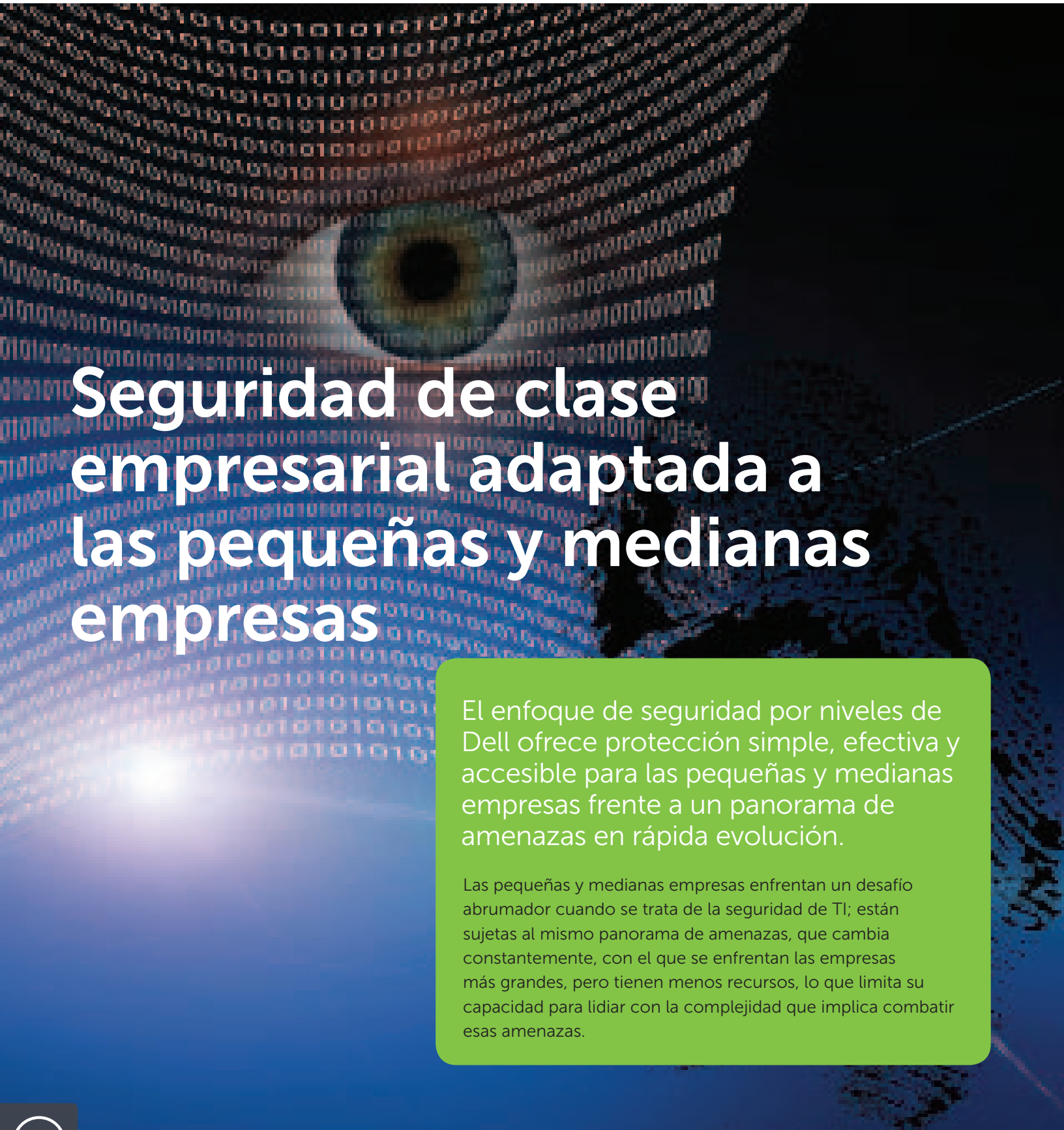


Seguridad de clase empresarial adaptada a las pequeñas y medianas empresas

El enfoque de seguridad por niveles de Dell ofrece protección simple, efectiva y accesible para las pequeñas y medianas empresas frente a un panorama de amenazas en rápida evolución.

Las pequeñas y medianas empresas enfrentan un desafío abrumador cuando se trata de la seguridad de TI; están sujetas al mismo panorama de amenazas, que cambia constantemente, con el que se enfrentan las empresas más grandes, pero tienen menos recursos, lo que limita su capacidad para lidiar con la complejidad que implica combatir esas amenazas.

