crecimiento.

Desafíos en la industria de servicios financieros

Disrupción tecnológica

La introducción de nuevos actores fintech y el crecimiento exponencial de la adopción de tecnología han obligado a los bancos tradicionales y a otras organizaciones financieras a innovar y adoptar nuevas formas de tecnología para seguir siendo relevantes y adelantarse a sus competidores. Es crucial que las organizaciones financieras tradicionales se adapten a las cambiantes expectativas de los clientes centrándose en iniciativas digitales que incluyan plataformas de pago digitales, [IA](#) y análisis de datos masivos, banca móvil, chatbots conversacionales y [blockchain](#) para agilizar sus procesos.

Riesgos cibernéticos

La ciberseguridad sigue siendo una de las principales preocupaciones para las organizaciones BFSI, con el ransomware y el phishing encabezando

la lista. Las medidas tradicionales de ciberseguridad ya no serán suficientes a medida que los ataques sean cada vez más sofisticados. Las organizaciones BFSI tendrán que reconocer la naturaleza dinámica de las amenazas e invertir en estrategias y soluciones de ciberseguridad robustas para proteger sus datos y sistemas. El uso de [IA](#) y [ML](#) para identificar posibles riesgos de seguridad, la inteligencia de amenazas avanzada para desarrollar contramedidas eficaces para combatirlos, la aplicación del marco de confianza cero para validar las identidades de usuarios, dispositivos y aplicaciones son algunas formas de protegerse proactivamente de las amenazas emergentes.

Gestión del cumplimiento

Las organizaciones BFSI manejan una gran cantidad de datos confidenciales, como detalles de pagos, PII, detalles de inversiones, registros de seguros, entre otros. Dada la naturaleza sensible de los datos, las instituciones financieras están obligadas a seguir un amplio conjunto de leyes reglamentarias y mandatos de cumplimiento. Incumplir con estas normativas puede acarrear enormes multas y la pérdida de confianza de los clientes. Es esencial que las organizaciones financieras inviertan en soluciones de cumplimiento y también tomen medidas adicionales para prevenir las [violaciones de datos](#).

Expectativas de los clientes

Es evidente que las expectativas de los clientes han cambiado tras la pandemia. Los clientes conocedores del mundo digital esperan una experiencia bancaria flexible. Buscan un proveedor que pueda ofrecer un acceso simple a los servicios bancarios en línea, garantizar una experiencia bancaria omnicanal segura y un soporte superior. Esto significa que las organizaciones financieras tradicionales tienen que ponerse a la altura de los clientes de la nueva era habilitando plataformas bancarias digitales eficientes, incluida la banca móvil y la banca en línea, proporcionando experiencias personalizadas con la ayuda de la IA y los análisis avanzados, ofreciendo asistencia rápida mediante chatbots basados en [IA](#), y mucho más.

La alineación entre TI-empresa

Las organizaciones financieras pueden maximizar su eficacia y alcanzar los objetivos empresariales generales alineando estratégicamente sus TI para alcanzar objetivos empresariales específicos.

Algunos de los beneficios empresariales comunes que impulsan la adopción de TI son:

**Escalar
libremente y
optimizar las
operaciones**



La creciente demanda de los clientes y la feroz competencia con empresas fintech relativamente nuevas han obligado a los bancos a racionalizar y modernizar sus operaciones. Los bancos tendrán que actualizar su infraestructura de TI, optimizar los procesos para mejorar la eficacia y crear aplicaciones que respondan a las necesidades del momento.

Modernizar las TI puede ayudar a reducir el costo operativo necesario para mantener los sistemas obsoletos, facilitar el crecimiento en función de las necesidades empresariales y ayudar a reducir los riesgos y vulnerabilidades cibernéticos.

Cómo ayuda la TI:

- Las soluciones de gestión de TI pueden facilitar la modernización gestionando la actualización del hardware, el software y la red según las necesidades.
- La migración a la nube también puede considerarse parte del proceso de modernización, y esto proporciona a las organizaciones la flexibilidad necesaria para escalar a un menor costo.
- Las aplicaciones financieras se pueden desarrollar en menos tiempo con la ayuda de la tecnología de desarrollo de aplicaciones de código bajo.
- Las operaciones se pueden agilizar optimizando los procesos repetitivos con la ayuda de la automatización del flujo de trabajo y la IA.

Desarrollar sistemas de pago seguros y eficientes



El sector BFSI ha sido un objetivo perfecto para los ciberdelincuentes simplemente por las posibilidades de obtener el máximo beneficio con un ataque. Los ciberdelincuentes pueden utilizar el phishing, llevar a cabo ataques DDoS, ataques internos, ingeniería social, exploits de día cero o alguna de las diversas formas de atacar a las organizaciones financieras.

Las organizaciones financieras funcionan con base en el concepto de confianza, y una ligera ruptura de la confianza puede suponer un gran revés para las organizaciones. Además, una pequeña interrupción de los servicios bancarios puede costar miles de millones a un banco. Esto significa que las organizaciones financieras tendrán que mantener la seguridad y resiliencia de sus operaciones bancarias, mitigar los riesgos y garantizar la continuidad del negocio.

