Sponsored content

CIO FROM IDG

DISEÑO DE SEGURIDAD INTEGRAL:

Mejora la Seguridad del Trabajo Híbrido

Google Workspace

Introducción

Desde principios de 2020, las empresas se han esforzado por predecir si sería posible que la vida de oficina volviera a la "normalidad" y cuándo sucedería.

La cruda verdad es que resulta cada vez evidente que una vuelta atrás así de tajante es poco probable, y que la mayoría de las empresas se están ajustando a la realidad de que el trabajo híbrido llegó para quedarse de alguna forma. Esta situación plantea desafíos transformadores acerca de cómo las empresas pueden ampliar de manera segura el entorno laboral y, al mismo tiempo, garantizar la flexibilidad necesaria para adaptarse rápidamente a cambios impredecibles.

Incluso a mediados de 2020, cuando muchos creían que el final de la pandemia del COVID-19 era inminente, una **encuesta de Gartner a líderes empresariales** reveló que el 80% planeaba permitirles a los empleados trabajar de manera remota al menos una parte del tiempo luego de la pandemia, y el 47% permitiría que los empleados trabajen desde sus hogares a tiempo completo.

Contenidos

“La pregunta que ahora enfrentan muchas organizaciones no es acerca de cómo gestionar una fuerza laboral remota, sino cómo administrar una fuerza laboral híbrida más compleja”, expresó Elisabeth Joyce, vicepresidenta de asesoría del departamento de RR. HH. de Gartner, cuando se anunció esa encuesta. “Si bien el trabajo remoto no es algo nuevo, su avance cambiará la manera en que las personas trabajan juntas para hacer su trabajo”.

Hacia finales de 2020, de acuerdo con la segunda encuesta de PwC acerca de las actitudes hacia el trabajo remoto, ejecutivos y empleados de EE. UU. “coincidían sobre un futuro posterior a la pandemia con mucha más flexibilidad”. Sin embargo, según la encuesta, **"muy pocos estaban preparados para abandonar por completo la oficina"**. Como resultado, según PwC, la mayoría de las empresas se dirigían a un espacio de trabajo híbrido que adopta la flexibilidad, con un gran número de trabajadores de oficina que rotan en espacios laborales compartidos.

Aún así, la flexibilidad del entorno de trabajo híbrido presenta un nuevo desafío a la hora de proteger los sistemas digitales empresariales, ya que los trabajadores dividen su horario laboral entre la oficina y el hogar, algunos trabajan a tiempo completo de manera remota, y otros colegas prefieren ir a la oficina la mayor parte del tiempo.

Las empresas ya se esforzaban por lidiar con la seguridad cibernética. Sin embargo, a pesar del aumento del trabajo remoto en 2020, menos del 40% de los **líderes en redes encuestados por CSO e IDG** afirman que han implementado políticas de seguridad de TI para utilizar dispositivos finales, videoconferencias o herramientas de colaboración. **En otra encuesta, IDG reveló** que el 90% de los líderes de seguridad “creen que su empresa no hace lo suficiente por abordar los riesgos cibernéticos”.

A pesar de esos problemas y preocupaciones, son pocas las organizaciones que probablemente “regresen a la normalidad”. Incluso los titanes de Wall Street que insistían en que todos los empleados debían regresar a la oficina lo antes posible han dudado ante la **resistencia de los trabajadores actuales y futuros.** Algunas organizaciones parecen estar **aprovechando el trabajo remoto para consolidar el espacio de oficina.** Muchas descubrieron que no había una disminución en la productividad; de hecho, **experimentaron aumentos de productividad**, lo que trajo aparejado acuerdos de trabajo más flexibles.

Parece casi seguro que nos espera un largo período de experimentación a medida que los empleadores evalúan los beneficios y las desventajas del trabajo remoto y las fuerzas laborales híbridas. Eso ejercerá una presión adicional en la seguridad de TI, según un 73% de **los líderes de seguridad encuestados por IDG en su sondeo CSO Pandemic Impact 2021**, quienes creen que el impacto de esta pandemia alterará la manera en que las empresas evalúan el riesgo durante al menos los próximos cinco años.

