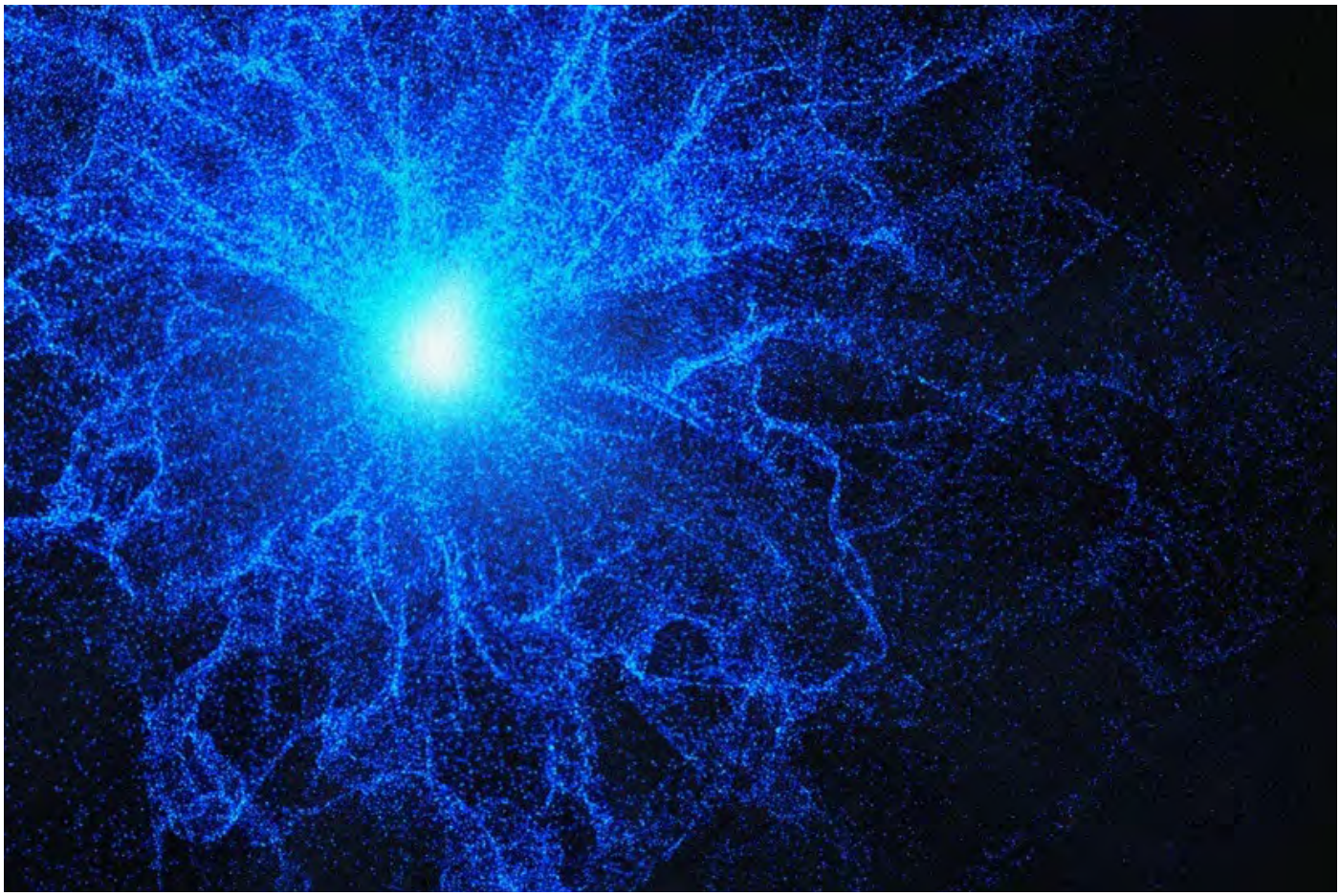
BlackBerry
Intelligent Security. Everywhere.

Documento técnico



El inevitable ascenso de Zero Trust

Asegúrese de que las actividades de los usuarios sean confiables sin interrumpir el flujo de trabajo

Cómo comprender el problema de la confianza

Existe una historia sobre la creación del juego ajedrez que ilustra por qué las soluciones de seguridad cibernética no pueden depender de los modelos de confianza tradicionales. La historia cuenta que el inventor del ajedrez presentó el juego a un rey. El rey estaba muy impresionado y le ofreció al creador lo que este quisiera como recompensa. El creador pidió un grano de arroz por la primera casilla del tablero. Además, cada casilla posterior recibiría el doble de arroz que la casilla anterior, hasta llegar al final del tablero.