Cómo ayuda la TI:

- Las soluciones SIEM ayudan a detectar, investigar y mitigar las amenazas persistentes avanzadas que podrían comprometer la red de los bancos.
- Las soluciones de gestión de identidades y gestión de accesos privilegiados se pueden utilizar para garantizar que sólo las personas adecuadas tengan acceso a los recursos sensibles.
- Las vulnerabilidades de la red y de los dispositivos se pueden parchear automáticamente con soluciones de gestión de la seguridad para endpoints y redes.
- Las soluciones de gestión y recuperación ante incidentes se pueden utilizar para garantizar la continuidad del negocio y minimizar el tiempo de inactividad.
- El análisis predictivo, ML y los algoritmos de IA se pueden utilizar para predecir y prevenir ciberataques, reducir el tiempo de respuesta ante anomalías y mejorar la detección y respuesta ante amenazas.
- Se pueden realizar evaluaciones periódicas de los riesgos digitales al escanear las páginas web relacionadas con el banco para comprobar diversos aspectos que pueden causar vulnerabilidades y evaluar la postura de seguridad de dichas páginas.
- Aplicar el marco de confianza cero y otras buenas prácticas de ciberseguridad pueden ayudar a las organizaciones a minimizar el riesgo cibernético.

Proteger los datos financieros y cumplir la normativa



Los ciberdelincuentes suelen buscar los datos confidenciales relacionados con las operaciones financieras (incluyendo los detalles de los pagos, la información de identificación personal, los detalles de las inversiones, los registros de seguros y la información de las cuentas) para realizar transacciones fraudulentas, pedir rescates, interrumpir las operaciones comerciales y llevar a cabo ataques selectivos.

Para evitarlo, proteger la privacidad de los clientes y reducir el riesgo de violación de los datos financieros, diversos organismos reguladores y países han presentado una serie de mandatos normativos y de cumplimiento. Las organizaciones tendrán que adherirse a directrices específicas y seguir medidas de cumplimiento críticas pero complejas para operar legalmente y evitar fuertes multas por incumplimiento.

Las organizaciones financieras tendrán que cumplir con la lista de regulaciones específicas de la industria que incluyen PCI DSS, GLBA, GDPR, FISMA, SOX, y las leyes de privacidad de datos geo-específicas como GDPR, CCPA, POPIA, etc.

Cómo ayuda la TI:

- Las soluciones automatizadas de monitoreo, auditoría e informes ayudarán a evaluar la eficacia de los controles aplicados, contribuirán a descubrir discrepancias y aportarán pruebas que respalden el cumplimiento del mandato por parte de la organización.
- Las soluciones de seguridad de datos pueden ayudar a evaluar el riesgo de los datos, escanear y analizar los archivos de documentos, y monitorear el control y el flujo de datos confidenciales con la ayuda de las funciones de prevención de filtración de datos.

Mejor experiencia del cliente y del empleado



Hoy en día, los clientes dependen de las soluciones bancarias en línea y móviles, por lo que esperan tener el mismo nivel de rapidez y accesibilidad para los servicios bancarios del que obtienen de otros servicios en línea. El soporte eficiente, la resolución rápida de los problemas y los servicios personalizados son otros factores importantes que los clientes buscan en las organizaciones financieras.

También se debe proporcionar a los empleados una experiencia superior para que puedan atender mejor a sus clientes. Esto significa construir un entorno de trabajo que ayude a los empleados a centrarse en sus tareas con interrupciones mínimas. Dotar a los empleados de herramientas que les ayuden a tomar decisiones informadas y a automatizar parte de su trabajo les ayudará a operar con eficacia.

Cómo ayuda la TI:

- Las soluciones de monitoreo de sitios web y aplicaciones pueden garantizar un acceso sin problemas a las aplicaciones de banca móvil.
- Los chatbots basados en IA se pueden utilizar para proporcionar respuestas rápidas a las consultas.
- Las soluciones de autoservicio se pueden utilizar para capacitar a clientes y empleados de modo que puedan llevar a cabo tareas específicas sin depender de otros.
- La analítica de datos se puede utilizar para analizar grandes volúmenes de datos y proporcionar información procesable para una mejor toma de decisiones.

Enfóquese en el crecimiento y en mejorar el ROI con las soluciones de ManageEngine

Las soluciones de gestión de TI de [ManageEngine](#) han ayudado eficazmente a las organizaciones financieras a alcanzar la excelencia empresarial a través de las TI. Las organizaciones financieras utilizan nuestras soluciones para agilizar sus operaciones, mejorar la gestión de la seguridad y el cumplimiento normativo, mitigar los riesgos y garantizar la continuidad del negocio.