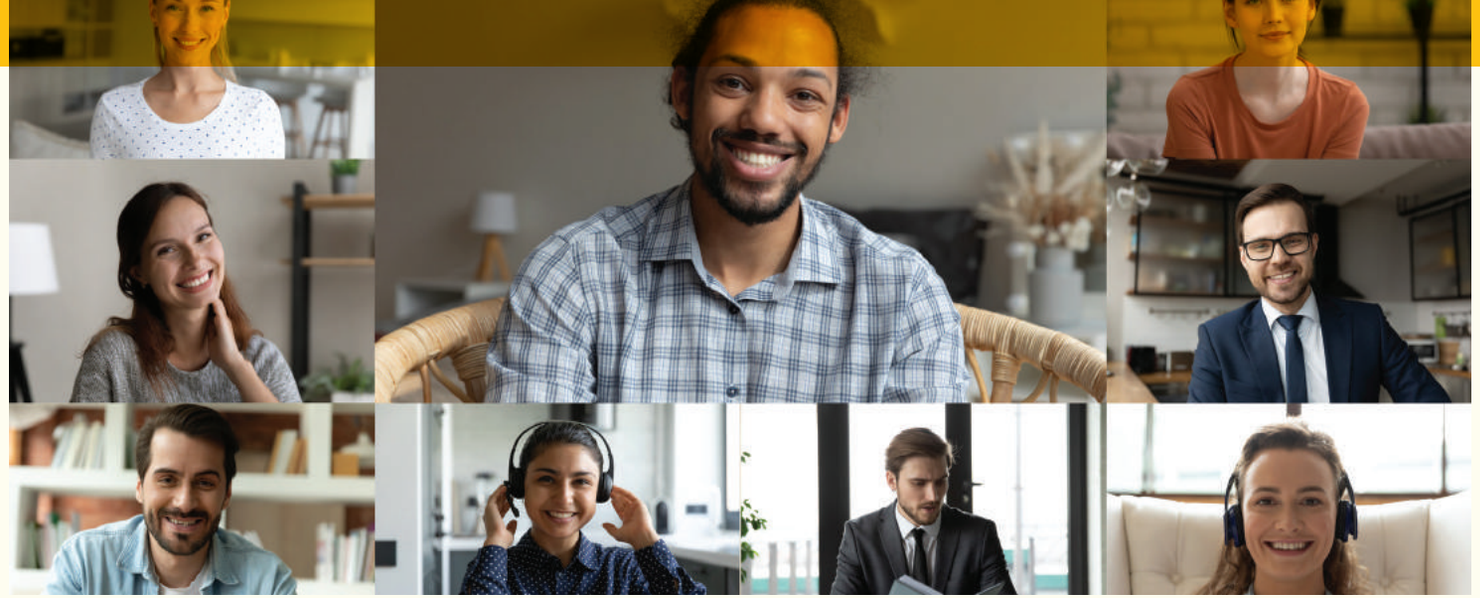
Mientras tanto, las empresas lidian con las consecuencias de las brechas de seguridad que han surgido a principios de 2020. **Según un informe de CBS** News, durante la pandemia, casi el 85% de las violaciones de datos exitosas estuvieron destinadas a engañar a los humanos, no a vulnerar la seguridad del código informático. Las amenazas como el ransomware han proliferado y crecieron un 151% durante los primeros seis meses de 2021 en comparación con el año anterior, **según ThreatPost.**

Independientemente de cómo evolucione el trabajo híbrido, los equipos de seguridad deben estar preparados para lo que venga.

de los líderes empresariales piensa permitirles a los empleados trabajar de manera remota al menos a tiempo parcial luego de la pandemia y

de los líderes empresariales permitiría a los empleados trabajar desde sus hogares a tiempo completo.

Fuente: Gartner



Identificar Puntos débiles, Oportunidades y Objetivos

Las herramientas heredadas simplemente no fueron creadas para el futuro cambiante del trabajo, en especial el híbrido, ya que exponen a las empresas a mayores riesgos de seguridad.

