BlackBerry
CYLANCE

CASO DE ESTUDIO ALIMENTACIÓN AGUAS MINERALES Y HOSTELERÍA-BALNEARIOS.

Vichy Catalan da un paso al frente en Ciberseguridad

INDUSTRIA
Alimentación
aguas minerales y
hostelería-balnearios.

ENTORNO
- 350 endpoints y 50 servidores protegidos por CylancePROTECT® y CylanceOPTICS®.

OBJETIVOS
- Asegurar los sistemas que contienen información confidencial y crítica para el negocio, y equipos de usuarios e industriales con una solución de detección de malware eficaz contra las nuevas amenazas de malware zero-day prácticamente del 100%.
- Disponer de mayor visibilidad, optimizar y automatizar la respuesta rápida a nuevas amenazas.

SOLUCIÓN
- Desplegar CylancePROTECT y CylanceOPTICS® para proteger los endpoints contra amenazas de ransomware con la máxima prevención.
- Reducción drástica del tiempo dedicado a la gestión de alertas e incidentes.

VICHY CATALAN CORPORATION

La empresa

Vichy Catalan Corporation lo forman tres líneas de negocio: Premium Mix Group (fabricante y comercializador de agua mineral natural, zumos y bebidas saludables sin azúcar), Manantial de Salud (distribuidor) y el Hotel Balneario Vichy Catalan. Como fabricante dispone de diferentes plantas, bases logísticas y productos exclusivos, como Monte Pinos, Mondariz, Font D'Or o Lambda.
La innovación de producto y el I+D+i forma parte de su estrategia con nuevas bebidas a base de agua mineral natural, ingredientes naturales y sin azúcar, que aportan salud y bienestar a sus consumidores. Su lema es "Empresa única sin papeles".
Ackcent es el proveedor de servicios y soluciones de ciberseguridad de Vichy Catalan, habiendo realizado el proyecto de despliegue y posterior servicio de gestión y monitorización 24x7 desde el SOC de Ackcent.

La situación

Vichy Catalan disponía de una protección de endpoint tradicional, basada en firmas de virus, desplegada en todos sus servidores y puestos de trabajo, teniendo en cuenta que muchos empleados los utilizan fuera de la red corporativa.

400
ENDPOINTS
PROTEGIDOS

"Desde que estamos con el servicio de Cylance gestionado por Ackcent tenemos mayor visibilidad preventiva de las amenazas y no hemos vuelto a tener por el momento incidentes de malware. Con la solución antivirus tradicional anterior llegó un momento en que perdimos la confianza de tener un nivel de protección adecuado."

Benito Cerrillo
CIO de Vichy Catalan

La anterior solución de antivirus requería una infraestructura dedicada de servidores para gestionar la protección implementada en los endpoints, lo que incrementaba la complejidad de la administración, al tiempo que exigía invertir un tiempo valioso, que se restaba a otros proyectos y servicios de mayor prioridad para la compañía.

Otro gran inconveniente identificado de este enfoque tradicional eran las actualizaciones de las firmas que, aparte de depender de constantes revisiones, no se realizaban correctamente, por lo que demandaba un mantenimiento correctivo, ya que constituía un gran factor de riesgo. Una de las grandes prioridades de Vichy Catalan es la seguridad de la información y, por ello, la compañía estableció como estratégico contar con una solución de protección de endpoint preventiva, capaz de detectar y bloquear malware de tipo zero days y amenazas avanzadas que puedan surgir, con un porcentaje de detección de malware prácticamente del 100%. Por todo ello, la compañía decidió que era necesario reemplazar la solución antivirus existente.

El proceso

En Vichy Catalan se realizó una comparativa para evaluar Cylance y la solución next-generation de otro fabricante. Teniendo en cuenta la efectividad de detección y de bloqueo de distintos softwares maliciosos (Wannacry, Cryptolocker, Cryptowall, Rombertik, Dridex, Dyre, etc.), en tiempo real antes de que se pueda ejecutar y causar daños. Además, se evaluó la dependencia de conexión a Internet y de actualizaciones permanentes. Finalmente, se evaluaron también los beneficios de la funcionalidad EDR (Endpoint Detection and Response).
Una vez analizadas las diferentes características tecnológicas y los beneficios ofrecidos, el cliente decidió por la solución de Cylance por su alto grado de protección frente a nuevas amenazas y por la total transparencia que ofrece frente al usuario.

Además, cabe destacar que la tecnología de Cylance reducía drásticamente la carga de trabajo del equipo IT para la gestión de alertas e incidentes de seguridad.

Para optimizar el despliegue y mitigar posibles riesgos, el proyecto se acompañó de servicios del fabricante, ThreatZero. Este servicio se llevó a cabo en tres fases: la primera de preparación y configuración, revisión y puesta en marcha de las mejores prácticas. En la segunda fase, se realizaron la gestión de alertas y revisión de las detecciones. En la tercera fase, se implementaron las políticas de seguridad de bloqueo.

Finalmente se configuró CylanceOPTICS, la solución EDR para proporcionar una visibilidad más detallada de las amenazas más complejas, con capacidad adicional de respuesta inmediata.

Los resultados

En primer lugar, el hecho de introducir la solución de Cylance, basada en Cloud, no ha requerido ninguna inversión en hardware, a la vez que se ha eliminado la infraestructura dedicada a la gestión de la solución antivirus reemplazada.

Desde que se ha implementado la solución de Cylance, el SOC de Ackcent ha detectado más de 800 alertas, incluyendo múltiples ficheros infectados con malware tipo ransomware, siendo todos ellos detenidos antes de su ejecución.

En cuanto a procesos, se ha eliminado la necesidad de actualizaciones y escaneos que se hacían periódicamente de su anterior antivirus, simplificando radicalmente los procesos de seguimiento, actualización y revisión de alertas.

Por último, a nivel de costes, se han eliminado los costes "ocultos", sobre todo aquellos asociados a incidentes de seguridad, difíciles de cuantificar, pero muy significativos.

ackcent cybersecurity
Passeig de Gràcia, 11
08007 Barcelona, España
info@ackcent.com
+34 933 620 002

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
BlackBerry CYLANCE