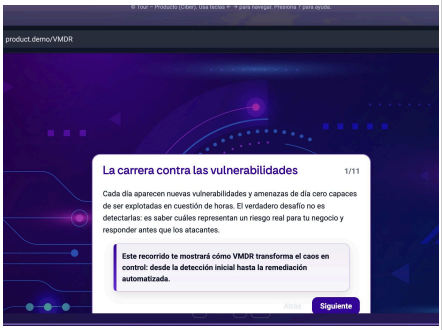
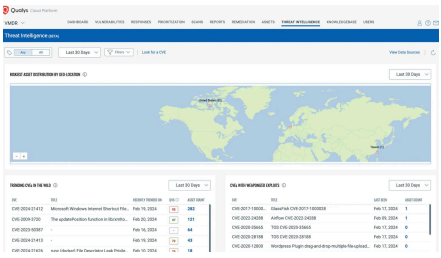
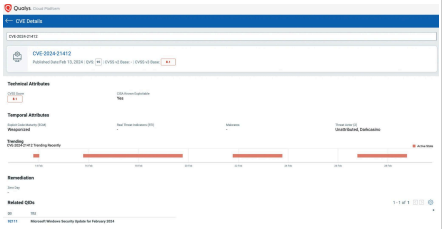
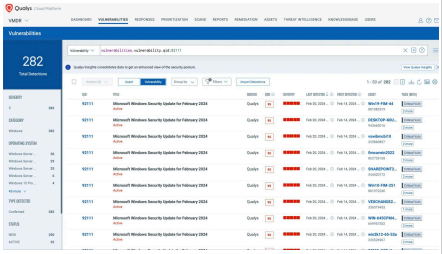
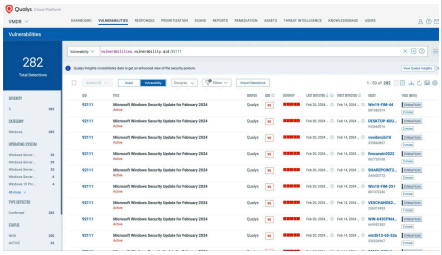
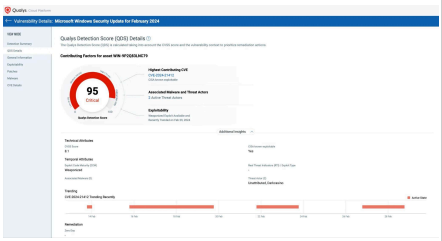
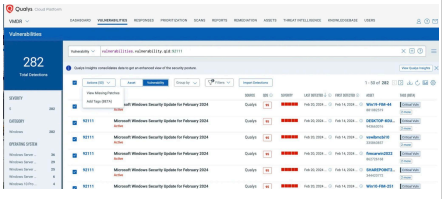
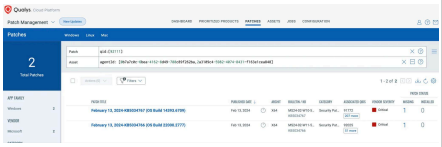
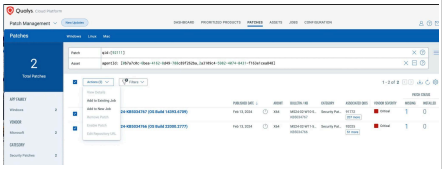
Guia Preventa - Product Tour (VMDR)

Storytelling VMDR (Zero-Day Case) (5 minutos)

⏱️ ***Duración estimada: cada bloque toma entre 35 y 45 segundos, sumando en total unos 5 minutos con ritmo fluido.***

Paso	Speech (para presentar)	Tarjetas (mini-storytelling autónomo)
1 – La carrera contra las vulnerabilidades 	Hoy las organizaciones están en una carrera constante contra el tiempo. Cada día aparecen vulnerabilidades y amenazas de día cero que pueden explotarse en cuestión de horas. El reto ya no es descubrirlas, porque alertas sobran; el reto es priorizar, identificar qué es realmente crítico para el negocio y actuar antes de que un atacante lo aproveche. Qualys VMDR cambia esa dinámica: convierte un escenario caótico en un flujo claro y controlado, automatizando desde la detección hasta la respuesta.	La carrera contra las vulnerabilidades: Cada día aparecen nuevas vulnerabilidades y amenazas de día cero capaces de ser explotadas en cuestión de horas. El verdadero desafío no es detectarlas: es saber cuáles representan un riesgo real para tu negocio y responder antes que los atacantes. Este recorrido te mostrará cómo VMDR transforma el caos en control: desde la detección inicial hasta la remediación automatizada.
2 – Detección de vulnerabilidad crítica 	La velocidad lo es todo. VMDR detecta en minutos la vulnerabilidad más crítica y evalúa de inmediato el impacto en toda la organización. Esto permite priorizar acciones y adelantarse a posibles explotaciones. En lugar de analizar cientos de alertas, la plataforma señala lo que de verdad puede comprometer operaciones.	Detección de vulnerabilidad crítica: En minutos, VMDR identifica la vulnerabilidad más relevante y evalúa su impacto en toda la organización, adelantándose a los atacantes.