Al principio, el rey pensó que el pedido sonaba manejable. Sin embargo, a medida que pasó el tiempo, se hizo evidente que sería imposible cumplir con él. Duplicar la cantidad de arroz era un pedido exponencialmente costoso que, en última instancia, requeriría de trillones (264 – 1) de granos. El rey no pudo cumplir con el pedido y se dice que mandó a ejecutar al inventor por su insolencia.

El problema del tablero de ajedrez y el arroz es similar al dilema de la seguridad de puntos finales que enfrentan muchas organizaciones hoy en día. En los primeros tiempos de la informática, proteger la estación de trabajo de un empleado era una tarea manejable. Cuando varias estaciones de trabajo formaron una red, o varias redes conectadas (y, finalmente, la Internet), proteger el entorno se hizo considerablemente más difícil. Ahora, con el crecimiento de dispositivos de la Internet de la cosas (IoT) interconectados, proteger toda la tecnología que afecta a los recursos del lugar de trabajo es casi imposible.

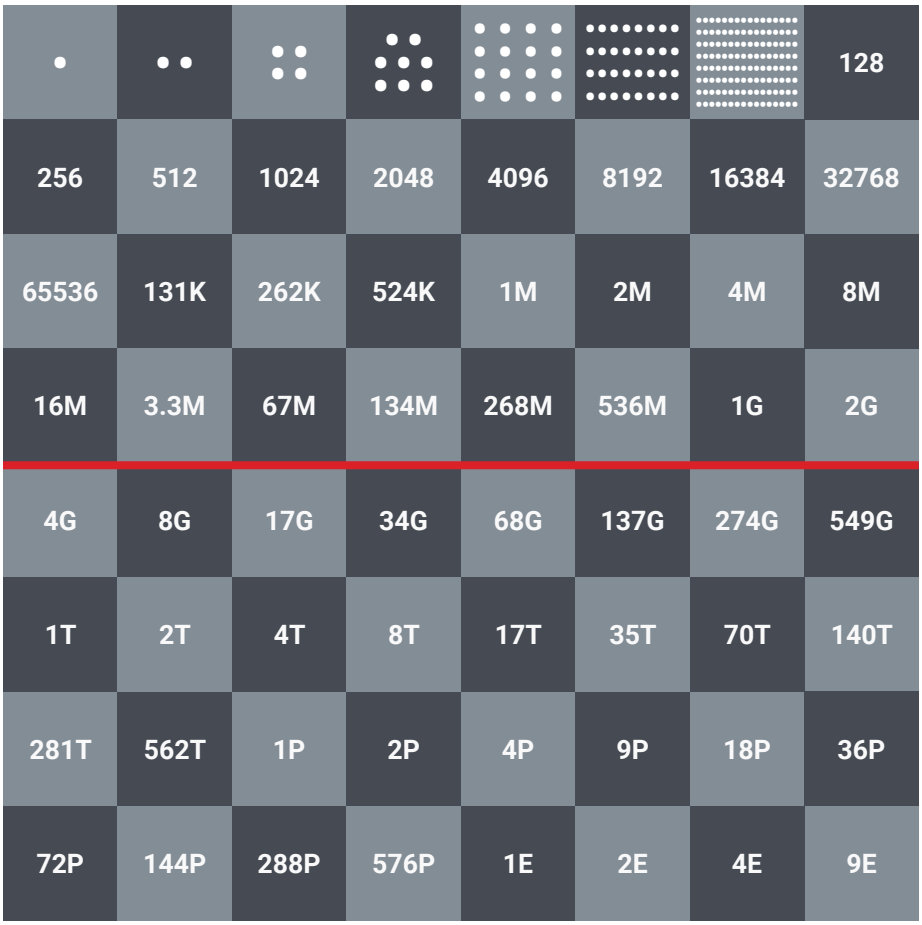


Figura 1. Un grano de arroz duplicado por cada casilla crece rápidamente a proporciones inimaginables.

"El problema del tablero de ajedrez y el arroz es similar al dilema de la seguridad de puntos finales que enfrentan muchas organizaciones hoy en día".

