

Gobierno de la Ciudad de Buenos Aires



Protección de las redes esenciales con Symantec Multi-tier Protection

Después de que un virus impidiera que los usuarios accedieran a la red durante 12 horas, el Gobierno de Buenos Aires supo que necesitaba una mejor solución de seguridad. Symantec Multi-tier Protection cumplió con todos los requisitos de la ciudad, ya que proporcionó administración desde una sola consola, elaboración de informes gráficos, protección contra software espía y protección antivirus para Linux. La solución redujo en gran medida el tiempo fuera de servicio provocado por los programas maliciosos, mejoró la efectividad con una sola consola de administración, redujo casi todo el spam que afectaba a los usuarios y ahorró más de 450 horas de personal por año que estaban destinadas a resolver el problema del spam.

PERFIL DE LA ORGANIZACIÓN

Con 200.000 empleados, el Gobierno de Buenos Aires en Argentina (www.buenosaires.gov.ar) supervisa prácticamente todo lo que ocurre en esta cosmopolita ciudad de 12,4 millones de personas, desde servicios de hospitales, de bomberos hasta la planificación urbana y el arte.

SECTOR

Gobierno: estatal y local

SOLUCIÓN

Protección de los Endpoints

“Symantec fue el que mejor cumplió con todos nuestros requisitos”

Gustavo Linares

Director de Seguridad de la Información
Gobierno de Buenos Aires

Algunas veces conocido como el “París de América Latina”, Buenos Aires cuenta con un rico patrimonio compuesto por arquitectura europea clásica, excelentes museos, un escenario cultural vibrante y clubes de tango conocidos en todo el mundo. Además, es el centro comercial y financiero de Argentina, y tiene uno de los puertos más activos del mundo.

Con 200.000 empleados, el gobierno municipal administra todos los aspectos de la vida de la ciudad, desde hospitales y servicios de emergencias hasta la policía, la planificación urbana y el arte. La red informática del gobierno respalda todas estas actividades, ya que brinda servicios a 10.000 usuarios y cuenta con una amplia gama de aplicaciones, incluidos el sistema de emergencias 103 de la ciudad, el presupuesto y la administración, entre otros.

La red estaba protegida con una solución antivirus de Trend Micro, pero el personal de TI del gobierno sentía muy insatisfecho con el producto. Para una cosa, el personal de TI tenía que administrar la seguridad de la red desde varias interfaces en lugar de una. Además, si bien el producto de Trend Micro proporcionaba protección contra virus, el gobierno tuvo que instalar otro producto por separado para brindar protección contra el software espía. El producto de Trend Micro tampoco ofrecía protección para los equipos basados en Linux de varios departamentos.

Lo peor de todo, las operaciones de Argentina de Trend Micro no parecía brindar un soporte adecuado para el producto. “Había problemas, tal vez como los tendría cualquier otro producto”, afirma Gustavo Linares, Director de Seguridad de la Información, Gobierno de Buenos Aires. “Lamentablemente, no existía un servicio de soporte capaz de solucionar estos problemas cuando surgían”.

Symantec Mail Security para SMTP eliminó el spam que atravesaba el filtro de la solución anterior.

Como la solución antivirus no se ejecutaba en un nivel óptimo, la ciudad descubrió que era vulnerable a los ataques. “En Agosto del 2004, un virus corrompió la base de datos SQL de Administración de los usuarios registrados de nuestra red”, explica Linares. “Los usuarios no pudieron acceder al sistema durante casi 12 horas, porque el virus hizo colapsar la red.” Esto implicó que 45 personas trabajaran durante tres o cuatros días para solucionar el problema, agrega.

LA SOLUCIÓN

Convencidos de que era hora de implementar una nueva solución de seguridad, el personal de TI evaluó cuatro soluciones de seguridad diferentes en agosto de 2007, que incluían Trend Micro, Panda Security, McAfee y Symantec. Si bien la solución Symantec™ Multi-tier Protection no era la opción de menor costo, “Symantec fue el que mejor cumplía con todos nuestros requisitos”, afirma Linares. “Y se acercaba a nuestro presupuesto”.

Symantec Multi-tier Protection combina Symantec™ Endpoint Protection con protección contra programas maliciosos para entornos heterogéneos de la empresa típica. Symantec Endpoint Protection ofrece tecnologías de antivirus, antispyware, firewall de equipo de escritorio, prevención de intrusiones y control de aplicaciones y dispositivos; todo esto controlado mediante un solo agente.

¿Por qué Symantec Multi-tier Protection fue la opción correcta? “Existían requisitos de cumplimiento legales que sólo funcionarían con el producto de Symantec”, comenta Linares. “Además, cumplía en un 100% con los requisitos técnicos que teníamos. Y utiliza menos recursos en el equipo de escritorio, lo que constituye un factor muy valioso para nosotros”.

La consola única de Symantec Endpoint Protection también ofrece beneficios. “Ése era uno de los requisitos de nuestras especificaciones técnicas, y era uno de los problemas que teníamos con la solución de Trend Micro, ya que se debía administrar desde diferentes consolas”, cuenta Linares.

Además, explica, la función de elaboración de informes gráficos basada en Web de

Symantec Endpoint Protection es una gran ayuda. “No es fácil controlar una red de miles de personas; por lo tanto, los informes son muy importantes para nosotros”, afirma. “El hecho de que Symantec incluya protección contra el software espía y el software de publicidad no deseada significa que ya no necesitamos utilizar dos soluciones diferentes. Para nosotros, es muy importante que un solo producto cubra estas necesidades”, dice Linares.

