INFINYT

Bases para implementar Autenticación Sólida en Call Centers

Introducción

El entorno de los call centers es acelerado y gestiona grandes volúmenes de transacciones a diario. Los call centers suelen operar las 24 horas del día, los 7 días de la semana, con agentes de servicio al cliente que inician y cierran sesión en sistemas clave, en varios turnos.

Los agentes de los cal centers necesitan un acceso rápido y seguro a datos importantes para que puedan maximizar rápidamente la satisfacción del cliente y también lograr métricas clave de éxito del call center, incluido el tiempo mínimo del cliente en la cola de llamadas; resolución del primer contacto; y tiempo medio de atención. Con una alta rotación de empleados, picos estacionales y otras dinámicas comerciales desafiantes, el ímpetu para lograr que los empleados del call center sean productivos rápidamente y garantizar que los controles de seguridad estén implementados es de suma importancia.

Los entornos de los call centers pueden beneficiarse enormemente de un enfoque seguro pero simple para verificar la identidad de sus agentes antes de proporcionar acceso a sistemas críticos para que puedan brindar rápidamente un excelente servicio al cliente.

La autenticación basada en teléfonos móviles es riesgosa

Dada la sensibilidad de la Informacion de Identificación Personal (PII) y de otros datos relacionados accesibles por los agentes de servicio al cliente, proteger adecuadamente esos datos es fundamental.

Cualquiera que acceda a información confidencial normalmente debe seguir los requisitos reglamentarios para una autenticación sólida, incluida la autenticación de dos factores (2FA). Sin embargo, muchas ofertas de autenticación de dos factores requieren el uso de un teléfono móvil.

El uso de teléfonos móviles dentro de los call centers plantea desafíos particulares debido a los riesgos de seguridad, productividad y cumplimiento.

Los dispositivos personales en un cal center impactan en el rendimiento

1 Muchos empleados usan sus dispositivos personales para hacer llamadas, enviar mensajes de texto o revisar sus cuentas de redes sociales mientras están en funciones. Para maximizar la productividad, el uso de dispositivos móviles personales solo debe permitirse fuera del ámbito del call center.

Amenazas internas de los trabajadores del call center con acceso a información confidencial

2 Se confía en los agentes del call center con acceso a datos financieros y de clientes altamente confidenciales. Con datos tan confidenciales y protegidos en juego, es fundamental que los dispositivos móviles personales no se utilicen para capturar imágenes y venderlos a actores malintencionados. El uso de dispositivos móviles para 2FA permite a los empleados del call center capturar fácilmente datos confidenciales en la cámara sin ser notados, lo que pone a la organización en un gran riesgo.

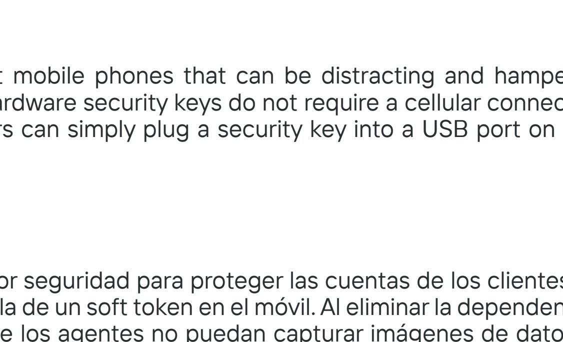
Requisitos de cumplimiento estrictos para proteger los datos y la privacidad

3 No se puede subestimar la importancia del cumplimiento en el call center. El cumplimiento es un factor para las organizaciones en casi todos los sectores siempre que se almacenan o acceden a datos confidenciales. Los call centers generalmente se basan en la PII para verificar las credenciales de la persona que llama y necesitan garantizar que la información, como los números de documento, los números de tarjetas bancarias, la fecha de nacimiento o las direcciones de correo electrónico, esté protegida. Por lo tanto, es fundamental garantizar que se habilite una autenticación sólida para que los agentes del call center cumplan con todas las regulaciones relevantes durante cada instancia de participación del cliente.