Los vectores de ataque aumentan a medida que se agregan dispositivos

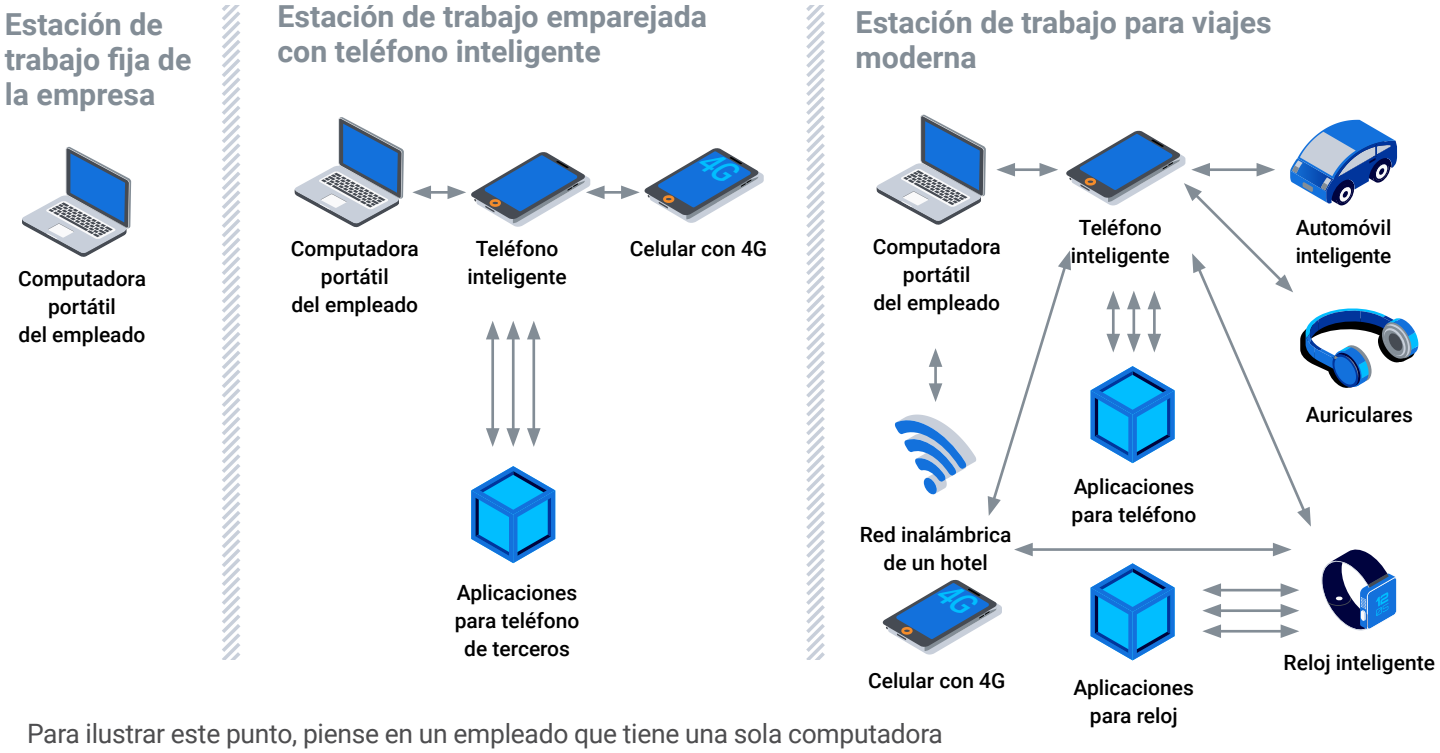


Figura 2. Los vectores de ataque (representados por las flechas de color gris) aumentan con cada dispositivo, aplicación y conexión de red adicional.

Para ilustrar este punto, piense en un empleado que tiene una sola computadora portátil asignada por la empresa. Proteger esa computadora es relativamente simple. Sin embargo, ese empleado también tiene acceso a activos de la empresa mediante su teléfono inteligente. ¿Qué tan seguras son las distintas aplicaciones de un teléfono inteligente? Nadie puede saberlo. Además, el empleado en ocasiones escucha música en su teléfono con auriculares Bluetooth® de avanzada (un dispositivo de la IoT) creados por un fabricante desconocido.