"La seguridad no discrimina según el tamaño de las empresas", dice Jon Oltsik, analista principal, seguridad de la información de Enterprise Strategy Group. "Las pequeñas y medianas empresas se enfrentan con los mismos tipos de riesgos que las empresas más grandes pero no tienen la habilidad, el presupuesto ni el privilegio de contar con muchas contramedidas sofisticadas en la red". Lo que las pequeñas y medianas empresas necesitan, dice Oltsik, es un enfoque simple en cuanto a la provisión del tipo de estrategia de seguridad por niveles que durante mucho tiempo ha sido un tema principal en el ámbito empresarial.

Mediante un enfoque sobre la seguridad por niveles, también conocido como defensa en profundidad, se intenta proteger a las pequeñas y medianas empresas brindando protección en múltiples puntos de ataque posibles.

"Ninguna tecnología de seguridad brinda protección absoluta por sí sola. Las organizaciones que practican la defensa en profundidad evitan las amenazas y responden rápidamente cuando hay una intrusión", dice Jon Ramsey, director técnico de SecureWorks. "La defensa en profundidad significa más que simplemente tener la tecnología de seguridad adecuada; también significa contar con la experiencia para manejar esas tecnologías, monitorear sus alertas y responder rápidamente a las amenazas reales de manera adecuada".

Una estrategia de defensa en profundidad incluye específicamente medidas de protección en el perímetro de la red, en los puntos terminales como las computadoras y laptops y, para los usuarios individuales, asegurar que nadie pueda acceder a sus datos sin autorización. Y, como sugiere Ramsey, el enfoque incluye en muchos casos servicios para las pequeñas y medianas empresas que no tienen personal de TI suficiente que se dedique a solucionar problemas de seguridad o que simplemente optan por aprovechar la experiencia externa.

Tal enfoque permite a las empresas seguir el ritmo de la naturaleza cambiante de las amenazas brindando varios niveles de defensa. Pero hace tiempo que está fuera del alcance de las pequeñas y medianas empresas debido a que las herramientas necesarias son demasiado complejas y costosas, especialmente cuando se trata de brindar seguridad de red.

Dell Inc. aborda el problema asociándose con Juniper para ofrecer Dell J-SRX Services Gateways, que combina un conjunto de capacidades de seguridad de nivel empresarial integral en un dispositivo único que es fácil de implementar y administrar. La familia J-SRX agrega al conjunto de seguridad y servicio existente de Dell soluciones que abordan los otros tres componentes de un enfoque de seguridad por niveles, todos adaptados especialmente para cumplir con los requisitos de las pequeñas y medianas empresas.

Un panorama de seguridad complejo

La necesidad de un enfoque hacia la seguridad por niveles nunca ha sido mayor, dado el panorama de seguridad cambiante que siempre representa un desafío. Atrás quedaron los días en que los hackers buscaban notoriedad o entusiasmo; los intrusos de hoy buscan dinero.

"Las empresas son atacadas día tras día, las 24 horas, por criminales cibernéticos que están motivados por el dinero. Cada día, estos atacantes se vuelven más sofisticados y más organizados y este es el motivo por el cual su seguridad también necesita ser cada vez más fuerte", dice Hensley. "En el primer trimestre de 2010, SecureWorks vio un 45% más de vulnerabilidades que en el primer trimestre de 2009 y detectamos y mitigamos un promedio de más de 6000 eventos de seguridad por día".

Los datos del último informe "Symantec Global Internet Security Threat Report" respaldan esta contención. En el año 2009 el informe encontró que los códigos maliciosos aumentaban y Symantec detectó más de 2,8 millones de firmas de códigos maliciosos nuevas, hasta más del 50% de lo que había en el 2008. Los ataques informáticos también estaban aumentando y constituían el 60% de los incidentes de exposición de la identidad en el 2009 a partir del 22% del año anterior. En la mayoría de los casos (el 98%) las amenazas a la información confidencial incluían el acceso remoto a partir del 83% en el 2008.

El estudio realizado en el año 2009 "CSI Computer Crime and Security Study" describe un panorama parecido, con aumentos en la cantidad de encuestados que fueron víctimas de ciberataques como fraude financiero, malware, ataques de denegación de servicio, espía de contraseñas y deformación intencionada de sitios web (consulte el cuadro).

Las pequeñas y medianas empresas no pueden ser víctimas, dados los costos posibles relacionados con los ataques exitosos o la pérdida de datos. El costo promedio de la filtración de datos o de la pérdida de datos era de $6,75 millones en el año 2009, según una encuesta realizada por Ponemon Institute, que estableció el precio de $204 por registro comprometido.