La autenticación de dos factores mediante dispositivos móviles expone a los call centers a numerosos riesgos. Las brechas recientes también han demostrado que el uso de SMS, dispositivos móviles y mecanismos relacionados dejan a las organizaciones y a sus usuarios altamente vulnerables al robo de datos. Dado que los call centers son cruciales para la satisfacción del cliente y la viabilidad de una organización, es fundamental que se habilite una autenticación sólida para proteger datos valiosos.

Beneficios de una autenticación sólida con llaves de seguridad

Las llaves de seguridad basadas en hardware ofrecen una alternativa moderna, eficaz y rentable al uso de teléfonos móviles como mecanismo 2FA. La credencial de un usuario se almacena en forma segura en la llave y no se puede extraer, las llaves de seguridad basadas en hardware deben ser un componente central de una solución de seguridad sólida.



Las llaves de seguridad son ideales para entornos con restricciones móviles, como los call centers. Una llave de seguridad que soporta multiples protocolos de autenticación en la misma llave puede proporcionar fácilmente la flexibilidad que necesitan los call centers.

Principales beneficios de la implementacion de llaves de seguridad basadas en hardware:

Maximizar la productividad del call center

1 Call centers can enable strong authentication for agents without mobile phones that can be distracting and hamper productivity. Unlike SMS codes and mobile push authentication, hardware security keys do not require a cellular connection, batteries, or any other external dependency to operate. Users can simply plug a security key into a USB port on a computer or other system and touch to authenticate.

Mitigar los riesgos de amenazas internas

2 Las llaves de seguridad basadas en hardware pueden brindar mayor seguridad para proteger las cuentas de los clientes, ofreciendo más tranquilidad que la autenticación basada en SMS o la de un soft token en el móvil. Al eliminar la dependencia de los teléfonos móviles, los call centers pueden garantizar que los agentes no puedan capturar imágenes de datos financieros y de clientes, como números de cuenta, fechas de vencimiento de tarjetas y numerosos detalles que podrían violar la privacidad del cliente.

Alcanzar los estrictos requisitos de cumplimiento

3 Al implementar llaves de seguridad, los call centers pueden proteger de manera efectiva los datos confidenciales y la privacidad del consumidor. Los call centers pueden implementar una solución de autenticación sólida que pueda verificar de forma segura la identidad de los agentes del call center antes de que se les otorgue acceso a PII y otros datos confidenciales, o realizar cambios en la cuenta de un cliente.

Casos de uso de autenticación en Call Centers

Una llave de seguridad basada en hardware, como la multiprotocolo YubiKey, permite a los call centers admitir una variedad de casos de uso de autenticación. YubiKey también se integra con la mayoría de las soluciones de gestión de acceso e identidad (IAM) y de inicio de sesión único (SSO).

Implementación de Yubikey Smart Card para el login en la estación de trabajo

Muchos call centers aprovechan la infraestructura de escritorio virtual (VDI) para mejorar la seguridad y la eficiencia operativa. YubiKey funciona con el software VDI para proporcionar una experiencia de inicio de sesión segura y sin problemas. Para un inicio de sesión más eficiente en el call center, YubiKey se puede implementar como una Smart Card para reemplazar la contraseña de inicio de sesión.

En lugar de ingresar una contraseña para iniciar sesión, un agente del call center simplemente presenta su YubiKey (se puede usar USB o NFC) e ingresa un PIN que rara vez cambia, si es que lo hace alguna vez.

Son muchos los beneficios de implemanet Yubikey como Smart Card para inicio de sesión, incluyendo:

Experiencia de inicio / cierre de sesión más rápida

1 El uso de YubiKeys como Smart Card elimina la necesidad de que los usuarios ingresen nombres de usuario y contraseñas para autenticarse. Los agentes pueden usar PIN fáciles de recordar que no están almacenados en un servidor y no caducan. Si se desconecta una YubiKey, se puede activar un evento de cierre o cierre de sesión para proporcionar una capa adicional de seguridad.