Estos dispositivos se emparejan con un automóvil, que almacena música, listas de contactos y otra información en su propio sistema interno. Cuando el empleado viaja, conecta su computadora portátil y su teléfono inteligente a distintas redes públicas para poder revisar el correo electrónico y trabajar en proyectos.

¿Qué tan protegidos están los recursos de la empresa entonces? La superficie de ataque que cubre a los recursos de la organización aumenta con cada aplicación, dispositivo y conexión de red adicional. El dilema demuestra claramente que las organizaciones deben adoptar un enfoque de seguridad de confianza cero (Zero Trust).

Confiar en entidades de forma predeterminada, o basándose en una confirmación de una única vez, ya no es una estrategia de seguridad viable. El mejor enfoque para limitar el riesgo es no confiar en nada de forma predeterminada sino desarrollar y mantener la confianza con los actores durante interacciones continuadas.

Seguridad cibernética: ¿un problema complicado o complejo?

La creación o implementación de soluciones de seguridad cibernética eficaces se basa en comprender la naturaleza del problema de confianza creado por los dispositivos de la Internet de las cosas (IoT) y la interconectividad masiva. Hoy, contar con entornos de trabajo seguros no es un problema complicado, sino un problema[1] complejo.

Para aclarar, los problemas complicados consisten de varios componentes que interactúan entre sí de formas predecibles. Las personas pueden predecir el resultado de un sistema complicado si conocen las variables. Por ejemplo, construir un submarino es una tarea complicada. Existen muchos sistemas interconectados dentro de un submarino que deben funcionar de una manera en particular para que este pueda sumergirse. Dado que cada uno de estos sistemas interconectados se comporta, en última instancia, de una manera predecible, si cuentan con suficiente tiempo y recursos, los ingenieros pueden crear un submarino sumamente complicado.

Por otro lado, los problemas complejos cuentan con varios sistemas interconectados pero la interacción entre estos es impredecible. Incluso cuando se conocen las variables, los resultados pueden, en el mejor de los casos, solo suponerse. Sistemas como los mercados financieros y el clima global son complejos. Con los sistemas complejos, podemos comprender piezas del rompecabezas más grande pero seguimos sin poder predecir de forma confiable resultados concluyentes.

Es posible que la seguridad cibernética moderna haya sido un problema complicado en el pasado, cuando las estaciones de trabajo estaban confinadas a los entornos comerciales. En la actualidad el aumento de los dispositivos de la IoT, la velocidad de la innovación tecnológica y el inmenso volumen de nuevo código de software, hacen que la seguridad cibernética eficaz se convierta en un problema complejo (es decir, que transciende la capacidad de predicción humana).

No obstante, la tecnología puede realizar cálculos y operaciones con una velocidad y eficacia que los humanos no pueden lograr. Contar con la ayuda de modelos predictivos, inteligencia artificial (IA), machine learning (ML) y autenticación continua ofrece a los analistas formas eficaces de lidiar con problemas de seguridad complejos.

"Con los sistemas complejos, podemos comprender piezas del rompecabezas más grande pero seguimos sin poder predecir de forma confiable resultados concluyentes".

¿Qué es Zero Trust?

Tal como su nombre lo indica, la confianza cero (Zero Trust) es un modelo de seguridad creado en torno a la idea de que no se puede confiar en nada dentro o fuera de una organización. Los cimientos de la arquitectura de confianza cero surgen del foro informático Jericho Forum a comienzos de la década de 2000, donde especialistas en seguridad analizaron la computación en la nube y la eliminación del perímetro[2]. John Kindervag, un analista principal de Forrester Research Inc., acuñó la frase "zero trust" en 2010[3].

El rol de la IA en la confianza cero

Una de las ventajas distintivas de la IA es su rapidez para procesar y encontrar correlaciones entre conjuntos de datos masivos. Es precisamente esa capacidad la que permite que la IA prediga con precisión la identidad de los usuarios, la seguridad de los archivos y la legitimidad de las actividades. Algunas de las maneras en que se puede utilizar IA para implementar confianza cero son:

