ESTUDIO DE CASO

AutoNation aborda rápidamente la protección y mejora la seguridad en los puntos finales

"Cuando obtuvimos una visibilidad completa de todo nuestro entorno, descubrimos que teníamos un problema importante con la moneda de revisión que no era visible con nuestras herramientas anteriores", dijo Ken Athanasiou, CISO de AutoNation.

AutoNation, el minorista automotriz más grande de los Estados Unidos, emplea a unas 26 000 personas en más de 300 sedes en todo el país. Aunque todas las sedes de AutoNation están conectadas a una red central de TI, la empresa había tenido dificultades para cumplir con las expectativas de aplicaciones de revisiones del CISO. Como resultado, no se estaban implementando las revisiones críticas de manera oportuna y no se estaban cumpliendo los objetivos. El equipo de Ken sabía que tenían un problema; sin embargo, Tanium les permitió ver la verdadera magnitud del problema y hacer un seguimiento en tiempo real de la efectividad de las actividades de corrección.

AutoNation utilizó Tanium por primera vez para implementar una actualización a gran escala de Microsoft BitLocker (una función de cifrado de disco) en todo su entorno, y lo hizo en un plazo de 30 días. El equipo de AutoNation se mostró escéptico de que se pudiera hacer en ese plazo sin recursos masivos de mano de obra. Aprovechando las habilidades del equipo de administración de cuentas técnicas de Tanium y las capacidades extensibles de la plataforma Tanium, AutoNation logró la implementación según lo programado sin requisitos adicionales de mano de obra. Este éxito le permitió a AutoNation ahorrar decenas de miles de dólares solo gracias a este esfuerzo y demostró el potencial de las capacidades exclusivas de Tanium dentro del entorno de AutoNation.

Casos de uso de Tanium

- Protección de la seguridad
- Detección y respuesta
- Administración de las operaciones de TI

Desafíos

- Visibilidad limitada: se demoraron días en obtener información del entorno
- Cientos de miles de revisiones faltantes, algunas que se remontaban al año 2007
- A muchos equipos les faltaban seis o más revisiones críticas
- Agentes SCCM rotos en un gran porcentaje de equipos
- Muchas demoras para actualizar las revisiones e incapacidad para garantizar la implementación de todas las revisiones

Beneficios para TI

- Visibilidad en tiempo real y tiempos de respuesta ante incidentes muy reducidos
- Más del 99 por ciento de éxito en la aplicación de revisiones y mayor velocidad para aplicar las revisiones en los sistemas
- Presencia evaluada de SCCM y completamente implementada en toda la empresa
- Mayor productividad administrativa de TI en general

> En mi vida profesional, nunca he visto este nivel de visibilidad en tiempo real.

Ken Athanasiou

Director de Seguridad de la Información

Aplicación de revisiones

Mediante Tanium, el equipo de AutoNation realizó una evaluación integral de la protección de la seguridad que validó las sospechas de deficiencias en la aplicación de revisiones del proceso de implementación de software existente. Esto confirmó que las herramientas actuales de administración eran, en cierto modo, menos efectivas. De hecho, cientos de miles de revisiones no se habían aplicado correctamente, entre ellas, algunas que databan de 2007. Además, el 91 por ciento de los puntos finales tenía una versión obsoleta de Adobe Flash. "Ahora podemos obtener respuestas en tiempo real de todo nuestro entorno, en segundos", dijo Ken. "En mi vida profesional, nunca he visto este nivel de visibilidad en tiempo real". Con más de 300 sedes dispersas en todo el país, ha sido difícil introducir las revisiones de manera eficaz. Con Tanium, AutoNation ahora puede implementar las revisiones con una tasa de éxito en el primer intento de más del 99 por ciento.

SCCM

AutoNation también utilizó Tanium para aumentar la eficacia de Microsoft SCCM (System Center Configuration Manager). Después de vincular Tanium con SCCM, descubrieron que SCCM no estaba funcionando completamente en un gran porcentaje del entorno. El equipo de AutoNation utilizó Tanium para corregir este problema al volver a implementar el agente SCCM en los puntos finales que no respondían. Víctor Pena, ingeniero de arquitectura de clientes de AutoNation, quedó muy impresionado por la velocidad de Tanium durante todo el proceso: "SCCM a veces demora una o dos horas solo para implementar un paquete en el equipo de un usuario. Ahora podemos escribir en ese equipo e implementar en minutos. Así fue como se convenció el equipo de operaciones de AutoNation".

Mejorar la seguridad actual de los puntos finales

Jeff Johnson, Director de operaciones de seguridad de la información de AutoNation, también aprovechó Tanium para ayudar a mejorar la estrategia de seguridad de los puntos finales de la empresa. La implementación de un nuevo software antivirus (AV) de terceros normalmente tardaría meses en instalarse en los 20 000 equipos de AutoNation. Gracias a Tanium, fue posible hacerlo en cuatro días.

Además de las capacidades de implementación, Tanium ayudó con el tiempo de respuesta ante incidentes. "Cuando llegamos a una estación de trabajo infectada, el software de AV anterior estaba roto o corrupto a causa de una mala instalación", dijo Jeff. "Tanium nos permite poner en cuarentena los equipos sospechosos o infectados para efectuar su corrección. Esto reduce nuestro tiempo de respuesta a menos de una hora en lugar de días y, mejor aún, ya no necesitamos enviar a un ingeniero a la tienda".

Casos de uso en el futuro

Como parte de su enfoque continuo en la promoción de sus funciones y capacidades de ciberseguridad, el equipo de AutoNation continúa aprovechando Tanium para explorar e implementar nuevos casos de uso y procesos que habrían sido difíciles, o incluso imposibles, sin la plataforma. Uno de los que genera más entusiasmo en Jeff es Tanium Comply: "El nuevo módulo Comply será revolucionario. Tanium proporciona visibilidad casi en tiempo real para determinar el cumplimiento de los requisitos normativos cada vez mayores de los auditores y satisfacer de inmediato las solicitudes de los auditores". Tanium Comply verifica los puntos finales comparándolos con las referencias de seguridad estándar y las definiciones de vulnerabilidades, proporcionando resultados casi instantáneos en toda la empresa. Con estos resultados completos, las organizaciones pueden mejorar la protección general de la seguridad y simplificar la preparación para auditorías como PCI, HIPAA y SOX.

TANIUM

Tanium ofrece una plataforma de seguridad y administración de puntos finales creada para los entornos de TI más exigentes del mundo. Muchas de las organizaciones más grandes y sofisticadas del mundo, incluida casi la mitad de las empresas de Fortune 100, los principales minoristas e instituciones financieras y varias ramas de las Fuerzas Armadas de los EE. UU., confían en Tanium para tomar decisiones seguras, operar de manera eficiente y mantenerse resilientes contra las interrupciones. Visítenos en www.tanium.com y síganos en LinkedIn y Twitter.

©2021 Tanium. Todos los derechos reservados.

TANIUM