Al entrar al segundo año de la crisis del COVID, **Computerworld** observó que "las organizaciones descubrieron que necesitan ampliar las capacidades de sus infraestructuras de seguridad existentes de maneras que tal vez no hubieran considerado antes del cambio al trabajo remoto. Eso incluye garantizar que las herramientas y prácticas de seguridad corporativa que fortalecen y defienden el perímetro de una empresa puedan cubrir una gama más amplia de ubicaciones geográficas para abarcar las oficinas hogareñas".

Con frecuencia, las empresas se han adaptado a nuevos problemas de seguridad con múltiples soluciones, y han agregado recursos modernos al crear interfaces e integraciones a sistemas más antiguos. Esto hace que todo sea más complejo y difícil al momento de responder rápidamente a una nueva amenaza. Con un enfoque basado en la nube, las plataformas de proveedores de servicios se actualizan constantemente, lo que reduce en gran medida la necesidad de aplicar parches en el software.

"Uno de los problemas más comunes que enfrentan los equipos de seguridad es alcanzar el máximo rendimiento de sus máquinas con los parches de software más recientes", señaló un **informe de Wall Street Journal** que calificó al lugar de trabajo híbrido como una pesadilla para la seguridad cibernética. "Estas actualizaciones se lanzan constantemente para garantizar que las vulnerabilidades de seguridad no queden expuestas para que los hackers las aprovechen. Si las empresas libran al azar simplemente una de ellas, podrían pagar un alto precio en términos de su propia vulnerabilidad corporativa".

Además de mantener actualizados las aplicaciones y los servidores principales, los equipos de TI deben considerar una combinación cada vez más diversa de dispositivos que ahora se conectan desde fuera de los firewalls tradicionales. Es posible que las laptops empresariales hayan estado fuera de la oficina por un año o más, lo que dificulta a los equipos de TI determinar y solucionar problemas de seguridad. Además, muchos empleados quizás utilicen sus sistemas personales en el hogar y los compartan con otros miembros de su familia, los que, a su vez, quizás frecuenten sitios web cargados de malware. O también: algunos incluso permiten a los miembros de la familia utilizar una laptop proporcionada por un empleador.

> **"Las organizaciones descubrieron que necesitan ampliar las capacidades de sus infraestructuras de seguridad existentes de maneras que tal vez no hubieran considerado antes del cambio al trabajo remoto".**
>
> — *Computerworld*

Muchas organizaciones simplemente no estaban preparadas para un cambio tan drástico en el lugar de trabajo, ni contaban con los controles de seguridad para abordar este modelo de trabajo en evolución. El crecimiento exponencial de los puntos de acceso a los datos y la creciente dependencia de los dispositivos de propiedad o administración personal está abrumando la capacidad de los administradores de redes y seguridad de supervisar lo que sucede en un momento dado.

Enfoque en las Personas

Los proveedores de seguridad y TI suelen decir que los humanos son el eslabón más débil en la cadena de defensa de seguridad. **Los datos de la encuesta de IDG** revelan que el "36% de los incidentes de seguridad en 2020 involucraron a empleados que fueron víctimas del phishing u otras violaciones no maliciosas de la política de seguridad. Este año, esa cifra aumentó a un 44% de todos los incidentes de seguridad, incluso después de que casi la mitad de esos líderes de seguridad priorizaran la capacitación y concientización sobre la seguridad de sus empleados el año pasado".

Desde luego, es cierto que los hackers han encontrado en los trabajadores un objetivo relativamente fácil para distribuir el malware. **Una encuesta de IDC lo confirma,** al revelar que los dispositivos no administrados, los hackers y las redes inseguras representan el mayor riesgo para los modelos de trabajo remoto e híbrido. Sin embargo, la mayoría de los empleados no son expertos en seguridad o TI, por lo que están centrados en sus labores y no en constante vigilia ante los ataques cibernéticos.

A diario, los usuarios finales quizás se enfoquen en chequear calificaciones o cientos de correos electrónicos, mientras que los hackers intentan constantemente nuevas atracciones para que esos mismos usuarios hagan clic en archivos adjuntos o enlaces con logos y advertencias de aspecto oficial que provienen supuestamente de entidades como bancos, organismos de seguridad, o proveedores de comercio electrónico. **Y, como señala la agencia Cybersecurity and Infrastructure Security Agency**, algunos malware pueden incluso enviarse simplemente al abrir un mensaje, si el cliente de correo electrónico lo permite.

