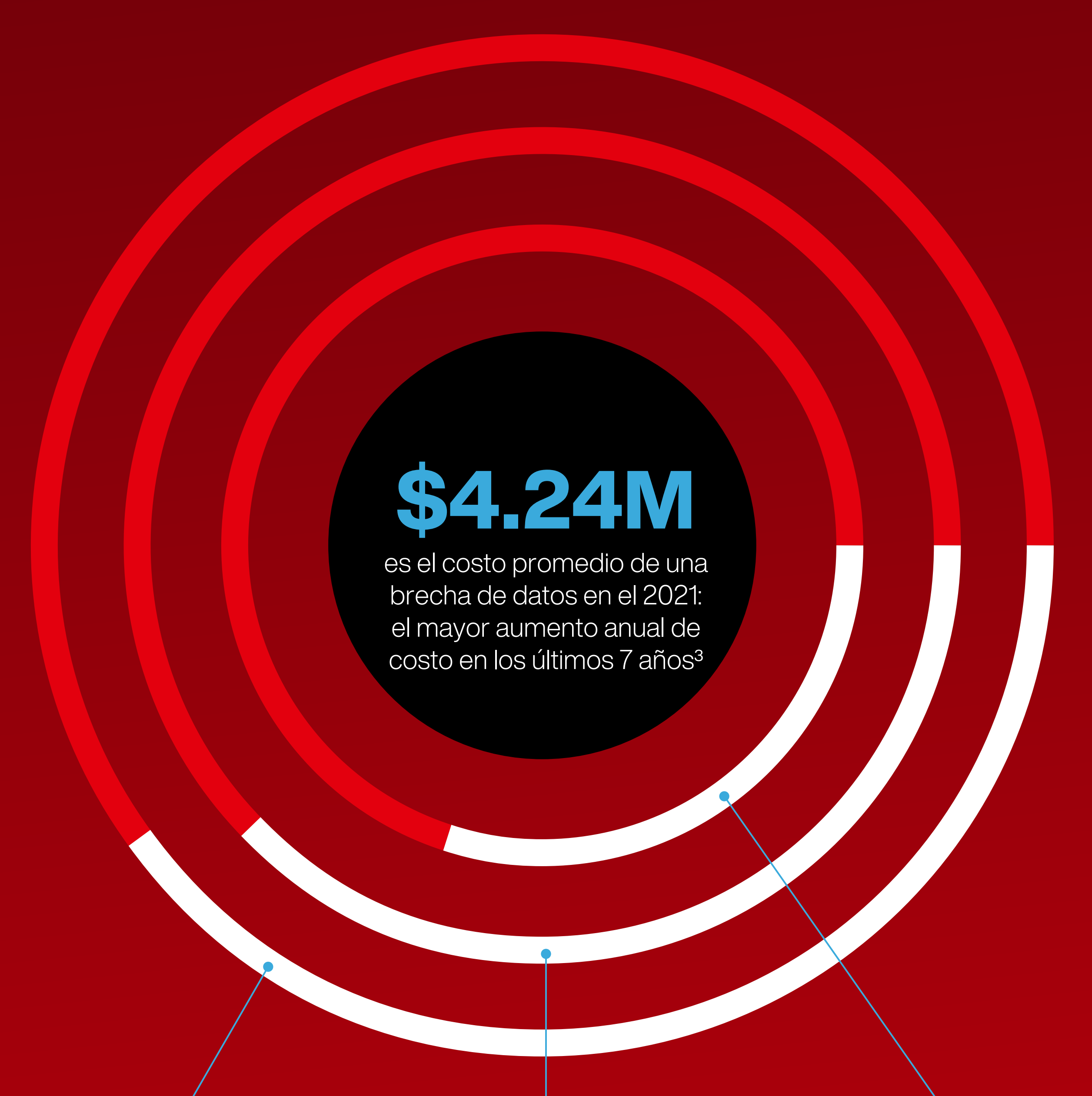
CROWDSTRIKE

Cómo impedir brechas en la nube

6 PUNTOS FUNDAMENTALES PARA PROTEGER APLICACIONES NATIVAS DE LA NUBE

Con la probabilidad de que el uso de las nubes siga aumentando, la protección de los activos de nube será un aspecto crítico en el apoyo de la transformación digital en organizaciones de cualquier tamaño, en cualquier industria, en cualquier parte del mundo. Sin embargo, el uso de la nube amplía la superficie de ataque y abre las puertas, permitiendo que los adversarios saquen ventaja. ¿Qué es necesario saber para proteger sus negocios?