En la siguiente sección le mostraremos algunos de los casos de uso más comunes relacionados con el sector BFSI y le explicaremos en detalle cómo se han utilizado nuestras soluciones para alcanzar objetivos empresariales específicos.



Casos de uso específicos de la industria BFSI

Caso de uso 1:

Garantizar un acceso ininterrumpido y simple a las aplicaciones bancarias

[Una organización financiera](#) quiere asegurarse de que sus clientes y empleados puedan acceder sin problemas a sus aplicaciones bancarias en línea. Es necesario proporcionar a los usuarios de la aplicación una experiencia consistente en todo momento y en todas las ubicaciones. Esto significa garantizar una alta disponibilidad de la aplicación y resolver los problemas que afectan al [rendimiento](#) de la aplicación lo antes posible.

Dado que la aplicación contiene información sensible, el acceso de los empleados se debe proteger mediante un proceso de autenticación; los usuarios sólo deben tener acceso mediante la autenticación de dos factores (2FA) o la autenticación basada en tokens.

Toda la experiencia de la aplicación debe ser simple, permitiendo a los usuarios iniciar sesión de forma segura y acceder a múltiples [servicios bancarios](#) sin tener que volver a introducir sus credenciales. También deben poder reportar problemas y hacer solicitudes de servicio rápidamente a través de [un portal de autoservicio](#), y necesitan tener acceso a la base de conocimientos necesaria para facilitarles el trabajo.

Cómo se adaptan los productos de ManageEngine:

Productos de ManageEngine	Cómo ayudan
<p><u>Applications Manager</u></p>	<p>Monitoree el rendimiento de la aplicación y mida los niveles de satisfacción del usuario final de su aplicación empresarial capturando las trazas de transacciones, aislando las consultas lentas, monitoreando el rendimiento de JVM y automatizando las acciones correctivas.</p> <p>Mida la experiencia de la aplicación en todas las geografías simulando y registrando los recorridos de los usuarios con transacciones sintéticas. Monitoree las transacciones críticas con capturas de pantalla y detalles de los elementos de la página con los tiempos de carga por separado.</p>
<p><u>OpManager Plus</u></p>	<p>Monitoree y obtenga información sobre el rendimiento de las aplicaciones críticas utilizadas para la banca en línea. Controle las métricas críticas como el tiempo de renderización de la página, el tiempo de descarga y mucho más, todo desde un lugar centralizado.</p> <p>Monitoree y controle los datos en tiempo real de las interacciones de los usuarios y determine el rendimiento de sus aplicaciones financieras en distintas geografías utilizando el RUM.</p>

<p><u>Site24x7</u></p>	<p>Analice cómo interactúan los clientes con las suites de planificación financiera, los sitios de seguros y las plataformas de inversión en tiempo real utilizando el RUM. Analice el comportamiento de las aplicaciones mediante APM y el monitoreo de API REST. Asegúrese de que no se interrumpan los flujos de trabajo críticos para la empresa. Puede realizar análisis sintéticos y supervisar el rendimiento de las aplicaciones respaldadas por 2FA.</p> <p>Monitoree las aplicaciones del sistema bancario central y las aplicaciones de procesamiento de pagos en entornos tradicionales, en la nube o Kubernetes (a través de volúmenes persistentes o gráficos helm) con integraciones estrechas.</p>
<p><u>Identity360</u></p>	<p>Aproveche el SSO protegido por MFA no sólo para permitir que los usuarios accedan de forma segura a las aplicaciones, sino también para evitar la fatiga de contraseñas gracias a su capacidad de permitir un mismo usuario, con una sola identidad. Los usuarios también pueden acceder sin problemas a varias aplicaciones de la empresa desde una consola central, utilizando el dashboard de SSO integrado.</p>
<p><u>Mobile Device Manager Plus</u></p>	<p>Gestione de forma centralizada las aplicaciones relacionadas con la banca implementadas en los dispositivos móviles de los empleados. Esto incluye actualizar las aplicaciones con las últimas versiones, incluir las aplicaciones en listas blancas y negras, y mucho más.</p> <p>Aproveche el SSO utilizando Kerberos, un protocolo de autenticación de red que protege las claves de acceso encriptándolas mediante el estándar de encriptación de datos.</p>