Además, valora la protección antivirus para Linux que proporciona Symantec Multi-tier Protection. “Muchas oficinas de la ciudad dependen de Linux, y antes de esta adquisición no contábamos con protección antivirus para ellas”, dice.

LOS RESULTADOS

La ciudad escogió a Symantec en octubre, y la solución fue implementada en diciembre. Al mismo tiempo, el personal de TI también implementó otro componente de Symantec Multi-tier Protection, Symantec™ Mail Security para SMTP, para reducir la cantidad de spam que ingresaba en su red.

En unas pocas semanas, Mail Security para SMTP ya había demostrado su valor. “Más del 25% del correo electrónico que recibían los usuarios solía ser spam, pero eso prácticamente se ha eliminado”, comenta Linares.

Con la solución anterior de Trend Micro, entre un 45 y 50% del correo entrante se identificaba como spam. Gracias a Symantec Mail Security para SMTP, ese porcentaje aumentó a un 65%. En el pasado, el spam que el filtro no detenía tenía que ser eliminado por el personal. “Ahora, parece que el spam casi no pasa”, dice.

La reducción del spam generó ahorros significativos de tiempo para el personal, agrega. Con la solución anterior, los usuarios no sólo tenían que perder tiempo en eliminar el spam, sino que también tenían que enviar informes sobre el spam a los administradores de TI. Como consecuencia, dos administradores perdían una hora al día, una durante la mañana y otra durante la tarde, eliminando de forma manual el spam del buzón de los usuarios. Por lo tanto, sólo en cuanto al tiempo que el personal de TI

“Más del 25% del correo electrónico que recibían los usuarios solía ser spam, pero eso prácticamente se ha eliminado”

Gustavo Linares

Director de Seguridad de la Información
Gobierno de Buenos Aires

dedicaba, Mail Security para SMTP generó ahorros de más de 450 horas al año.

El partner ComPlus Seguridad Informática de Symantec ayudó al Gobierno de Buenos Aires mediante la evaluación y la implementación de productos de las soluciones de Symantec. También brinda la primera línea de soporte para estos productos. “Son muy útiles”, dice Linares. Además, el Gobierno de Buenos Aires cuenta con Symantec Essential Support Services para proporcionar soporte continuo; otro elemento requerido en las especificaciones del gobierno.

Los planes futuros incluyen una posible activación de la función Network Access Control opcional que está incorporada en el agente de Symantec Endpoint Protection. Esto proporcionaría una mayor protección para la red de la ciudad cuando empleados como los inspectores conecten sus equipos portátiles a la red después de trabajar fuera de la oficina. El gobierno también puede utilizar Symantec Consulting Services en dos futuros proyectos importantes: la creación de un manual de política de seguridad y la evaluación de vulnerabilidades para garantizar que la red esté completamente protegida.

Cuando se le preguntó cuánto tiempo le llevaría al Gobierno de Buenos Aires recuperar la inversión en Symantec, Linares contestó: “Ésta es una evaluación diferente para un gobierno cuando se tiene en cuenta la importancia de la información. Si se produjera un ataque contra la información del gobierno, la confianza en éste se desmoronaría inmediatamente. La ciudad se vería afectada, y se produciría un daño cuantitativo. Por lo tanto, los beneficios de un producto que protege la red gubernamental se consideran inmediatos”.

Por este motivo, dice, la relación con Symantec es tan importante. “Es esencial para nosotros confiar nuestra seguridad a una empresa dedicada a brindar seguridad. Antes de esta adquisición, nuestro sistema de seguridad apenas era lo suficientemente fuerte. Ahora contamos con una solución mucho más sólida.”

DESCRIPCIÓN GENERAL DE LA SOLUCIÓN

Principales Desafíos

- Evitar los costos derivados de reparaciones y de tiempo fuera de servicio provocados por incidentes de programas maliciosos
- Mejorar el soporte local para la infraestructura de protección de los endpoints
- Proporcionar seguridad para servidores y equipos de escritorio basados en Linux
- Simplificar la elaboración de informes y la administración de la seguridad
- Consolidar las soluciones de antivirus y antispyware
- Lograr el cumplimiento de las normas de la ciudad

Solución

Soluciones de protección de endpoints unificadas y más rápidas con una única consola de administración; seguridad de la red más sólida; spam reducido

Productos de Symantec

- Symantec™ Multi-tier Protection

Servicios de Symantec

- Symantec Essential Support Services

Partner de Symantec

ComPlus Seguridad Informática (www.complus-arg.com.ar)

Entorno tecnológico

- Aplicaciones: numerosas aplicaciones propias y con licencia, incluido el sistema de emergencia 103 del gobierno, y la aplicación de presupuesto y contabilidad del gobierno
- Bases de datos: SQL Server 2005, Oracle 7, MySQL 5, PostgreSQL 8.2
- Servidores: alrededor de 80 servidores, principalmente HP e IBM, que ejecutan Microsoft Windows Server 2000 y 2003, Sun Solaris 10, Debian 4.0 y Linux

Resultados comerciales

- Protección más sólida contra los costos derivados de reparaciones y tiempo fuera de servicio provocados por incidentes de programas maliciosos.
- Protección antivirus para servidores y estaciones de trabajo Linux.
- Ahorros de tiempo del personal de TI mediante la administración desde una sola consola para la protección de los endpoints.
- Protección unificada contra virus y software espía.
- Prácticamente el spam no afecta a los usuarios, se reduce en más del 25% el correo entrante.
- Se ahorran más de 450 horas de personal al año que se dedican a eliminación de spam
- Cumplimiento de las normas de la ciudad.
- Recuperación completa inmediata de Symantec Multi-tier Protection.