Menos llamadas al centro de soporte de TI

2 Aprovechar la YubiKey para iniciar sesión en una estación de trabajo con un PIN reduce la cantidad de contraseñas que los agentes del call center deben recordar y, por lo tanto, la cantidad de llamadas a soporte cuando se olvidan las contraseñas.

2FA incorporado

3 Las implementaciones de Smart Card cumplen con los requisitos de 2FA. Además, la mayoría de las herramientas de gestión de Identidades tienen compatibilidad con Smart Card incorporadas para permitir el inicio de sesión único y / o la compatibilidad con 2FA.

Flexibilidad para aprovechar herramientas de terceros

4 Con YubiKeys, las herramientas de terceros también se pueden aprovechar para el inicio de sesión 2FA, sin una implementación de Smart Card tradicional.

Autenticación Sólida con controles granulares

5 Las YubiKeys cumplen con los más altos estándares de autenticación, como NIST SP 800-63. Además, en un entorno de Microsoft, el sistema puede reconocer si un operador inicia sesión con una Smart Card o con un nombre de usuario y contraseña. Esto permite otorgar acceso adicional automáticamente cuando el sistema reconoce a un usuario que inicia sesión con una Smart Card.

Herramientas de incorporación administradas localmente

6 Se pueden usar herramientas listas para usar y de terceros para delegar la administración de Smart Cards al personal de primera línea. Los call centers tienen flexibilidad en la forma en que administran los eventos de incorporación, soporte y salida. También hay herramientas disponibles para proporcionar autoservicio, administración local o soporte centralizado para administrar Smart Cards.

Las capacidades de YubiKey agilizan enormemente la implementación de Smart Cards en las organizaciones. Sin embargo, la implementación de YubiKey como una Smart Card requiere un entorno PKI, que puede ser desde sencillo hasta complejo, y se debe tener cuidado al diseñar el entorno para las necesidades específicas del call center.

Opciones sólidas de 2FA con YubiKey

La YubiKey se usa comúnmente para proporcionar un segundo factor de autenticación, como una capa de protección más allá de los nombres de usuario y las contraseñas. Esto proporciona seguridad adicional y cumple con una serie de requisitos normativos y de clientes que deben adoptar los call centers. Con YubiOTP (OTP = One Time Password - código de acceso de un solo uso), YubiKey proporciona capacidades basadas en OTP de uso común, así como capacidades de OTP mejoradas.

La YubiKey también es compatible con los estándares abiertos de autenticación moderna FIDO2 y U2F, en los que Yubico fue pionero, en colaboración con la Alianza FIDO. Estos estándares combinan alta seguridad con facilidad de uso para brindar protección adicional contra ataques de phishing.Las YubiKeys también admiten códigos de acceso de un solo uso basados en tiemp (TOTP) y basados en hash (HOTP) que son comunes en toda la industria. YubiKey no está vinculado a un dispositivo móvil, por lo que es una opción ideal para call centers, ni requiere un entorno PKI.

La YubiKey ofrece múltiples beneficios como solución de 2FA:

Seguridad Sólida

1 Al aprovechar los protocolos de autenticación modernos, la llave de seguridad basada en hardware proporciona una autenticación de segundo factor muy sólida. Además, las YubiKeys proporcionan una solución OTP fuerte y flexible.

Facilidad de Uso

2 Se pierde menos tiempo iniciando sesión en sistemas con YubiKey. Al requerir que un usuario no haga más que tocar la YubiKey en lugar de solicitar, recibir y escribir un código, 2FA acelera significativamente el proceso de inicio de sesión del usuario. Google hizo un estudio intensivo y descubrió que el uso de YubiKeys reducía el tiempo de inicio de sesión en casi un 50%. En un call center donde el tiempo es crítico, este aumento en la eficiencia operativa es significativo. Cuantas más aplicaciones necesite iniciar sesión un agente, más importante se vuelve esto.