<p><u>ServiceDesk Plus</u></p>	<p>Implemente una plataforma de gestión de servicios omnicanal con un portal de autoservicio empresarial para garantizar la facilidad de acceso para reportar problemas y crear solicitudes de servicio.</p> <p>Intégrelo con soluciones de monitoreo y observabilidad de TI como Site24x7 para convertir anomalías y alarmas en tickets de incidentes y activar flujos de trabajo automatizados de respuesta a incidentes.</p> <p>Mapee las relaciones empresariales entre personas, activos y servicios con la CMDB completa.</p> <p>Emplee a Zia, un chatbot inteligente basado en IA, para ofrecer asistencia conversacional a sus empleados 24/7. Con Zia, los bancos pueden construir flujos de trabajo de conversación exhaustivos para los problemas más comunes y las preguntas más frecuentes.</p> <p>Manténgase preparado para las auditorías contabilizando todos los activos informáticos y no informáticos que alimentan su infraestructura digital. Realice un seguimiento granular del uso de las licencias de software y del cumplimiento de los acuerdos y contratos de licencia.</p>
<p><u>AD360</u></p>	<p>Permita que los usuarios accedan a varias aplicaciones con un solo clic mediante el SSO.</p> <p>Proteja el SSO con MFA adaptable que admite 20 métodos de autenticación diferentes, incluidos los biométricos, las claves FIDO resistentes al phishing, smart card, YubiKey y TOTP.</p> <p>Garantice el acceso ininterrumpido a los sistemas de los usuarios permitiéndoles restablecer de forma segura las contraseñas y desbloquear las cuentas por sí mismos.</p> <p>Realice copias de seguridad automáticas de las identidades y sus datos, buzones de correo, archivos, carpetas y calendarios, y recupérelos sin problemas garantizando la continuidad del negocio.</p>

Caso de uso 2:

Optimizar las operaciones bancarias

Una organización financiera tiene dificultades para gestionar sus operaciones. Sigue utilizando una [infraestructura de TI heredada obsoleta](#) con una escalabilidad limitada. Sin embargo, tiene previsto modernizar sus operaciones para admitir la banca de nueva generación migrando a la nube y adoptando las [últimas tecnologías](#).

La organización también tiene que garantizar un alto rendimiento de sus aplicaciones de banca electrónica y de sus sistemas bancarios centrales. Esto significa disponer de las [herramientas adecuadas para monitorear](#) y garantizar la salud, la disponibilidad y el rendimiento óptimos de su [infraestructura de TI crítica](#), que repercute directamente en las aplicaciones bancarias.

Aparte de esto, la mayoría de los [procesos operativos](#) de la organización también siguen siendo manuales, y esto está provocando muchos errores y retrasos. De hecho, los empleados no tienen tiempo suficiente para centrarse en algunos de los elementos cruciales del trabajo, ya que la mayoría de los procesos, aunque sean repetitivos, necesitan la atención del empleado. Por eso tiene previsto implementar flujos de trabajo, [soluciones de autoservicio](#) e IA para agilizar algunas de sus funciones con el fin de garantizar una mayor eficacia operativa y reducir los costos.

Cómo se adaptan los productos de ManageEngine:

Productos de ManageEngine	Cómo ayudan
<p><u>OpManager</u></p>	<p>Obtenga visibilidad en tiempo real del estado, la disponibilidad y el rendimiento de los componentes de su red, incluidos los servidores de su banco, las aplicaciones y las bases de datos, y resuelva los problemas antes de que afecten a sus clientes.</p> <p>Diseñe y automatice flujos de trabajo para solucionar los problemas de red. Las reglas automatizadas activan flujos de trabajo basados en eventos de red, alineándose con un enfoque de observabilidad proactiva.</p>
<p><u>Applications Manager</u></p>	<p>Monitoree el estado y la disponibilidad de sus servidores, equipos virtuales, infraestructura de contenedores o convergente. Asegúrese de que su rendimiento es óptimo para soportar las aplicaciones críticas que se ejecutan en ellos.</p>
<p><u>Site24x7</u></p>	<p>Obtenga una visibilidad completa del estado y el rendimiento de sus aplicaciones bancarias centrales y de banca electrónica, servidores, sistemas de almacenamiento de datos, redes y sitios web desde una consola unificada.</p> <p>Monitoree los sistemas tradicionales, la nube moderna y la infraestructura nativa de la nube, las aplicaciones que alojan y toda la pila tecnológica para comprender sus dependencias y mapearlas. Utilice la automatización de TI para auto-gestionar las tareas repetitivas y reducir los esfuerzos manuales.</p> <p>Aproveche los datos basados en IA para prever las necesidades de recursos de su creciente infraestructura de TI. Esto incluye planificar la capacidad de sus servidores y recursos en la nube.</p>

<p><u>Endpoint Central</u></p>	<p>Monitoree y gestione los activos informáticos del banco, incluidos el software y el hardware, además de controlar las licencias y garantías, y configure alertas para notificarlo si se detecta algún cambio.</p> <p>Monitorear la ubicación, el estado y el uso de los activos ayudará a reducir los costos operativos, ya que evitará compras innecesarias, pérdidas, robos y depreciación.</p> <p>Brinde a los usuarios un catálogo de aplicaciones que los empleados puedan descubrir e instalar fácilmente, ahorrando así tiempo y reduciendo la necesidad de recurrir al soporte de TI. Garantizar que sólo se utilizan las aplicaciones aprobadas puede ayudar a la organización a seguir cumpliendo las normativas del sector y los requisitos de protección de datos.</p> <p>Obtenga información relacionada con el análisis de endpoints. El servidor de Endpoint Central recopila datos telemétricos de los endpoints, que comprenden el espacio en disco, el uso de la CPU, el uso de la memoria, la garantía, la antigüedad del dispositivo, el rendimiento de las aplicaciones, entre otros. A los dispositivos se les asigna una puntuación de referencia. Si se detecta que alguno de los dispositivos incumple las puntuaciones de referencia, Endpoint Central sugerirá las acciones adecuadas para resolver los problemas.</p>
<p><u>AD360</u></p>	<p>Automatice rutinas cruciales como el aprovisionamiento de usuarios, el desaproveccionamiento de recursos críticos, el desbloqueo de usuarios y el restablecimiento de contraseñas aprovechando una política de automatización controlada basada en la revisión y aprobación.</p>
<p><u>PAM360</u></p>	<p>Establezca un control estricto sobre el uso compartido de cuentas y endpoints privilegiados para los usuarios adecuados utilizando flujos de trabajo de control de acceso basados en roles, atributos y políticas.</p>

