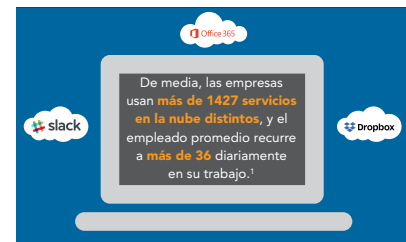


Acceso seguro a las aplicaciones empresariales



La tecnología ha experimentado grandes avances: las antiguas y rudimentarias redes conmutadas por paquetes han pasado a convertirse en una compleja y amplísima gama de soluciones autónomas que actúan en sincronía para distribuir datos de manera global y rápida. La gran variedad de trabajadores que existe en la actualidad accede a aplicaciones empresariales cada vez más distribuidas (es decir, in situ, IaaS y SaaS). Además, la popularidad de las aplicaciones en la nube crece como la espuma. De media, las empresas usan más de 1427 servicios en la nube distintos, y el empleado promedio recurre a más de 36 diariamente en su trabajo.¹



Las arquitecturas de red tradicionales en estrella o hub and spoke, así como los marcos de seguridad casi medieval que aplican, no son suficientes para un mundo cada vez más móvil y en la nube como el actual. La mayoría de las empresas ya no trabajan tras un perímetro de red centralizado tradicional, por lo que el enfoque unilateral de "confiar, pero verificar" no hace sino incrementar los riesgos del acceso a la empresa. Cada usuario o dispositivo necesita autenticación cada vez que solicite el acceso a una aplicación para que este le sea concedido.



Esto cobra especial importancia si se tienen en cuenta las características del panorama de amenazas actual. La ciberdelincuencia es un negocio valorado en un billón de dólares, en el que una única filtración de datos supone un coste de 3,86 millones de dólares.² Quizá resulte más sorprendente el hecho de que más del 40 % de las filtraciones están vinculadas a usuarios autorizados.³ Además, el modelo de empresa típico utiliza más de 500 aplicaciones, muchas de las cuales ponen en riesgo los datos: el 85 % de los datos provienen de aplicaciones de uso compartido de archivos, y el 81 % de los datos se descargan a través de una aplicación que no dispone de cifrado de datos en reposo.⁴ Resulta evidente que la seguridad de las aplicaciones, y la limitación y cualificación de acceso, constituyen dos imperativos que los ejecutivos y los profesionales de seguridad de TI no pueden ignorar.

La mayoría de los altos cargos comprenden ya estos riesgos y están tomando medidas para reforzar la defensa de su organización. Gartner prevé que el gasto global en seguridad alcance los 96 000 millones de dólares en 2018, un 8 % más que en 2017.⁵ No obstante, aunque el gasto en TI sigue creciendo (un 4,3 % con respecto a 2017, y se prevé que alcance los 3,7 billones de dólares en 2018), no basta con añadir soluciones de seguridad a la pila de la empresa.⁶ Es necesario un modelo de acceso seguro que satisfaga los requisitos del entorno y de los trabajadores de hoy en día.



¿Cómo puede el equipo de TI reforzar el nivel de seguridad de la empresa sin que esto suponga complejidad adicional? Akamai Enterprise Application Access es una solución de eficacia probada que se ha diseñado para que los equipos de TI puedan:

1. Mejorar radicalmente la seguridad



Mantenga fuera de la red a todos los usuarios ofreciendo un acceso a nivel de aplicación, en lugar de a nivel de red. Cierre el firewall o el grupo de seguridad a todo el tráfico entrante y haga que las direcciones IP de su aplicación sean invisibles a Internet. Añada autenticación multifactorial (MFA) a cualquier aplicación con un solo clic.

Acceso seguro a las aplicaciones empresariales



2. Consolidar y simplificar las tecnologías de acceso



Proporcione un inicio de sesión único optimizado a los usuarios en todas las aplicaciones empresariales, independientemente de que sean locales, IaaS o SaaS. Una los controladores de distribución de aplicaciones (ADC), las tecnologías de optimización de WAN, las VPN y la autenticación multifactorial en una sola herramienta que no requiere configurar hardware interno ni cambios en la red (como reglas de cortafuegos, listas blancas de direcciones IP, etc.). Permita a los usuarios acceder a las aplicaciones desde cualquier dispositivo sin necesidad de software adicional, ni siquiera VPN ni plugins.

3. Dejar de configurar dispositivos

Olvídese de la gestión de la configuración del lado del cliente con una herramienta que no requiere actualizaciones ni mejoras de software, ni siquiera hardware para proporcionar acceso.

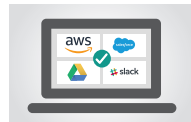


4. Simplificar la elaboración de informes

Implemente un único portal de gestión donde se ofrezcan visibilidad, control, auditorías e informes de cumplimiento normativo detallados, ya sea con informes preincorporados o integrándolos con sus herramientas de SIEM actuales.



5. Optimizar el tiempo



Configure nuevos usuarios y aplicaciones en minutos, no en días. A través de un portal web, puede conectar varios IdP para integrar sus soluciones existentes o una opción nativa. De esta manera, podrá configurar los usuarios con un solo clic, sin necesidad de usar varios dispositivos de hardware o software para otorgar el acceso.

6. Aumentar la satisfacción de los usuarios finales



Evite el uso de varias contraseñas y proporcione acceso a la aplicación a través de un único portal web. Los usuarios disfrutarán de un inicio de sesión sin problemas a todas las aplicaciones a las que tengan acceso, en cualquier dispositivo y desde cualquier punto del planeta. Reduzca la latencia para fomentar una mayor adopción de la aplicación y recibir menos solicitudes de asistencia técnica de TI. Los usuarios dejarán de experimentar retrasos, al no tener que esperar a que TI les envíe el hardware específico necesario.

El resultado es un método de acceso a aplicaciones más seguro que simplifica la gestión de TI y la experiencia de los usuarios finales.

Para obtener más información sobre Enterprise Application Access e iniciar una prueba gratuita, visite akamai.com/eea.

FUENTES

- 1) <https://www.skyhighnetworks.com/cloud-security-blog/12-must-know-statistics-on-cloud-usage-in-the-enterprise/>
- 2) Ponemon Institute, 2018 Cost of Data Breach Study: Global Overview: <https://www.ibm.com/security/data-breach>
- 3) <https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf>
- 4) <https://blog.trendmicro.com/how-your-enterprise-applications-could-be-putting-your-company-at-risk/>
- 5) <https://www.gartner.com/newsroom/id/3836563>
- 6) <https://www.gartner.com/newsroom/id/3811363>



Akamai, la mayor plataforma de entrega en la nube del mundo y en la que confían más usuarios, ayuda a los clientes a ofrecer las mejores y más seguras experiencias digitales en cualquier dispositivo, en cualquier momento y en cualquier lugar. La plataforma ampliamente distribuida de Akamai ofrece una escala inigualable para garantizar a sus clientes el máximo rendimiento y protección frente a las amenazas. La cartera de soluciones de rendimiento web y móvil, seguridad en la nube, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente excepcional y una supervisión ininterrumpida durante todo el año. Para descubrir por qué las principales instituciones financieras, líderes de retail online, proveedores de contenidos multimedia y de entretenimiento, y organizaciones gubernamentales confían en Akamai, visite www.akamai.com, blogs.akamai.com, o siga a @Akamai en Twitter. Puede encontrar los datos de contacto de todas nuestras oficinas en www.akamai.com/locations. Publicado en agosto de 2018.