Durabilidad

3 Las YubiKeys son extremadamente duraderas. Las llaves no requieren acceso celular o de Internet para funcionar correctamente, por lo que se pueden usar en cualquier entorno. Además, a diferencia de los teléfonos o las aplicaciones, no es necesario actualizarlos ni cargarlos.

Alto ROI

4 La configuración de 2FA la puede realizar uno mismo y no requiere un administrador de TI.
La implementación de llaves para los nuevos empleados del call center es muy rápida y rentable.

Mejores Prácticas para implementar y administrar YubiKeys en un call center

UPara maximizar el éxito, garantizar una seguridad sólida y ofrecer un retorno de la inversión, se romiendan las mejores prácticas para la implementación de YubiKey en un modo de autenticación descentralizado basado en hardware.

Dado que las operaciones del call center varían según la organización, un factor clave en la implementación y gestión de las llaves de seguridad basadas en hardware es determinar los requisitos y el entorno operativo del call center. La administración de YubiKeys debe alinearse con otros controles operativos, incluidos los procesos para informar y revocar el acceso por llaves perdidas.

Controles de Seguridad estrictos

Los controles estrictos de YubiKeys se pueden abordar distribuyendo las llaves al comienzo de un turno y devolviéndolas al gerente o al guardia de seguridad al final del turno. En este escenario, las llaves nunca salen del edificio y están aseguradas mientras no se usan legítimamente. Este procedimiento puede adoptarse por razones de la economía también. Para garantizar la devolución de las llaves, algunas empresas tienen procesos de check-in y check-out donde los empleados intercambian pertenencias personales, como su teléfono móvil con YubiKeys. Cuando los empleados del call center devuelven las YubiKeys, se devuelven su teléfono u otras pertenencias personales. Para una identificación más fácil, las YubiKeys se pueden unir a un cordón junto con el “badge” de la empresa.

Controles de seguridad medios

Si no se requieren controles estrictos, un empleado tendría el control de la llave, pero solo se le entregaría una YubiKey. Si el empleado pierde la llave, necesitará la aprobación del gerente para recibir otra YubiKey del equipo de seguridad. Alternativamente, se puede enviar una notificación simple al administrador cuando se entrega una YubiKey. El equipo de seguridad también desactivaría la YubiKey perdida. Esto reduce la fricción para el empleado y permite que el gerente solo actúe cuando sea necesario. Todos los empleados deberán devolver sus YubiKeys al dejar la organización.

Controles de seguridad bajos

Con un nivel bajo de control, los empleados tienen el control de sus YubiKeys en todo momento y no necesitan devolverlas al final de sus turnos. Si un empleado pierde u olvida su YubiKey, se podría utilizar un proceso de autoservicio para garantizar que el empleado pueda regresar rápidamente al trabajo.

Algunas empresas han instalado máquinas expendedoras que dispensan YubiKeys para que un empleado pueda adquirir rápidamente una nueva llave. Se podría solicitar al empleado que pague el reemplazo de YubiKey.

Para los call centers virtuales, se recomienda que el empleado tenga una YubiKey de respaldo que se pueda usar si se pierde la llave principal. En este caso de uso, se supone que los empleados no están obligados a devolver YubiKeys ya que las eficiencias en el lugar de trabajo son más importantes.

Seguir un enfoque recomendado en la implementación y administración de YubiKeys garantiza una adopción rápida y efectiva por parte del usuario y la máxima seguridad para los activos críticos. Con requisitos de seguridad específicos y una alta rotación en los centros de llamadas, es importante tener en cuenta que las YubiKeys no representan un riesgo para la seguridad si se pierden, se las roban o no se devuelven cuando los empleados dejan una organización. Las YubiKeys se pueden conservar o restablecer para su reutilización, según las necesidades y requisitos. SE puede encontrar información de como reutilizar una Yubikey en: YubiKey LifeCycle Management - Key Retirement.

+ 52 (81) 2474 5555
info@infinyt.mx
INFINYT.MX