
okta
Seguridad de la plantilla híbrida
ADAM121/ADOBE

Establecer confianza para asegurar el trabajo dinámico en el negocio pospandémico

Las empresas deben comprender y planificar eficazmente la próxima etapa del lugar de trabajo pospandémico, con identidad y seguridad vinculadas. Afortunadamente, la ayuda está al alcance de la mano

La pandemia de Covid-19 ha revolucionado nuestra forma de trabajar. Muchos empleados cambiaron un espacio de oficina, donde sus sistemas de TI estaban protegidos por seguridad perimetral, por un hogar o un entorno remoto con conectividad inestable y desafíos en materia de seguridad.

La tarea inicial de los responsables de TI era permitir ese cambio a gran velocidad. Con las reglas ahora más flexibles, el siguiente reto es cómo construir sobre ese cambio drástico y crear un acceso flexible a los sistemas y datos para permitir a los empleados trabajar de forma segura donde les convenga.

La transición tiene riesgos inherentes si las organizaciones se equivocan, pero enormes ventajas si lo hacen bien. Los CIO quieren evitar las violaciones de datos, pero el negocio puede beneficiarse de este nuevo modelo dinámico de oficina –menores costos inmobiliarios, una plantilla más feliz con un mejor equilibrio entre la vida laboral y personal, y el acceso al talento sin restricciones por ubicación, son solo algunos de los potenciales beneficios.

Pero, ¿cómo pueden los jefes de TI proteger los datos al tiempo que permiten la flexibilidad necesaria de acceso a las aplicaciones y sistemas para garantizar una buena experiencia de trabajo, dondequiera que se encuentren los usuarios? Para empezar, necesitan crear un lugar de trabajo híbrido que conecte de forma segura a las personas adecuadas con las tecnologías apropiadas, en el momento oportuno –y necesitan un socio con la comprensión y la experiencia de la vida real de ese nuevo entorno de trabajo dinámico.

El proveedor de identidad digital Okta conoce los retos de seguridad a los que se enfrentan las empresas y ofrece las soluciones tecnológicas para superarlos

Trabajo pospandémico

Okta, el principal proveedor de identidad digital de confianza, cuenta con más de 10.000 clientes en todo el mundo y conoce los retos de seguridad a los que se enfrentan las empresas, con la experiencia de cómo ofrecer las soluciones tecnológicas necesarias para superarlos.

La experiencia de Okta en el uso de tecnologías clave, como la gestión de identidad y acceso, la seguridad de confianza cero y la autenticación multifactor, está proporcionando un camino para que muchas empresas establezcan sus acuerdos de trabajo pospandémico.

“Durante el confinamiento, muchas empresas tuvieron una reacción instintiva en la que fue necesario implementar tecnología de seguridad para permitir a su plantilla trabajar desde casa”, dice Ian Lowe, director de soluciones de marketing para EMEA en Okta.

“Pero ahora tenemos una verdadera contraposición entre las organizaciones. Algunas abogan por un enfoque híbrido o de prioridad digital que permite a los empleados trabajar desde donde quieran”, añade. “Otras están dando un paso atrás y revisando la tecnología que implementaron de forma precipitada y mirando desde una perspectiva integral a su enfoque de la gestión de identidad

para permitir la flexibilidad. Otro grupo está exigiendo a sus empleados que vuelvan a la oficina como si fuera la época anterior a la pandemia".

Muchas organizaciones optaron por la autenticación multifactor para acceder de forma segura a las aplicaciones en la nube, pero ahora se están dando cuenta de que hay más que ganar evolucionando hacia un lugar de trabajo híbrido y dinámico.

Confianza en el trabajo

Aunque algunas empresas quieran animar a los empleados a volver a la oficina, la verdad es que la mayoría se enfrenta a una nueva realidad que combina múltiples entornos de trabajo, opciones de tecnología y estilos de trabajo que se adaptan mejor a las necesidades individuales de los empleados.

Otros empleados, por su parte, se oponen a los empresarios que quieren volver al mismo entorno prepandémico. Lowe afirma que hasta el 70% de los empleados quieren seguir teniendo opciones. Las organizaciones deben evaluar cómo hacer que este nuevo enfoque dinámico funcione para proporcionar la flexibilidad, pero también deben mitigar el riesgo.