Los ataques de malware pueden poner en riesgo una cuenta, propiciar el robo de datos y, posiblemente, proporcionar acceso adicional a una red. En 2020, según el **Internet Crime Complaint Center del FBI**, los esquemas que pueden comprometer al correo electrónico empresarial dieron como resultado casi 20,000 reclamos, lo que representa $1,800 millones en pérdidas.

Según **informes del sector**, el 94% del malware se envía por correo electrónico, y casi el 50% de los adjuntos maliciosos en correos electrónicos se presentan en forma de documentos infectados. Si bien los servicios de correo electrónico emplean tecnología sofisticada de análisis para detectar URL infectadas para fines de malware phishing, los atacantes cibernéticos suelen modificar sus tácticas en un esfuerzo por eludir dicha seguridad.

Las aplicaciones antivirus comerciales y tradicionales deben actualizarse con frecuencia para que sean eficaces contra las amenazas emergentes. En la actualidad, con el crecimiento de la fuerza laboral remota, muchos equipos de TI simplemente no cuentan con la capacidad de realizar un seguimiento de los puntos de conexión remotos que están actualizados. Según un **informe**, los productos de supervisión pasan por alto entre el 10% y el 20% de los puntos de conexión.

No hay duda de que las redes domésticas y las de WiFi público representan una mayor amenaza a las empresas que la red de oficina protegida. El personal de seguridad tiene que luchar por supervisar la avalancha de alertas generadas por esta proliferación de puntos de conexión que utilizan las redes domésticas. Un **estudio de IDC** reveló que el 45% de las alertas son falsos positivos y que el 35% de los empleados de seguridad encuestados ignoran las alertas "¡cuando hay demasiadas!".

de los ataques de malware se dan por medio de correos electrónicos y casi

de los adjuntos maliciosos en correos se presentan como documentos infectados.

En el entorno empresarial actual, se espera que los trabajadores colaboren entre sí independientemente de si están dentro o fuera de la oficina. También deben responder a los clientes actuales y potenciales, y a los crecientes ecosistemas de socios y proveedores. Los modelos heredados de autenticación e identidad simplemente no pueden seguir el ritmo de las demandas del trabajo híbrido, ya que crean fricciones para el acceso de los usuarios, ralentizan o impiden la colaboración, y brindan posibles puntos de entrada para los atacantes.

Las herramientas, los sistemas y los procesos que los empleados utilizan cada día, sin importar dónde trabajen o qué dispositivo usen, deben contar con un diseño de seguridad integral. Además, deben ser lo suficientemente flexibles para mantenerse actualizados conforme a todas las maneras en que el trabajo continuará evolucionando.

Los Tiempos Modernos Exigen Herramientas Modernas

No alcanza con simplemente adaptar las herramientas laborales heredadas a estilos más modernos. Estas herramientas, típicamente diseñadas para entornos locales, no están integradas a la creciente cantidad de servicios de nube de los que dependen los trabajadores. Además, no están bien equipadas para lidiar con la sofisticación y automatización que los atacantes cibernéticos aplican contra sus objetivos.

Con frecuencia, las empresas almacenan datos en forma local y dependen de herramientas de seguridad en la nube o viceversa, con latencia adicional que inhibe la respuesta instantánea ante las amenazas y agrega enlaces adicionales en la cadena de seguridad para que los atacantes los aprovechen.

Debido a que empresas de todos los sectores se esfuerzan por transformarse digitalmente, la seguridad debe ser esencial, ya que las organizaciones evolucionan las infraestructuras de servicios de nube y locales para mejorar los procesos empresariales, estimular la innovación y alcanzar nuevas oportunidades. La seguridad debe ser eficaz, pero también debe garantizar la productividad de la fuerza laboral. Mantener una productividad segura siempre ha sido un desafío, pero lo es aún más con la repentina transformación de la fuerza laboral.

Según la investigación de IDC, los principales desafíos de TI para el trabajo híbrido son: soporte de TI, acceso seguro a los datos, aplicaciones y contenidos, visibilidad del rendimiento y seguridad de los activos de TI.