Sin tener en cuenta los costos financieros, una sola filtración puede ocasionar daños a largo plazo a la reputación de una empresa. Además, las pequeñas y medianas empresas se encuentran bajo la misma presión que sus contrapartes empresariales para cumplir con las distintas regulaciones, que los obliga a proporcionar seguridad adecuada como GLBA, HIPAA, estándares de seguridad de datos PCI y la Ley Sarbanes-Oxley.

El enfoque hacia la seguridad por niveles, también conocido como defensa en profundidad, está diseñado para proteger a las pequeñas y medianas empresas, brindándoles protección en múltiples puntos de ataque posibles.

Definición de la seguridad por niveles

La seguridad por niveles está diseñada para simplificar la seguridad y ayudar a las pequeñas y medianas empresas a lidiar con el aumento de la sofisticación y de la cantidad de amenazas. Divide la seguridad en tres niveles distintos e incluye servicios para brindar experiencia y monitoreo de seguridad activo las 24 horas, todos los días.

Mediante la división de la seguridad en estas tecnologías individuales, las pequeñas y medianas empresas pueden visualizar y comprender las capacidades de cada nivel y, cuando se aborda cada una, se puede construir una estrategia de seguridad superpuesta integral y simplificada.

I. Seguridad de red

La seguridad de red es la primera línea de defensa ya que la mayoría de los atacantes ingresan por medio de una red y, eventualmente, todos alcanzan la red en cierto punto. Una estrategia de seguridad de red completa incluiría varias tecnologías diferentes, incluidos los firewalls, las redes privadas virtuales, el escaneo antivirus, el filtrado de contenido web y antispam y los sistemas de detección/prevención de intrusiones para proteger las redes de las pequeñas y medianas empresas de los ataques de correos electrónicos y originados en la Web realizados por los criminales cibernéticos.

Antes, las empresas necesitaban instalar, configurar y ajustar los productos separados continuamente para llevar a cabo cada una de estas funciones de seguridad, creando un nivel de complejidad que la mayoría de las pequeñas y medianas empresas no podían alcanzar. Hoy, los proveedores están consolidando algunas o todas estas funciones en un único dispositivo de seguridad de red que está diseñado para que sea fácil de instalar y operar, haciendo realidad la seguridad de red adecuada para las pequeñas y medianas empresas.

II. Seguridad Endpoint

La seguridad Endpoint está diseñada para proteger a las computadoras y laptops de las amenazas que no ingresan mediante la red segura y para permitir a los administradores de TI asegurar los puntos terminales y evaluar las vulnerabilidades. Dell se ha asociado con Trend Micro, que ofrece software de seguridad para la protección contra virus, spam y malware, así como el filtro de contenido y las URL.

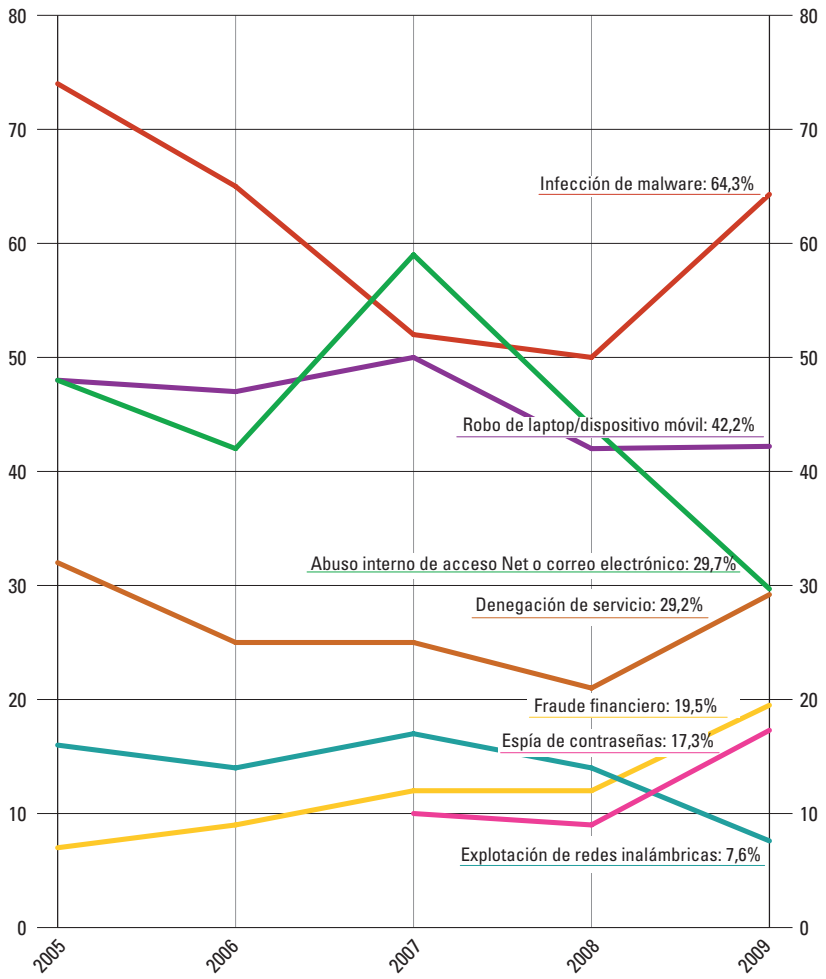
Fuera del software de seguridad tradicional, Dell depende de KACE para brindar una solución de seguridad completa que permite que TI evalúe los puntos terminales en busca de vulnerabilidades, implemente parches de seguridad, bloquee y elimine aplicaciones e incluso bloquee las computadoras para que solo un administrador pueda realizar cambios. Teniendo en cuenta que la mayoría de las amenazas se realizan a través de Internet, KACE y Dell han anunciado un navegador seguro que aísla el navegador web del usuario, evitando que el contenido malicioso que el usuario descarga infecte el resto de la máquina.