¿Cuáles son las consecuencias?
"Datos fuera, malware dentro"



$4.24M
es el costo promedio de una brecha de datos en el 2021: el mayor aumento anual de costo en los últimos 7 años[3]

40%
de las empresas reportaron acceso no autorizado a las aplicaciones y datos debido a errores de configuración en la nube[2]

38%
de las empresas reportaron la introducción de malware debido a errores de configuración en la nube[2]

30%
de las empresas reportaron la introducción de ransomware debido a errores de configuración en la nube[2]

¿Por qué está ocurriendo esto?

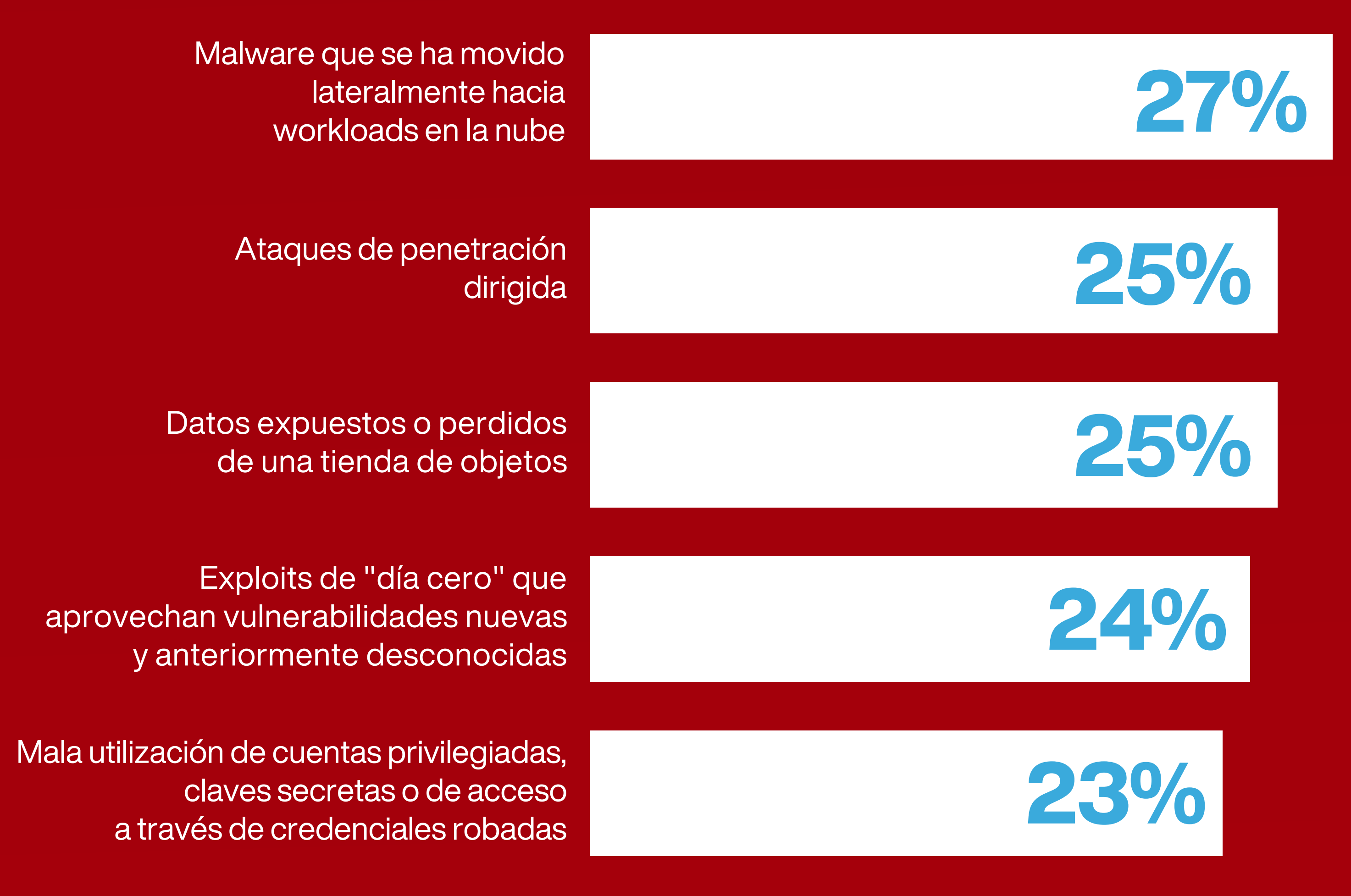
Shadow IT
- Falta de visibilidad
- Uso no autorizado
- Activos no protegidos

