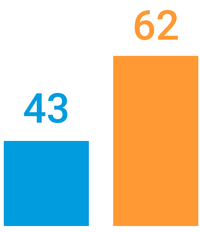
INFOGRAFÍA

Segmentación: la clave para la transición de los servicios financieros a Zero Trust

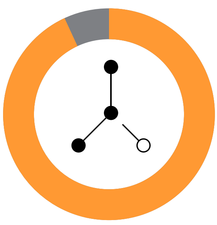
Superar los obstáculos de la implementación para proteger los sistemas bancarios esenciales

Al enfrentarse a un aumento significativo del número de ataques de ransomware, solo las instituciones financieras con una segmentación más avanzada han transformado sus defensas y han reducido la carga financiera y operativa.

El número de ataques de ransomware (que lograron o no su objetivo) ha experimentado un aumento del 50 % en los últimos dos años...



de una media de 43 en 2021 a 62 en 2023.



92 %

Porcentaje de los responsables de la toma de decisiones de seguridad de TI que coinciden en que la segmentación es fundamental frente a los ataques.

88 %

Porcentaje de instituciones financieras que afirma que la microsegmentación es, como mínimo, una prioridad alta para su organización, y el 39 % afirma que es su máxima prioridad.

Aunque las empresas confían en la tecnología, las implementaciones de segmentación han sido lentas. En 2023, solo el 39 % de las instituciones de servicios financieros ha segmentado más de dos áreas de negocio críticas (en comparación con el 26 % de 2021), mientras que el 45 % afirma haber iniciado un proyecto de segmentación de red hace dos años o más, lo que sugiere que las iniciativas se han estancado.

La adopción de un marco Zero Trust es una de las principales razones que han llevado a las instituciones financieras a iniciar un proyecto de segmentación; sin embargo, menos de la mitad (el 47 %) afirman haber definido y completado la implementación de dicho enfoque.

La perseverancia tiene su recompensa. Las empresas que han segmentado seis áreas de negocio críticas han conseguido transformar su defensa.

El alcance de la segmentación es importante

Después de una filtración, un ataque de ransomware se detiene por completo 5 veces más rápido si se han segmentado seis áreas.

¿Cómo pueden las instituciones financieras beneficiarse de la segmentación?

01
Simplificar y acelerar el cumplimiento de las normativas con una visibilidad detallada

02
Proteger los sistemas esenciales, como las transferencias de dinero, los pagos y las aplicaciones de los clientes

03
Evitar el movimiento lateral no autorizado aislando adecuadamente el acceso de terceros y gestionando las rutas de acceso

04
Adoptar la nube, la plataforma como servicio (PaaS) y otras tecnologías emergentes de manera rentable y segura

Descargue el informe completo para iniciar su transición a Zero Trust