Netdata®

CYBERSECURITY

Caso de éxito

Como asegurar de forma integral de más de 6000 cajeros automáticos

Aislamiento de amenazas

en 1 a 2 minutos

Bloqueo del 100%

de intentos de penetración

Aislamiento inmediato

por comportamiento sospechoso

Reglas automáticas con IA

para infraestructura Legacy

Netdata®

Desafío

Una entidad financiera líder en Latinoamérica opera como un conglomerado regional con una presencia en el mercado colombiano y en toda Latam. Su infraestructura constituye uno de sus activos más críticos, sustentada en una red que supera los 6000 cajeros automáticos y quiscos en la región, los cuales funcionan como el principal punto de contacto físico y transaccional para millones de ciudadanos. La relevancia de esta red no se limita únicamente a la disponibilidad de efectivo, sino que representa la capilaridad de la entidad en el territorio nacional, exigiendo una operatividad continua y segura.

Esta red regional masiva demanda un modelo de ciberseguridad unificado y altamente sofisticado, capaz de proteger nodos críticos de procesamiento de datos en entornos geográficamente dispersos y con diferentes especificaciones de hardware.

Esta organización enfrentaba el problema de tener vulnerabilidades críticas en su infraestructura física. El incidente detonante ocurrió cuando actores maliciosos lograron violentar un cajero y acceder a su hardware interno, conectando dispositivos periféricos no autorizados para intentar ejecutar acciones maliciosas. La solución de seguridad anterior, basada en un antivirus tradicional, demostró tener límites frente a dispositivos personalizados y amenazas avanzadas que no dependen de firmas conocidas.

La empresa intentó con otras desplegar diferentes soluciones para proteger su red de cajeros y quiscos, pero varias tenían limitantes, sin que dieran respuesta integral a las necesidades de aseguramiento.

Netdata®

Proceso

El proyecto inició con un levantamiento minucioso de la diversidad de hardware de la entidad, que incluía más de 10 modelos de cajeros de distintas marcas y Quioscos que también permiten transacciones en efectivo. El equipo técnico identificó entre 60 y 70 componentes específicos por cada modelo (lectores, impresoras, chipsets PCI) que debían ser mapeados para garantizar su correcto funcionamiento bajo un esquema de seguridad restrictivo.

Se aplicó una metodología de "bloqueo total" inicial, habilitando progresivamente solo los procesos lógicos y conexiones PCI esenciales para la operación. Este proceso de higienización permitió eliminar riesgos de dispositivos periféricos desconocidos y asegurar que cada máquina funcionara exclusivamente con sus piezas originales.

Netdata®

Solución

Se implementó una arquitectura de protección avanzada basada en **Cortex XDR**, que permitió centralizar la administración de la seguridad y el firewall local de cada cajero. La solución integra:

- Detección de amenazas basada en comportamiento (tácticas y técnicas MITRE).
- Automatización de respuesta para el aislamiento inmediato de máquinas ante sospechas de compromiso.
- Control total sobre dispositivos periféricos y USB.

Netdata®

Resultados Tangibles

Bloqueo del 100% de ataques en pruebas de penetración

El control detuvo todos los intentos de ejecución de malware y conexión de hardware no autorizado, incluyendo dispositivos con identificadores de clase ocultos.

Aislamiento en tiempo real:

Se logró reducir el tiempo de respuesta ante incidentes, permitiendo que una máquina sea contenida y aislada de la red en un intervalo de 1 a 2 minutos.

Visibilidad profunda de procesos:

La telemetría avanzada ahora permite identificar fallos operativos y errores de configuración en el software del cajero que antes eran invisibles para el equipo de soporte.

Testimonio del Cliente

"Logramos elevar la protección de nuestra infraestructura crítica a un nivel de sofisticación que el mercado actual exige. Ahora tenemos la certeza de que cada conexión física en nuestros cajeros está monitoreada y que podemos actuar sobre cualquier anomalía de forma remota y automática, sin afectar la experiencia de nuestros usuarios."

Gerencia de Ciberseguridad.

Conclusión

La seguridad en cajeros automáticos no se resuelve con herramientas genéricas. Este caso confirma que la combinación de un mapeo detallado de hardware, junto con una capacidad de respuesta automatizada, transforma una infraestructura vulnerable en un entorno resiliente y bajo control total.

Netdata conoce los diferentes tipos de infraestructuras críticas en cajeros automáticos. Al haber mapeado la diversidad de hardware legacy y los componentes internos de múltiples marcas disminuye drásticamente el tiempo de levantamiento de información para nuevas implementaciones, permitiendo una transición eficiente hacia modelos de seguridad restrictivos sin comprometer la operación del negocio. Más allá de la protección contra amenazas, obtiene una capacidad de respuesta automática que aísla máquinas sospechosas en cuestión de minutos y una telemetría avanzada que brinda visibilidad sobre errores lógicos del sistema, transformando la ciberseguridad en una herramienta de diagnóstico y control preventivo para toda la red financiera.

Netdata®

www.netdatanetworks.com