Complejidad de la nube
- Errores de configuración
- Constancia en la seguridad
- Uso de APIs no seguras

Amenazas de Tiempo de Ejecución
- Adversarios
- APTs/exploits de día cero
- Vulnerabilidades

Escasez de Competencias
- Gestión de identidades y accesos (IAM), gestión estratégica
- Nube/seguridad
- Responsabilidad compartida

Realidad actual:
Una amplia gama de ciberataques



Pese a todo esto, apenas **1 de cada 5 organizaciones** revisa regularmente su postura de seguridad en la nube[4]

4 principales prioridades de DevSecOps

#1 Generar constancia de seguridad en los centros de datos y ambientes de nubes públicas y privadas

#2 Automatizar la introducción de controles y procesos mediante la integración con el ciclo de vida de desarrollo de software y las herramientas de integración continua/entrega continua (CI/CD)

#3 Mejorar el conocimiento y la comprensión del modelo de amenazas y de los adversarios para las aplicaciones e infraestructura nativas de nube

#4 Consolidar una plataforma integrada nativa de nube de protección de workload de la nube

6 puntos fundamentales para proteger aplicaciones nativas de la nube

1 Que erradicar vulnerabilidades se transforme en su misión
Conozca sus imágenes. Comprenda cómo han sido construidas y qué código se utiliza, incluyendo tanto el software como la configuración.

2 Implemente la inmutabilidad del contenedor
Fortalezca sus imágenes, contenedores y hosts. Adopte la automatización para realizar monitoreos continuos e implemente verificaciones a medida que gestiona y cumple con los reglamentos.

3 Reduzca la superficie de ataque antes del tiempo de ejecución
Utilice un abordaje "shift left" en la seguridad para identificar y corregir vulnerabilidades de forma temprana. Haga la integración con sus herramientas de CI/CD como DevOps de Azure o Jenkins.

4 Implemente el control de acceso
Asegure la segregación de su ambiente de contenedor e integre las herramientas de control de acceso con directorios de la empresa para una gestión detallada de los accesos y una mejor visibilidad.

5 Automatice la protección en tiempo de ejecución
La inmutabilidad de los contenedores permite una identificación más rápida y precisa de las amenazas. Dimensione la protección en tiempo de ejecución mediante la automatización de la protección contra amenazas y la detección de anomalías con base en el comportamiento del contenedor.

6 Auditar, auditar y auditar nuevamente
Adopte procedimientos para minimizar la proliferación de contenedores y elimine contenedores e imágenes de riesgo.

Fuentes:
1. State of Cloud Security 2021 (Ermetic/IDC)
2. The Maturation of Cloud-native Security: Securing Modern Apps and Infrastructure (ESG, March 2021)
3. https://www.foley.com/en/insights/publications/2021/07/4-24m-now-the-average-cost-per-data-breach
4. Implementing Cloud Security Best Practices — August 2020 (Tripwire)

Acerca de CrowdStrike

CrowdStrike, líder mundial en ciberseguridad, está redefiniendo la seguridad para la era de la nube con una plataforma de protección de endpoints construida desde cero para detener las brechas. La arquitectura de un agente único y liviano de la plataforma CrowdStrike Falcon® aprovecha la inteligencia artificial (IA) en escala de nube y ofrece protección y visibilidad en tiempo real en toda la empresa, evitando ataques en endpoints y workloads, dentro o fuera de la red. Con la tecnología patentada de la CrowdStrike Threat Graph®, CrowdStrike Falcon correlaciona más de 1 billón de eventos por semana en tiempo real relativos a endpoints de todo el mundo, alimentando una de las plataformas de datos más avanzadas del mundo en seguridad.