<p><u>AppCreator</u></p>	<p>Identifique y automatice las tareas repetitivas y aumente su eficacia operativa global. Utilizando la interfaz de arrastrar y soltar de la plataforma, personalice sus reglas de negocio, procesos empresariales y flujos de trabajo de forma granular. Saque el máximo partido a sus soluciones de ManageEngine ampliándolas mediante AppCreator. Implemente sin problemas y rápidamente aplicaciones personalizadas con su marca en iOS y Android con un solo clic.</p>
<p><u>ServiceDesk Plus</u></p>	<p>Codifique cada proceso interno o POE en flujos de trabajo visuales sin código que guíen a sus técnicos en cada paso del camino.</p> <p>Minimice los riesgos durante la transformación digital controlando los cambios y liberaciones de TI, con aprobaciones, notificaciones y automatizaciones del flujo de trabajo de código bajo.</p> <p>Incorpore a los interesados multifuncionales a los proyectos y garantice el cumplimiento de los plazos y objetivos fijando hitos y realizando un seguimiento en diagramas de Gantt.</p> <p>Reduzca sus volúmenes de tickets L1 creando y publicando bases de conocimientos exhaustivas en diferentes departamentos como recursos humanos, instalaciones, asesoría legal y finanzas.</p>

Caso de uso 3: Reducir el riesgo cibernético

Una gran empresa financiera se enfrenta a graves amenazas de los [ciberdelincuentes](#). Algunos de sus competidores ya han sido atacados, y se ha robado información sensible sobre pagos, credenciales de clientes y mucho más. La empresa tiene previsto renovar su estrategia de [ciberdefensa](#), aplicar el marco de confianza cero y algunos de los marcos de ciberseguridad más populares para reducir sus riesgos cibernéticos.

Para evitar la violación de su red y sus datos, la empresa debe aplicar las medidas de seguridad necesarias. Esto incluye:

- Disponer de una visibilidad completa de todas las identidades, dispositivos, datos y aplicaciones que acceden a la red.
- Monitorear y analizar todas las entidades y la actividad dentro de la red e identificar las actividades sospechosas o las amenazas.
- Responder a las amenazas y riesgos según proceda, forzando la autorización y autenticación adicionales, restringiendo los privilegios de los usuarios, poniendo en cuarentena los dispositivos, finalizando las sesiones, etc.
- Resolver los problemas de seguridad tomando medidas preventivas y reforzando la seguridad de los endpoints y las cuentas, por ejemplo, restableciendo las credenciales y parcheando las vulnerabilidades.

También necesita disponer de un plan de gestión de incidentes en caso de que los atacantes logren su cometido; para garantizar la continuidad del negocio y el respaldo de los datos en caso necesario.

Cómo se adaptan los productos de ManageEngine:

Productos de ManageEngine	Cómo ayudan
<p><u>AD360</u></p>	<p>Proporcione un acceso seguro con un solo clic a las aplicaciones bancarias importantes con el SSO.</p> <p>Evite los ataques basados en credenciales y el phishing con la autenticación FIDO2 sin contraseña y resistente al phishing en las aplicaciones bancarias.</p> <p>Realice evaluaciones exhaustivas de los riesgos, identifique las amenazas y redúzcalas con recomendaciones prácticas.</p> <p>Asegúrese de que las personas adecuadas tienen el acceso adecuado a los activos de la empresa automatizando la certificación de acceso.</p> <p>Responda activamente a las amenazas detectando al instante anomalías en los inicios de sesión de los usuarios, bloqueos de cuentas y cambios de permisos configurando respuestas automáticas para los incidentes.</p>
<p><u>PAM360</u></p>	<p>Detecte, incorpore, almacene y gestione automáticamente usuarios, cuentas y recursos privilegiados, utilizados tanto por humanos como por software, desde una consola central.</p> <p>Evite los riesgos de seguridad que plantean los privilegios permanentes al utilizar la elevación de privilegios justo a tiempo y los flujos de trabajo con mínimos privilegios para el aprovisionamiento de acceso.</p>