- **Análisis de comportamiento de usuarios y entidades:** La IA puede monitorear la actividad de los usuarios, la ubicación y los datos biométricos y compararlos con patrones normales para determinar si un actor es confiable. El acceso a cuentas puede modificarse automáticamente para reflejar cambios en la confianza, y se pueden iniciar pasos para solicitar una nueva autenticación cuando las puntuaciones de confianza descienden demasiado.
- **Prevención de malware:** Se puede enseñar a la IA a identificar malware de día cero o desconocido al entrenarla con millones o miles de millones de archivos benignos o maliciosos. Una IA altamente entrenada puede detectar con éxito malware conocido y previamente desconocido mediante el análisis de las características de un archivo antes de la ejecución. Esta capacidad le brinda a los agentes de seguridad impulsada por IA una ventaja respecto de las amenazas y puede fácilmente reemplazar los modelos tradicionales de seguridad de archivos basados en la confianza.
- **Caza de amenazas:** Los modelos matemáticos pueden implementarse directamente en los puntos finales para monitorear su actividad e informar comportamientos anómalos. Las capacidades de detección de amenazas en los dispositivos permiten a los puntos finales informar rápidamente actividad sospechosa, iniciar una corrección automatizada y aislar el dispositivo de otros recursos durante un ataque.

El modelo de confianza cero se beneficia significativamente de la capacidad de la IA de hacer predicciones basadas en combinar y analizar datos. La confianza cero permite que las organizaciones dejen de lado las estrategias de autenticación de uno y dos factores que los atacantes han estudiado y aprendido a vulnerar desde hace ya mucho tiempo. Al ser examinada por la IA, la confianza se convierte en un proceso continuo de interacciones seguras y esperadas, en lugar de ser una presentación de credenciales por una única vez.

El rol de las personas en la confianza cero

Los especialistas en seguridad disponen de diversas herramientas para implementar una infraestructura de confianza cero. Al contar con que la IA maneje la detección y respuesta, los analistas pueden enfocarse en otras tareas como garantizar que el acceso a los recursos de la organización sea seguro. A medida que la fuerza laboral moderna se vuelve cada vez más móvil, las empresas deben encontrar maneras nuevas y seguras de brindar servicios de trabajo remoto. Poder proteger y monitorear una amplia variedad de tecnologías es uno de los componentes críticos de las soluciones de seguridad cibernética modernas.

"El modelo de confianza cero se beneficia significativamente de la capacidad de la IA de hacer predicciones basadas en combinar y analizar datos".

Las empresas deben considerar los siguientes factores al seleccionar herramientas para su personal de seguridad interno:

- ¿Pueden los empleados acceder de manera confiable y segura a los recursos de trabajo de forma remota?
- ¿Es posible acceder a los recursos de trabajo de manera segura desde cualquier dispositivo?
- ¿Existe una solución que admita distintas plataformas y modelos de propiedad, tales como Windows®, iOS®, Android™, macOS® y Linux®?
- ¿Es la solución escalable y con capacidad de mapearse fácilmente a una nuevas tecnologías?
- ¿Están disponibles los recursos de trabajo con y sin conexión, y es posible acceder a ellos sin usar una VPN?
- ¿Existe una solución que ofrezca una única interfaz donde realizar tareas de seguridad o los analistas se verán forzados a dividir su atención entre varias interfaces?
- ¿Pueden los analistas de seguridad garantizar que los empleados utilicen aplicaciones confiables en un dispositivo móvil seguro?

Cultivar un entorno de confianza cero viable requiere que las organizaciones además vayan al ritmo de las innovaciones tecnológicas y las prácticas comerciales cambiantes. Cada vez más trabajo se realiza fuera de las oficinas físicas y en dispositivos personales. Dicho de forma sencilla, la confianza cero no puede limitarse a los perímetros de las redes tradicionales. Debe abarcar el acceso a los datos de la empresa desde cualquier dispositivo, en cualquier lugar.

Lograr una experiencia sin intervención en un entorno de confianza cero

Una de las principales inquietudes que tienen las organizaciones que evalúan un modelo de confianza cero es cómo esta infraestructura afectará a sus usuarios. Los empleados buscarán soluciones alternativas para evitar procesos de verificación intrusivos o que producen interrupciones, lo que podría introducir nuevas vulnerabilidades en sus intentos por crear atajos. Esto significa que crear una experiencia mínimamente intrusiva, o sin intervención, para los usuarios es un componente clave de una robusta infraestructura de confianza cero.

Utilizar soluciones basadas en la IA para realizar una autenticación continua es una forma viable de disfrutar de lo mejor de ambos mundos. El análisis en tiempo real de datos contextuales de usuarios, dispositivos y ubicaciones puede asegurar que las actividades sean confiables sin interrumpir el flujo de trabajo. A los usuarios solo se les pide volver a verificar su identidad cuando realizan transacciones particularmente riesgosas o se comporten de manera anómala. La amplia mayoría de las tareas diarias son operaciones de bajo riesgo y nunca activarán una solicitud de nueva autenticación.