"Sea como sea, hay una pieza fundamental que las empresas deben poner en marcha, y que Okta llama ´confianza en el trabajo´", agrega Lowe.

Para proporcionar la tecnología que respalda el enfoque de "confianza en el trabajo", el marco de confianza cero de Okta ofrece a las organizaciones una visión integral de su estrategia de identidad y seguridad.

Gartner define la seguridad de confianza cero como "nunca confíes, siempre verifica". El objetivo es proteger a todos los usuarios, estén donde estén, en cualquier momento, independientemente del dispositivo que utilicen.

"La confianza cero es fundamental incluso para las organizaciones que quieren volver a un entorno de trabajo prepandémico, porque todavía tienen trabajadores contingentes que pueden no ser capaces de regresar o están utilizando sus

Las aplicaciones de menor prioridad se pueden proteger con un simple nombre de usuario y contraseña, mientras que las aplicaciones de misión crítica pueden tener protección adicional a través de autenticación multifactor o autenticación biométrica

PROSTOCK-STUDIO/ADOBE

propios dispositivos. La confianza cero también es vital para ofrecer un enfoque híbrido o de prioridad digital en el que los empleados puedan trabajar desde cualquier lugar", dice Lowe.

Las organizaciones tuvieron que cambiar rápidamente de forma escalable durante la pandemia, modificando las políticas y realizando mejoras y actualizaciones en sus recursos tecnológicos para permitir el teletrabajo. La adopción y la ampliación de tecnologías de colaboración como Zoom o Slack, por ejemplo, se convirtieron en una práctica habitual y aumentaron los retos de seguridad al compartir datos en un entorno de trabajo distribuido.

Según el informe *Businesses at Work* de Okta, sus clientes utilizan un promedio de 88 aplicaciones, y solo el uso de Zoom creció más de 45% entre marzo y octubre de 2020.

"Si nos fijamos en la transformación digital y colaboración en el lugar de trabajo prepandemia, la mayoría de esos proyectos tardaban, en promedio, más de 200 días para entregar una nueva herramienta de colaboración al cliente", dice Lowe.

"Cuando se produjo la pandemia, esos proyectos de 200 días se entregaron en tan solo 10 días y medio –un adelanto significativo. El equipo de TI tuvo que pasar de la velocidad de la luz a la velocidad disparatada. Sin la seguridad necesaria para soportar esa transición, muchas empresas no tuvieron más remedio que aumentar sus licencias de autenticación multifactor".

"La confianza cero es vital para ofrecer el enfoque híbrido o de prioridad digital donde los empleados pueden trabajar desde cualquier lugar"
Ian Lowe, Okta

Apertura del perímetro

Muchas de esas implementaciones rápidas fueron soluciones puntuales, y ahora las organizaciones están dando un paso hacia atrás para mirar de manera integral cómo se ha abierto el perímetro de sus negocios.

"Se han introducido nuevas aplicaciones que requieren que se establezcan controles. Las personas trabajan a distintas horas, desde diferentes lugares y a través de direcciones IP desconocidas. Hay muchos retos de seguridad a los que nos enfrentamos ahora. La complejidad y la velocidad del cambio han aumentado drásticamente", dice Lowe.

Él dice que una pregunta que debe hacerse cada responsable de TI es: "¿Cuál es la experiencia ideal que busco ofrecer?".

Las organizaciones deben proteger múltiples identidades y ofrecer una solución perfecta para los usuarios, ya sea accediendo a aplicaciones o proporcionando registro o incorporación a sistemas. Trabajando con Okta, las empresas pueden consolidar diferentes bases de datos de identidad e integrarlas con las aplicaciones necesarias.

"La consolidación ofrece una visión de 360 grados, completa y holística, de la identidad y seguridad, bien como una implementación más sencilla de la política en diferentes aplicaciones. Se puede aumentar la seguridad al extraer información de otros sistemas más fácilmente, ya que se dispone de una base de datos central de identidad, que permite extraer señales de riesgo de diferentes aplicaciones mediante una mayor integración", afirma Lowe.