<p><u>Endpoint Central</u></p>	<p>Monitoree continuamente la publicación de parches por parte de diversos proveedores y aplique rápidamente los parches de seguridad según la política de gestión de parches del banco utilizando la función de gestión de parches automatizada.</p> <p>Garantice una gestión de vulnerabilidades basada en el riesgo tanto para los sistemas de información críticos como para los no críticos, de modo que los administradores puedan priorizar las vulnerabilidades en función de métricas como la puntuación CVSS, la disponibilidad de parches y mucho más.</p> <p>Garantice la protección contra el ransomware utilizando algoritmos de detección de comportamientos basados en ML para detectar y analizar alteraciones inusuales de los archivos en sus endpoints que se asemejen a un ataque de ransomware. Determine si se trata de un verdadero positivo o de un falso positivo, inicie el proceso de recuperación de archivos si se trata de un verdadero positivo y, si el proceso se identifica como falso positivo, marque automáticamente este tipo de eventos en el futuro como falso positivo.</p>
<p><u>Log360</u></p>	<p>Utilice el monitoreo de seguridad en tiempo real para supervisar sus conexiones VPN y buscar inicios de sesión remotos sospechosos.</p> <p>Detecte instalaciones sospechosas de software y servicios en su red utilizando el motor de correlación basado en reglas.</p> <p>Aproveche el análisis de amenazas avanzado basado en el conocimiento y las funciones de MITRE ATT&CK para detectar amenazas internas y externas.</p> <p>Detecte señales de amenazas internas y de compromiso de cuentas monitoreando actividades como accesos inusuales al sistema, horas de acceso inusuales, accesos o modificaciones inusuales de archivos, errores de autenticación excesivos, instalaciones de software inusuales, entre otros.</p> <p>Utilice los flujos de trabajo automatizados para incidentes y el módulo de tickets para agilizar la respuesta y la corrección de amenazas.</p>

<p><u>Firewall Analyzer</u></p>	<p>Monitoree las políticas de firewall en busca de anomalías, que pueden generar brechas en la seguridad de la red. Elimine todas las políticas no deseadas y ajuste las políticas válidas para mejorar el rendimiento del firewall.</p>
<p><u>ADAudit Plus</u></p>	<p>Obtenga una visibilidad completa de todas las actividades en su AD, Azure AD, servidores de archivos (Windows, NetApp, EMC, Synology, Hitachi, Huawei, Amazon FSx y QNAP), servidores Windows y estaciones de trabajo con la ayuda de más de 250 informes y alertas en tiempo real.</p>
<p><u>Site24x7</u></p>	<p>Ofrezca una experiencia digital segura a sus clientes monitoreando las fechas de caducidad de los dominios y los certificados SSL.</p> <p>Analice su sitio web con regularidad para detectar la inyección de contenidos maliciosos, imágenes, scripts, iFrame y otros elementos que contribuyan al phishing y la desfiguración del sitio.</p> <p>Prevenga las amenazas a la seguridad detectando proactivamente las vulnerabilidades del firmware en sus redes bancarias críticas y obteniendo información actualizada sobre la disponibilidad de parches. Proteja su red frente a posibles amenazas y supervise el cumplimiento de las normas del sector, como Cisco IOS, SOX, HIPAA o PCI DSS, y de cualquier política organizacional personalizada mediante el cumplimiento de la configuración de red.</p>
<p><u>ServiceDesk Plus</u></p>	<p>Integre con varias soluciones de seguridad de TI y de ITOM para recibir alertas en tiempo real y crear tickets de incidentes en ServiceDesk Plus.</p> <p>Coordine su respuesta a incidentes de ciberseguridad alertando a los técnicos de TI, a los analistas del SOC y a los ejecutivos corporativos a través de múltiples canales como Microsoft Teams y Slack.</p> <p>Establezca el contexto desde el principio asociando los CI a los incidentes y analizando las dependencias críticas y el impacto descendente.</p>

Caso de uso 4:

Proteger los datos financieros críticos

Una organización financiera global, que cuenta con múltiples sucursales en todo el mundo, se enfrenta al reto de proteger sus datos financieros. El [creciente número de violaciones de datos](#), las complejas normativas del sector y los mandatos de privacidad han dificultado la [gestión y protección de los datos críticos de la organización](#).

Además, la organización cuenta con múltiples socios y proveedores externos para [gestionar sus operaciones en todo el mundo](#). Esto significa que los datos son aún más vulnerables, por lo que es importante garantizar un control de acceso adecuado y evitar la transmisión no autorizada y la [filtración de datos](#).

Las organizaciones financieras como la suya tienen que adherirse a marcos de cumplimiento específicos del sector como [PCI DSS](#), GLBA, GDPR, FISMA, SOX, y leyes de privacidad de datos geo-específicas como GDPR, CCPA, POPIA, etc. Por tanto, la organización tiene que realizar auditorías de datos periódicas y elaborar informes personalizados para evaluar la eficacia de sus [prácticas de protección](#) de datos y garantizar el cumplimiento de estos requisitos normativos específicos.