Las encuestas de Gartner Inc. indican que luego de la pandemia, entre un 30% y un 40% de los empleados continuarán trabajando desde casa. “Para muchas organizaciones, este cambio requiere una reconfiguración total de las políticas y herramientas de seguridad... Por ejemplo, los servicios de protección de puntos de conexión deberán pasar a servicios prestados en la nube. Los líderes en seguridad también deberán reconsiderar las políticas de protección de datos, recuperación ante desastres y backup para asegurarse de que aún funcionen en un entorno remoto”.

Estos líderes también deben asegurarse de que sus estrategias reflejen objetivos claros y bien definidos sobre los equipos de TI, las líneas de negocio y sus propios equipos. “A medida que las empresas reimaginan sus procesos y rediseñan la arquitectura ante el COVID-19, los equipos de seguridad cibernética se perciben de otra manera”, destacaron **analistas de McKinsey.** “Ya no deben ser vistos como una barrera para el crecimiento, sino que deben ser reconocidos como socios estratégicos en la toma de decisiones tecnológicas y empresariales”.

En el pasado, los analistas de seguridad y los administradores de TI podían simplemente bloquear a los usuarios remotos que intentaban obtener acceso desde redes externas, como redes de WiFi públicas o remotas en países específicos. De hecho, se les indicaba a esos usuarios que iniciaran sesión con una VPN corporativa o que vayan a la oficina para acceder a la red interna. Eso ya no es viable en un mundo donde muchos usuarios trabajan de manera remota, con frecuencia, desde sus propios dispositivos personales. Por eso, las organizaciones deben esforzarse por crear modelos más flexibles que les permitan extender el acceso seguro desde varios puntos externos que no están bajo su control directo.

A medida que evolucionan las amenazas y el trabajo híbrido, el modelo de seguridad debe respaldar, y no bloquear, la ejecución de modelos empresariales, y equilibrar los controles con la necesidad de garantizar una productividad y colaboración sin fricciones. Ese es un desafío que las herramientas de seguridad heredadas no pueden enfrentar.

> **“A medida que las empresas reimaginan sus procesos y rediseñan la arquitectura ante el COVID-19, los equipos de seguridad cibernética se perciben de otra manera”.**
>
> ***— McKinsey***

Infraestructura del Trabajo Híbrido: Evaluar el Contexto actual y Planificar inversiones

La transición al trabajo remoto ha revolucionado las nociones tradicionales del lugar de trabajo.

"No todos los empleados trabajarán en las oficinas las instalaciones empresariales tradicionales, ni todos serán remotos", afirma **Computerworld**. "Muchos empleados trabajarán desde sus casas, pero muchas personas aún necesitarán trabajar en las instalaciones de las empresas, por ejemplo, en una fábrica, un centro de datos, una tienda minorista, un centro de distribución, un laboratorio o incluso una oficina tradicional. También hay empleados cuyo trabajo es independiente de la ubicación, pero que no pueden trabajar desde sus hogares debido a la falta de espacio o acceso insuficiente a Internet".

De hecho, esto ilustra la naturaleza de la fuerza y el lugar de trabajo híbridos en constante evolución. Algunos empleados trabajarán algunos días de manera remota y otros días en la oficina. Otros trabajarán a tiempo completo en un lugar o el otro. Esta fluidez genera nuevos niveles de tensión en la infraestructura de seguridad y de TI tradicional, que debe adaptarse rápidamente para garantizar que los trabajadores sean productivos y puedan colaborar sin importar dónde se encuentren ni de qué día de la semana se trate.

"En la medida de lo posible, los procesos laborales deben ser digitales y estar disponibles a través de Internet, ya que los empleados están distribuidos y lo seguirán estando", destacó Computerworld. "Esto significa que los trabajadores necesitan acceso a un ancho de banda y entorno laboral adecuados, que la experiencia del usuario para los empleados ahora es fundamental para la eficiencia empresarial, y que los empleados necesitan trabajar estrechamente con el equipo de TI, y no considerarse como simples consumidores de herramientas proporcionadas por TI".