3 – Análisis de la CVE 	Una vez identificada la amenaza, necesitamos comprenderla a fondo. VMDR nos da el detalle completo de la vulnerabilidad: cómo funciona, qué sistemas puede afectar y en qué contexto podría explotarse. Esa información permite tomar decisiones informadas y preparar la respuesta más adecuada.	Análisis de la CVE: Accedemos al detalle de la vulnerabilidad (CVE) para entender su funcionamiento, alcance y los activos que podrían verse comprometidos.
4 – Indicadores de explotación 	No todas las vulnerabilidades requieren la misma urgencia. VMDR utiliza inteligencia de amenazas para confirmar si una vulnerabilidad ya está siendo explotada en el mundo real. Cuando esto ocurre, la prioridad pasa de importante a crítica inmediata. Así, los equipos saben dónde actuar sin perder tiempo en ruido.	Indicadores de explotación: Verificamos si la vulnerabilidad ya está siendo explotada en ataques reales. Cuando esto ocurre, la necesidad de respuesta se vuelve inmediata.
5 – Activos afectados 	Aquí es donde entra en juego la priorización inteligente. Una organización puede tener miles de vulnerabilidades detectadas, pero no todas tienen el mismo peso. Con Qualys Detection Score, VMDR prioriza de manera automática aquellas que realmente amenazan al negocio. Esto asegura que el esfuerzo se concentre en lo que más importa.	Activos afectados: VMDR detecta múltiples vulnerabilidades, pero con Qualys Detection Score (QDS) priorizamos solo las que realmente amenazan al negocio, optimizando recursos.
6 – Evaluación precisa del riesgo 	El siguiente paso es evaluar el riesgo con precisión. Con Qualys Vulnerability Score, no solo tenemos un listado de fallos, sino un puntaje que refleja el nivel real de riesgo para la continuidad del negocio. Esto ayuda a alinear a los equipos técnicos y a la dirección en una visión común de lo que es verdaderamente crítico.	Evaluación precisa del riesgo: Qualys Vulnerability Score (QVS) combina indicadores clave y determina si una vulnerabilidad representa un riesgo crítico para la continuidad del negocio.
7 – Parches pendientes 	Una vez que sabemos qué vulnerabilidad debemos atender, VMDR nos indica de inmediato qué parches faltan. Lo más potente es que no se trata de una búsqueda manual: en un clic se identifican los parches pendientes y se habilita su aplicación inmediata, reduciendo la ventana de exposición.	Parches pendientes: Con un solo clic, VMDR identifica los parches faltantes y habilita su aplicación inmediata, reduciendo al mínimo el tiempo de exposición.

8 – Gestión de parches integrada 	VMDR integra la gestión de parches en el mismo flujo de trabajo. Eso significa que podemos pasar directamente de la detección a la corrección, priorizando los sistemas más críticos y reduciendo tiempos de manera significativa.	Gestión de parches integrada: En un flujo unificado pasamos de la detección al parcheo, asegurando la protección de los sistemas más críticos de forma ágil y efectiva.
9 – Acciones integrales 	Más allá de corregir, VMDR ayuda a demostrar control. La plataforma permite orquestar acciones, programar trabajos de parches y generar reportes claros con métricas de riesgo como TruRisk. Así, el área técnica muestra evidencia concreta a auditores y líderes de que los activos críticos están bajo control.	Acciones integrales: VMDR permite gestionar trabajos de parches y generar reportes de riesgo y métricas TruRisk, demostrando control total sobre los activos impactados.
10 – Reportes y tablero VMDR 2.0 	Finalmente, todo lo anterior se traduce en visibilidad clara y en tiempo real. Con VMDR 2.0, el tablero ejecutivo muestra exposición, reducción de riesgo y estado de cumplimiento en un solo lugar. Así, tanto equipos técnicos como dirección pueden ver el nivel de riesgo de negocio de un vistazo.	Reportes y tablero VMDR 2.0: De la visibilidad técnica al impacto ejecutivo: reportes claros muestran exposición, reducción de riesgo y cumplimiento. Con VMDR 2.0, el tablero evoluciona para ofrecer una visión en tiempo real del riesgo de negocio, de un vistazo.
11 – Seguridad proactiva con VMDR 	Este tour nos lleva de un punto inicial —una vulnerabilidad crítica— hasta la respuesta completa: detección, priorización y remediación en un flujo continuo. Con VMDR, la gestión de vulnerabilidades deja de ser reactiva y se convierte en una estrategia proactiva, alineada con los objetivos del negocio y respaldada por métricas claras.	Seguridad proactiva con VMDR: De una vulnerabilidad crítica a una respuesta completa: detección, priorización y remediación en un solo flujo. VMDR convierte la gestión de vulnerabilidades en una estrategia clara, medible y alineada con los objetivos de negocio. Has completado el tour. Ahora tienes una visión precisa de cómo VMDR protege a tu organización frente a las amenazas más críticas.