Por ejemplo, la empresa de fitomejoramiento KWS trabajó con Okta para ayudar en el despliegue seguro de Office 365 para 4.500 usuarios en todo el mundo que utilizan el inicio de sesión único y la autenticación multifactor. Okta coordinó todas las identidades de usuario al mismo tiempo que facilitaba el uso del nuevo sistema de forma segura.

Los beneficios incluyeron el ahorro de 125 horas al mes en tareas de incorporación y la habilitación de 187 aplicaciones integradas listas para su uso en la nube y en las instalaciones.

Una visión integral

Proporcionar esa visión completa de las identidades y validarlas remotamente supone un cambio de rumbo para muchas empresas que antes dependían de procesos manuales para incorporar y autenticar a sus nuevos empleados. A menudo, se les pedía que acudieran a la oficina con algún tipo de identidad, como un permiso de conducir, y que se reunieran con un representante de RRHH antes de que se les diera acceso a los edificios y sistemas informáticos.

“Si tienes una visión integral y las integraciones ya realizadas, bien como el control de la gestión del ciclo de vida de la identidad para soportar la incorporación remota, puedes tener una experiencia mejor que en la época de prepandemia. Hoy se puede automatizar el proceso de inicio-cese-traslado y reducir la carga en el servicio de asistencia de TI”, afirma Lowe.

Sin embargo, reducir la carga de soporte y permitir la productividad desde el primer día solo merece la pena si hay seguridad.

“En el entorno de trabajo remoto, tenemos un gran número de vectores de ataques potenciales que se han abierto, incluyendo el phishing y ataques de malware. Tener una visión completa de la identidad permite implementar diferentes políticas de seguridad para diferentes aplicaciones”, dice Lowe.

Las aplicaciones de menor prioridad se pueden proteger con un simple nombre de usuario y contraseña, por ejemplo, mientras que las aplicaciones de misión crítica tienen protección adicional con la autenticación multifactor, como una

PROSTOCK-STUDIO/ADOBE

contraseña de un solo uso enviada al teléfono del usuario o la autenticación biométrica.

“Tener este nivel de flexibilidad es fundamental cuando los empleados ya no están en la oficina y no se conoce el perímetro”, dice Lowe.

La carga de seguridad puede aliviarse porque es posible tener una única política automatizada de reestablecimiento de contraseñas, por ejemplo, lo que reduce aún más la carga de trabajo del soporte de TI.

Las mejores prácticas para planificar

Para ayudar a planificar, Okta proporciona servicios profesionales y guías de mejores prácticas. Hay pasos clave que las empresas deben dar para garantizar un entorno de trabajo dinámico, que incluye hacer preguntas como:

- ¿Qué aspecto tiene mi escenario de identidad y dónde se encuentran mis identidades?
- ¿Qué aspecto tiene mi ecosistema tecnológico?
- ¿Cuál es el proceso de RRHH y la experiencia de incorporación ideal?
- ¿Cuál es mi experiencia ideal de acceso a las aplicaciones de la plantilla?
- ¿Cuál es la cultura empresarial y cómo afecta a la experiencia?

“Una vez que se define la experiencia y se conoce la aplicación y el escenario de identidad, se puede empezar a ver qué tecnología hay que implementar para apoyar esa visión”, dice Lowe.

Una vez que las organizaciones tengan una visión unificada de la identidad y la seguridad, podrán conectar diferentes tecnologías que examinarán las señales de riesgo, como la hora del día en que los empleados se conectan o las direcciones IP típicas y atípicas, para poder crear un perfil de la identidad de los empleados.

“Okta es compatible con múltiples socios que nos dan esas informaciones y las organizaciones pueden empezar a automatizar las respuestas a comportamientos inusuales de usuarios y señales de riesgo”, dice Lowe. “El acceso puede ser bloqueado sin intervención humana o la autenticación puede ser reforzada con más validación, requerida antes de que un empleado obtenga acceso”.

La multinacional Imerys, especializada en la producción y procesamiento de minerales industriales, trabajó con Okta para reducir su carga operativa cuando adoptó la transformación digital con un enfoque global basado en la nube para 13.000 empleados.

Okta ayudó en la gestión segura de identidad y la gestión del ciclo de vida, bien como aceleró la incorporación y el cese de empleados a través de la automatización. Los derechos de acceso se manejan de manera específica con inicio de sesión único (SSO) y autenticación multifactor, proporcionando medidas de seguridad avanzadas basadas en el dispositivo, la ubicación o los contextos de red. Los empleados no quedan excluidos de las cuentas de modo innecesario y se reduce la carga del soporte de TI, al tiempo que se mejora la seguridad.