> **"En la medida de lo posible, los procesos laborales deben ser digitales y estar disponibles a través de Internet, ya que los empleados están distribuidos y lo seguirán estando".**
>
> ***— Computerworld***

IDC insta a los CIO a “centrarse en aplicaciones que fomenten la colaboración segura independientemente de la ubicación, [y brinden] soporte de red para la interacción omnicanal”.[1]

Satisfacer estas necesidades no es una tarea sencilla para las organizaciones de TI que utilizan infraestructuras inmensas y complejas que abarcan centros de datos, servidores de sucursales, redes de área amplia y VPN. Estos entornos son simplemente demasiado inflexibles para adaptarse a los cambios rápidos que están ocurriendo con la fuerza y el lugar de trabajo.

No esperes cambios rápidos aquí. Gran parte de esa infraestructura existente es fundamental para los procesos empresariales centrales, y seguirá funcionando por necesidad, debido a cuestiones regulatorias y de cumplimiento, la resistencia a migrar hacia nuevas alternativas, y el equilibrio entre prioridades y costos. El desafío para los líderes de TI consiste en identificar qué infraestructura modernizar y migrar a la nube, y cuál continuar operando en las instalaciones. Muchas empresas ya han adoptado entornos híbridos locales y de nube para comenzar a abordar este desafío. Sin embargo, no siempre son fáciles de administrar o compatibles con las nuevas consideraciones de los usuarios finales.

Una **encuesta de Economist Impact**, realizada por encargo de Google Workspace, reveló las principales preocupaciones tecnológicas que surgen del cambio al trabajo híbrido, entre las que se incluyen:

- Acceso a Internet poco fiable
- Dependencia de herramientas lentas u obsoletas
- Mantenimiento y acceso a archivos desde múltiples lugares
- Dependencia de demasiadas aplicaciones para realizar el trabajo

1 Presentación de IDC, “Transforming security for a hybrid future of work”, Amy Loomis PhD., diciembre de 2021.

La colaboración híbrida finalmente será la norma, pero muchas organizaciones aún están evaluando sus experiencias durante los últimos dos años y planificando sus estrategias de cara al futuro. Claramente, la fuerza laboral híbrida necesita una infraestructura moderna y sencilla que le permita ser productiva y comprometerse con el trabajo. Los usuarios finales requieren herramientas de colaboración que sean más fáciles de usar y faciliten la interacción, sin importar si un empleado está en un salón de conferencias, una sala de estar u otro lugar.

La naturaleza de la oficina fija ya está cambiando. **Muchas empresas se están adaptando a las circunstancias cambiantes**, al adoptar o evaluar conceptos del “office hoteling”, por medio del cual los lugares de trabajo individuales ya no se asignan, sino que se programan y fijan para los trabajadores según sea necesario.

Los procesos empresariales y las aplicaciones deben adaptarse rápidamente a esta nueva realidad con actualizaciones en términos de identidad y autenticación. Los trabajadores deben tener acceso instantáneo a las mismas herramientas de productividad y colaboración, ya sea en la oficina o en cualquier otro lugar, y desde diferentes tipos de dispositivos. Las empresas también deben tener en cuenta cómo usar la tecnología para compensar la falta de interacción en los pasillos de oficina y garantizar que los empleados junior aprovechen las oportunidades virtuales de mentoría y aprendizaje de los empleados sénior.

Todo este cambio debe lograrse de una manera que no solo mantenga la seguridad, sino que también la haga más eficaz y eficiente.

La fuerza laboral híbrida necesita una infraestructura moderna y sencilla que le permita ser productiva y comprometerse con el trabajo.

Desarrollar una Infraestructura de Trabajo Centrada en la Nube

Las soluciones de productividad y colaboración nativas de la nube, como Google Workspace, adoptan un enfoque significativamente diferente para proteger la colaboración y el trabajo. El trabajo en equipo en cualquier momento y lugar debe ser un aspecto fundamental del trabajo híbrido, ya que es la única manera de garantizar que los empleados permanezcan conectados y sean productivos.