Cómo se adaptan los productos de ManageEngine:

Productos de ManageEngine	Cómo ayudan
<p><u>Data Security Plus</u></p>	<p>Realice análisis de contexto para descubrir archivos importantes relacionados con las operaciones bancarias y clasifíquelos en función de sus vulnerabilidades.</p> <p>Monitoree continuamente el acceso y las modificaciones realizadas en estos archivos sensibles, y automatice las respuestas inmediatas a incidentes de seguridad como ataques de ransomware, intentos de exfiltración de datos, anomalías en la transferencia de archivos, entre otros.</p>
<p><u>Endpoint DLP Plus</u></p>	<p>Automatice la inspección de contenidos exhaustiva para localizar todos los datos sensibles estructurados y no estructurados, incluida la propiedad intelectual y la información personal, como las cuentas financieras.</p> <p>Una vez identificados los datos sensibles, se pueden definir reglas para definir exactamente qué aplicaciones en la nube se pueden utilizar para subir datos. Endpoint DLP Plus puede impedir automáticamente que el contenido sensible se exporte a través de navegadores web no autorizados a varias aplicaciones de almacenamiento en la nube de terceros.</p>
<p><u>Log360</u></p>	<p>Automatice el monitoreo de los datos de log de firewalls, routers, switches, estaciones de trabajo, servidores y aplicaciones críticas, y reciba notificaciones cada vez que se produzca una infracción de la normativa, una actividad sospechosa o indicios de una violación o exfiltración de datos.</p> <p>Use los informes de cumplimiento out-of-the-box para demostrar el cumplimiento de los requisitos establecidos en las normativas, simplificando así las auditorías de seguridad.</p>

<p><u>EventLog Analyzer</u></p>	<p>Recopile, monitoree y analice los datos de log para la gestión del cumplimiento.</p> <p>Exporte informes de cumplimiento exhaustivos en cualquier formato, modifique las plantillas de informes de auditoría de cumplimiento existentes o cree informes de cumplimiento personalizados para satisfacer los requisitos de las regulaciones.</p> <p>Además, archive los datos de log por períodos de tiempo personalizados para cumplir con los requisitos cruciales de archivado de logs.</p>
<p><u>ADAudit Plus</u></p>	<p>Manténgase al tanto de los accesos a los archivos y los cambios de permisos en los sistemas de archivos de Windows, NetApp, EMC, Synology, Hitachi, Huawei y Amazon FSx para Windows y QNAP con la ayuda de informes, alertas instantáneas y análisis del comportamiento de los usuarios.</p>
<p><u>AD360</u></p>	<p>Controle los derechos de acceso a los datos monitoreando los cambios de propietario y permisos de las carpetas, y reciba alertas sobre los cambios en archivos y carpetas críticos por correo electrónico y SMS.</p> <p>Evite el acceso no autorizado a los datos financieros aprovechando las funciones de ML de ADAudit Plus para detectar volúmenes inusuales de cambios en archivos y cambios que se producen en momentos inusuales.</p> <p>Proteja los datos financieros confidenciales aplicando distintos factores de autenticación para diferentes usuarios en función de factores de riesgo como la dirección IP, la hora de acceso, el dispositivo y la geolocalización con un control de acceso automatizado basado en el riesgo.</p> <p>Revise y valide periódicamente los derechos de acceso de las identidades a los datos financieros para garantizar que sólo las personas autorizadas tienen acceso a la información sensible, satisfaciendo así los requisitos de cumplimiento.</p>

<p><u>Endpoint Central</u></p>	<p>Coloque las aplicaciones móviles en contenedores para uso exclusivo de la empresa, de forma que estén cifradas y separadas de otras aplicaciones. Esto ayuda a borrar la aplicación contenedorizada de forma remota o a hacer que los datos sean ilegibles. Evite la fuga de datos a través de portapapeles, copias de seguridad en la nube, USB, entre otros.</p> <p>Esta solución permite identificar y clasificar rápidamente los datos mediante técnicas como huellas dactilares, expresiones regulares, filtrado por extensión de archivo y búsqueda por palabra clave. Además, Endpoint Central clasifica los datos confidenciales en función de factores como el origen y el formato utilizando una variedad de plantillas prediseñadas y personalizadas.</p>
<p><u>PAM360</u></p>	<p>Cree y asigne usuarios con roles específicos y niveles de acceso definidos. Asegúrese de que solo los usuarios autorizados tengan acceso para ver, editar o gestionar los "recursos" permitidos (los recursos asignados a ellos) en función de sus roles.</p>

Caso de uso 5: **Aprovechar el análisis de datos para tomar decisiones informadas**

Una popular institución financiera quiere mejorar su eficiencia operativa. Su objetivo es aprovechar los datos existentes para extraer información significativa que les permita tomar decisiones fundamentadas para optimizar sus operaciones, mejorar la experiencia del cliente y reducir los riesgos, entre otras cosas.