Okta Integration Network

Muchas empresas tienen un entorno híbrido complejo con una mezcla de aplicaciones locales y en la nube, pero a los empleados no les importa dónde residen sus datos, solo quieren un acceso sin problemas para hacer el trabajo.

Una vez que las organizaciones tengan una visión unificada de la identidad y la seguridad, podrán conectar diferentes tecnologías que examinarán las señales de riesgo – como la hora del día en que los empleados se conectan, o las direcciones IP típicas y atípicas– para poder crear un perfil de la identidad de los empleados

Al elegir Okta, las empresas pueden beneficiarse al permitir el trabajo dinámico a sus empleados mediante la autenticación de identidades en la nube o un entorno local. Okta también ofrece soporte a la gestión de identidad del cliente para sitios web de comercio electrónico en una única plataforma.

La Okta Integration Network ofrece más de 7.000 aplicaciones integradas listas para usar, incluidas aplicaciones de marketing y suites de colaboración como Google Workspace, Office 365 y Slack.

“Este es un diferencial único para nosotros, al igual que nuestro soporte a estándares abiertos. Esto nos permite integrarnos con otras aplicaciones en la nube para el inicio de sesión único y la autenticación multifactor. Okta también trabaja con estándares heredados para la integración local”, dice Lowe.

Las empresas pueden adquirir productos empaquetados como la autenticación multifactor, la gestión del ciclo de vida o el directorio universal para uso inmediato, lo que permite una solución unificada de seguridad e identidad.

Si una empresa desea integrar una aplicación que no es compatible con Okta, los desarrolladores pueden utilizar las interfaces de programación de aplicaciones (API) de Okta y los kits de desarrollo de software (SDK) y ampliarlos donde consideren oportuno, por lo que no hay límites a la elección de la aplicación, aprovechando la adquisición de AuthO en 2021.

“Tenemos un portal de desarrolladores y una red de soporte que lo permite”, dice Lowe. “La mayoría de las empresas no tienen equipos de desarrollo con experiencia en seguridad o identidad. Podemos posibilitar que los desarrolladores se conviertan en expertos a través de esos conjuntos de herramientas. Ayudamos a las empresas a través de nuestra plataforma tecnológica a ofrecer seguridad e identidad a cualquier caso de uso que tengan”.

La agencia de publicidad WPP utilizó Okta para establecer una base mínima de seguridad y estandarizar los controles de acceso. Después de la pandemia, la empresa proporciona un acceso rápido y seguro a una serie de nuevas soluciones de trabajo remoto para sus usuarios.

Elige tu política de trabajo

La ventaja para las empresas que trabajan con Okta es que los empleados pueden trabajar de la forma que más les convenga, y se liberan los locales, reduciendo el alquiler. La base del enfoque de “confianza en el trabajo” permite a las empresas ofrecer cualquier tipo de política de trabajo que deseen –en la oficina, remoto o híbrido.

“El trabajo dinámico consiste en la flexibilidad para establecer diferentes políticas de acceso en función de lo que se esté haciendo, ya sea en casa o en una oficina, de modo que se puedan adaptar las políticas de acceso según varíe el riesgo, dependiendo de la ubicación”, dice Lowe.

Este enfoque unificado de la identidad es fundamental para crear un entorno dinámico y una experiencia positiva del usuario.

“Si una empresa tiene una política de autenticación multifactor general para acceder a cada aplicación, se convierte en una experiencia de usuario bastante terrible”, dice Lowe.

Al trabajar con Okta, las empresas pueden conocer y planificar eficazmente la próxima etapa del lugar de trabajo pospandémico.

Lowe concluye: “Hemos pasado por una evolución de la vida laboral, desde la prepandemia en la oficina hasta el trabajo remoto y ahora un entorno dinámico e híbrido. Para ofrecer la flexibilidad y escalabilidad requeridas para este nuevo entorno, se necesita un enfoque esencial –confianza en el trabajo fundamentada en la seguridad de confianza cero”. ■

ART_PHOTO/ADOBE