Las herramientas basadas en la nube tienen algunas ventajas únicas. Con Google Workspace, la seguridad se integra en cada nivel de diseño del producto. Dado que los datos y la seguridad residen en la nube, los servicios de seguridad no afectan negativamente el rendimiento debido a la latencia generada por las inspecciones de ida y vuelta y las alertas entre los recursos locales y en la nube.

El enfoque de Google Workspace centrado en la nube garantiza que la seguridad opere a escala global para detectar todas las amenazas potenciales y proteger a toda la organización frente a ataques de phishing, malware, ransomware y de cadena de suministro. No importa si los empleados utilizan sus propios dispositivos u otros brindados por la empresa, Google Workspace protege puntos de conexión seguros que se actualizan constantemente.

La solidez en infraestructuras y sistemas de seguridad es la opción predeterminada para cada cliente de Google Workspace. Los administradores tienen pleno control para configurar la infraestructura, las aplicaciones y las integraciones del sistema con un solo panel en la consola de administración, lo que elimina el proceso demandante y a menudo propenso a errores de aplicar parches y configurar servidores individuales.

Google Workspace brinda acceso por medio de una interfaz conocida a un complemento integral de herramientas de productividad, para que los empleados creen, se comuniquen y colaboren: Gmail, Calendario, Drive, Documentos, Hojas de cálculo, Presentaciones, Meet y más. Los empleados pueden trabajar con las mismas herramientas, ya sea que estén en la oficina o en sus casas, en las oficinas de clientes, o en viaje desde un dispositivo móvil. Una experiencia sencilla y unificada que les brinda a los empleados acceso a un solo lugar donde se encuentran todas las herramientas principales que necesitan para conectarse, crear y colaborar.

Los empleados pueden trabajar con las mismas herramientas, ya sea que estén en la oficina o en sus casas, en las oficinas de clientes, o en viaje desde un dispositivo móvil.

La administración de documentos nativos de la nube permite una colaboración en línea sin necesidad de que los usuarios descarguen un archivo adjunto en sus dispositivos. Esto permite dejar atrás los conflictos de versiones y hace posible que muchos más usuarios colaboren de manera eficaz en un único documento. Los empleados pueden compartir información de manera externa con un enlace de Google Drive, invitar a usuarios externos a colaborar y editar y, al mismo tiempo, garantizar que se cumplan las políticas de protección de datos y seguridad de la organización de origen.

Las herramientas de productividad y la infraestructura de Google Workspace fueron diseñadas con un enfoque de confianza cero que muchas organizaciones esperan poder emplear en el futuro. Las funcionalidades de verificación, encriptación y los controles integrados de Google Workspace les permiten a los empleados trabajar desde cualquier lugar, y eliminan la necesidad de usar VPN. Los datos pertenecientes a organizaciones que utilizan Google Workspace están encriptados en reposo y en tránsito: si se interceptan, no tendrán valor alguno para los intrusos.

Para obtener capas de protección adicionales, el programa Work Safer de Google brinda seguridad integral y defensa exhaustiva que se adapta y detecta amenazas en evolución en tiempo real. Work Safer reúne lo mejor de Google Workspace, con un ecosistema de soluciones de seguridad cibernética en un paquete todo en uno, para que las empresas puedan potenciar a sus empleados gracias a una colaboración sin esfuerzo y una experiencia de trabajo híbrida y moderna que establece un nuevo estándar de seguridad.

BeyondCorp Enterprise, como parte de Work Safer, es la solución de confianza cero de Google que se ha desarrollado por más de una década como una iniciativa interna que permite el trabajo seguro desde prácticamente cualquier ubicación sin la necesidad de contar con una VPN tradicional. Cuenta con inicio de sesión único, políticas de control de acceso, proxy de acceso, y autorización y autenticación basadas en usuarios y dispositivos.

Ahora disponible en forma comercial, BeyondCorp Enterprise brinda acceso seguro con protección integrada de datos y contra amenazas. Las organizaciones pueden usar BeyondCorp Threat and Data Protection para integrar Chrome a una variedad de funciones de seguridad, mejorar protecciones de seguridad existentes de Chrome o utilizar funciones nuevas con Chrome. Las organizaciones pueden aplicar protecciones adicionales contra amenazas basadas en la web, como el malware o la ingeniería social, y usar reglas de prevención de la pérdida de datos (DLP), alertas de seguridad y herramientas de creación de informes para respaldar la protección de seguridad cibernética.