"El análisis en tiempo real de datos contextuales de usuarios, dispositivos y ubicaciones puede asegurar que las actividades sean confiables sin interrumpir su flujo de trabajo".

¿Por qué confianza cero?

¿Cómo puede beneficiarse una organización al adoptar un modelo de seguridad de confianza cero? Para entender los muchos beneficios de la confianza cero, tenga en cuenta lo siguiente:

- ¿De qué manera se beneficiaría su entorno al tener que tratar solo con usuarios identificados positivamente y autenticados de manera continua?
  - ¿Qué programas, políticas o prácticas dejarían de ser necesarios?
  - ¿Qué nuevas oportunidades podrían buscarse una vez que su organización pueda confiar plenamente en la identidad de los usuarios?
- ¿Qué cambios habría en su organización si cada dispositivo se verificara como confiable durante cada interacción?
  - ¿De qué manera cambiaría su selección de tecnología?
  - ¿Cómo cambiaría la productividad de sus empleados?
- ¿De qué forma se beneficiaría la postura de seguridad de su organización si se pudieran modificar los derechos de acceso prácticamente en tiempo real para reflejar el nivel de confianza actual de los usuarios y dispositivos?
  - ¿Cambiaría el porcentaje de empleados de oficina en comparación con el de empleados remotos?
  - ¿Podría utilizarse al personal de seguridad de TI de formas nuevas y eficaces?

El modelo de confianza cero puede beneficiar a las organizaciones de muchas maneras sorprendentes que no se limitan a lo obvio. Por ejemplo, en 2020 más del 80 % de los incidentes de seguridad informados fueron ataques de phishing[4]. Una infraestructura de confianza cero limita el daño que puede provocar un usuario comprometido al restringir su acceso y requerir una nueva autenticación cuando ocurren comportamientos inesperados.

De la misma manera, la confianza cero dificulta que las amenazas se propaguen en el entorno sin ser detectadas ya que se benefician de los recursos y modifican el acceso de forma sumamente sospechosa. Las vulnerabilidades comunes como la falta de actualizaciones del sistema y parches de software resultan menos desastrosas bajo el escrutinio constante y la postura restrictiva del modelo de confianza cero.

Conclusión

El modelo de confianza cero es el enfoque racional al interactuar con sistemas y tecnologías modernas. Proteger el entorno comercial mediante técnicas tradicionales deja de ser factible cuando los dispositivos del lugar de trabajo interactúan con una IoT en expansión. Las organizaciones deben entender que no pueden examinar cada aplicación, dispositivo y red externos que utilicen sus empleados.

Sin embargo, interactuar con entidades conocidas, confiables y autenticadas de manera continua es una solución viable para los problemas de seguridad creados por el avance tecnológico. De la misma manera, la IA puede mejorar enormemente a los equipos de seguridad mediante la realización de análisis de fuerza bruta y su correspondiente corrección a velocidades y en volúmenes que superan la capacidad humana.

La suite BlackBerry Spark® reúne las herramientas de seguridad, administración y productividad que necesitará para alcanzar sus objetivos de confianza cero con un enfoque sin intervención para sus empleados y contratistas.

Para obtener más información, visite http://www.blackberry.com/sparksuite.

1 https://thearmyleader.co.uk/team-of-teams/

2 https://blog.banyansecurity.io/blog/the-evolution-of-zero-trust

3 https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

4 https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) brinda servicios y software de seguridad inteligente a empresas y gobiernos alrededor del mundo. La compañía protege a más de 500 millones de puntos finales, lo que incluye a 150 millones de automóviles que están en las calles hoy en día. Con sede en Waterloo, Ontario, la compañía emplea IA y aprendizaje automático para brindar soluciones innovadoras en las áreas de la seguridad cibernética, soluciones de seguridad y privacidad de datos, y es líder en los campos de gestión de seguridad de puntos finales, cifrado y sistemas incorporados. La visión de BlackBerry es clara: garantizar un futuro conectado en el que pueda confiar.

BlackBerry. Intelligent Security. Everywhere.

Para obtener más información, visite BlackBerry.com y siga @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

MKTG20-0334 | 200917