Cómo se adaptan los productos de ManageEngine:

Productos de ManageEngine	Cómo ayudan
<p><u>Analytics Plus</u></p>	<p>Genere informes preconfigurados y personalizados para explorar los puntos débiles financieros e iniciar acciones correctivas para racionalizar los costos operativos.</p> <p>Acelere los planes de digitalización y modernización con información precisa para las instituciones bancarias que están abandonando gradualmente los sistemas heredados. Acceda a información esencial sobre la arquitectura, las relaciones y el uso de los sistemas para actualizar la infraestructura bancaria y completar las iniciativas de transformación con mayor rapidez.</p> <p>Aproveche el análisis predictivo para diseñar el crecimiento prediciendo las cargas de trabajo y las necesidades de infraestructura de cada sucursal.</p> <p>Analice los datos de las pruebas sintéticas para detectar problemas en los sistemas actuales e idear formas de eliminarlos invirtiendo en nueva tecnología.</p> <p>Correlacione los datos de la gestión de aplicaciones, redes, servidores y configuraciones, con el fin de identificar los sistemas que corren el riesgo de fallar. Esta información se puede utilizar para mitigar eficazmente los riesgos y trasladar las cargas de trabajo a servidores de respaldo, con el fin de garantizar la disponibilidad de los servicios bancarios 24/7.</p> <p>Conéctese con cualquier aplicación o fuente de datos a través de conectores de datos y API para permitir a los usuarios obtener una visión más profunda de los datos de los clientes. Esto puede ayudar a los bancos a ofrecer servicios y soluciones personalizados a los clientes para fomentar la fidelidad y la confianza, como recomendaciones de inversión, sugerencias financieras o consejos para elaborar un presupuesto inteligente. Cómo se adaptan los productos de ManageEngine:</p>

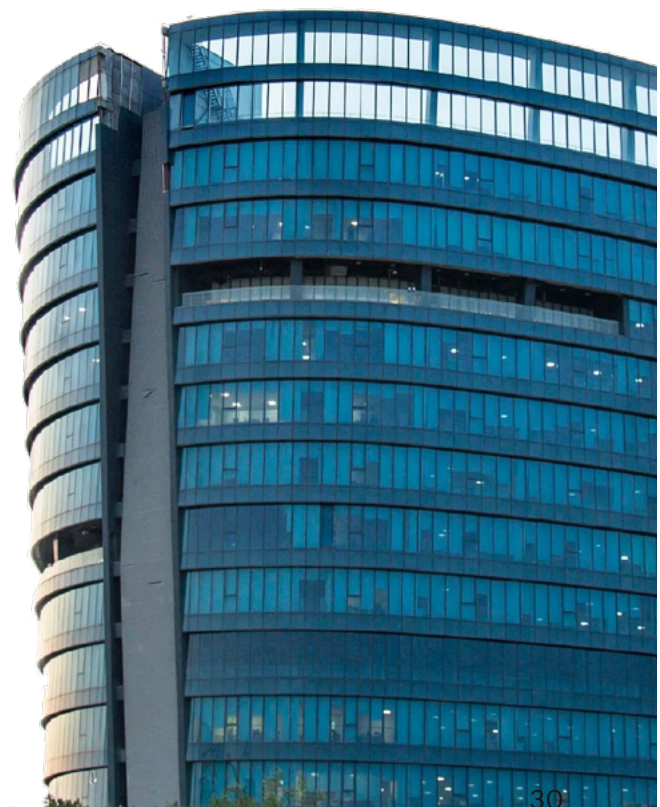


Acercas de ManageEngine

ManageEngine ofrece el paquete de software de gestión de TI más completo de la industria. Tenemos todo lo que necesita (más de 120 productos y herramientas gratuitas) para gestionar todas sus operaciones de TI, incluidos servidores, redes, aplicaciones, mesas de servicio, AD, seguridad, desktops y dispositivos móviles.

Desde el 2002, los equipos de TI como el suyo han recurrido a nosotros en busca de un software asequible, rico en funciones y fácil de usar. Nuestras soluciones on-premises y en la nube fortalecen la TI de más de 280.000 empresas en todo el mundo, incluidas nueve de cada 10 empresas de Fortune 100.

Mientras se prepara para enfrentar los desafíos de gestión de TI que se avecinan, allanaremos el camino con nuevas soluciones, integraciones contextuales y otros avances que solo pueden provenir de una empresa dedicada especialmente a sus clientes. Y como una división de Zoho Corporation, seguiremos trabajando fuertemente para garantizar el estrecho alineamiento entre la TI y su negocio que necesitará para aprovechar las oportunidades en el futuro.



Con la confianza de las principales
organizaciones financieras de todo el
mundo.

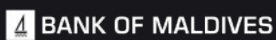
fiserv.



HDFCLife



1ST SECURITY BANK



ManageEngine

una división de Zoho Corp.

Para más información: www.manageengine.com/latam/
| sales@manageengine.com