Los principios detrás de la solución de confianza cero de Google brindan un modelo que muestra cómo las empresas pueden respaldar de manera segura a la fuerza de trabajo híbrida:

- El acceso a los servicios no debe estar determinado por la red desde la que te conectas
- El acceso a los servicios se otorga en función de los factores contextuales del usuario y su dispositivo
- El acceso a los servicios debe estar autenticado, autorizado y encriptado

Google Workspace brinda a los administradores control empresarial sobre la configuración de sistemas y aplicaciones. Los controles granulares para las aplicaciones de Google Workspace, basados en la identidad del usuario y el contexto de la solicitud (como el estado de seguridad del dispositivo o la dirección IP) permiten acceder a aplicaciones web y recursos de infraestructura desde prácticamente cualquier dispositivo, en cualquier lugar. Sin embargo, las organizaciones también pueden establecer políticas de acceso, como la verificación en dos pasos, para todos los miembros de una unidad o grupo de la organización.

Los empleados pueden compartir información de manera externa con un enlace de Google Drive, invitar a usuarios externos a colaborar y editar y, al mismo tiempo, garantizar que se cumplan las políticas de protección de datos y seguridad de la organización de origen.

Los modelos de aprendizaje automático de Google ayudan a bloquear más del 99.9% de las amenazas para que no lleguen a las bandejas de entrada de Gmail. Google escanea automáticamente todos los correos electrónicos y archivos adjuntos con varios motores en busca de virus o enlaces maliciosos antes de que los usuarios los descarguen. Gmail también busca virus en los archivos adjuntos que están por enviarse, lo que ayuda a prevenir la propagación del malware.

Las soluciones empresariales de Google Workspace ofrecen recursos de colaboración flexibles que se adaptan a todas las maneras en que está cambiando el trabajo. Al garantizar una colaboración fluida entre quienes están en la oficina y los que trabajan de manera remota (en reuniones y en todas las formas de colaboración), Google Workspace puede ayudar a los equipos híbridos a conectarse, crear y colaborar, desde cualquier lugar y en cualquier dispositivo.

Cómo Google Workspace Protege la Colaboración y el Trabajo

El software de productividad y colaboración nativo de la nube adopta un enfoque significativamente diferente para proteger la colaboración y el trabajo.

- **Enfoque en la nube:** un enfoque basado en navegador que es arquitectónicamente superior y se actualiza de manera constante, sin necesidad de dispositivos locales, aplicaciones nativas ni archivos adjuntos de correo electrónico
- **Confianza cero:** un enfoque de confianza cero con verificación, encriptación y controles integrados para que tus empleados trabajen desde cualquier lugar y sin necesidad de contar con una VPN
- **Detección total:** escala global para proteger tu información frente a los ataques de phishing, malware, ransomware y de cadena de suministro sin necesidad de contar con complementos
- **Protección integral:** todas las personas se sienten más seguras con puntos de conexión seguros (brindados por la empresa o BYOD) que no requieren de parches y están protegidos de manera sólida contra la apropiación de cuentas.

Las herramientas, los sistemas y los procesos que los empleados utilizan cada día, sin importar dónde trabajen o qué dispositivo usen, deben contar con un diseño de seguridad integral. Además, deben ser lo suficientemente flexibles para mantenerse actualizados conforme a todas las maneras en que el trabajo continuará evolucionando. Google Workspace impulsa un futuro del trabajo construido sobre la base de la flexibilidad, seguridad y la conexión humana. Haz clic **aquí** para obtener más información acerca de cómo Google puede brindar protecciones constantemente actualizadas contra el phishing, malware, ransomware y otros ataques cibernéticos.

Al garantizar una colaboración fluida entre quienes están en la oficina y los que trabajan de manera remota (en reuniones y en todas las formas de colaboración), Google Workspace puede ayudar a los equipos híbridos a conectarse, crear y colaborar, desde cualquier lugar y en cualquier dispositivo.