III. Seguridad del usuario

Las estrategias de seguridad son el eslabón más débil de la cadena de protección y la seguridad del usuario se trata específicamente de controlar el acceso a los datos del usuario. Dell se ha asociado con Credant para ofrecer una solución de cifrado de un toque simple que elimina las suposiciones de la conformidad y realiza el cifrado de datos en el almacenamiento interno y externo. El cifrado puede proteger los datos en el caso de que se produzca un robo, pero solo si se resguarda el acceso al punto terminal con políticas de autenticación sólidas.

Tipos de ataques experimentados

por porcentaje de encuestados



Encuesta 2009 CSI Computer Crime and Security Survey

2009: 185 encuestados

Dell J-SRX combina todas las tecnologías necesarias para la seguridad de red por niveles incluido un firewall que es el mejor de su clase, VPN, IPS y antispam, antivirus y tecnología de filtrado web.

Servicios

Las empresas de todos los tamaños pueden mejorar su posición ante la seguridad y disminuir los costos de TI descargando el monitoreo de seguridad, la administración y las correcciones diarios en un proveedor de servicios y socio confiable. Al trabajar como una extensión del personal de TI del cliente, Dell, en asociación con SecureWorks, ofrecerá una gama de servicios de seguridad potentes que incluye monitoreo de seguridad las 24 horas del día, todos los días, monitoreo y administración de firewalls y dispositivos IPS/IDS, prueba de penetración y escaneo de aplicaciones web.

Al implementar estos servicios, los clientes de Dell no solo mejorarán su posición ante la seguridad sino que también ayudarán a facilitar el cumplimiento con las regulaciones que evolucionan constantemente, como GLBA, HIPAA, NERC/CIP, PCI, Sarbanes-Oxley y muchos otros mandatos regulatorios.

El enfoque de Dell

Dell reconoce que para enfrentar todas estas amenazas de seguridad se necesitan muchos niveles de protección ya que ninguna tecnología de seguridad simple puede brindar protección ante todas las formas de ataque. Al mismo tiempo, la solución debe adaptarse al entorno de las pequeñas y medianas empresas: simple para instalar y fácil de usar, así como accesible.

El servicio y la simplicidad de Dell, el rendimiento y la seguridad sólida de Juniper

Dell J-SRX Services Gateways es el último ejemplo de cómo Dell está cumpliendo esa premisa. J-SRX está basado en tecnología desarrollada por Juniper para sus clientes empresariales y Dell la entrega en un factor de forma de dispositivo integrado que es simple y conveniente para los clientes de las pequeñas y medianas empresas y sucursales.

"Históricamente, J-SRX estaba fuera de alcance para las pequeñas y medianas empresas porque Juniper lo colocaba en un extremo elevado del mercado", dice Oltsik. "Sin embargo, al trabajar con Dell, Juniper está sacando de la caja todas las cosas buenas, incluido el rendimiento, y está llevándolo al mercado. Es una buena combinación de la experiencia de Dell de entregar productos simples y efectivos al mercado medio y los golpes de tecnología de Juniper".

Dell J-SRX combina todas las tecnologías necesarias para la seguridad de red por nivel, incluido el mejor firewall de su clase, VPN, IPS y la tecnología antispam, antivirus y filtrado web; todas probadas por los clientes empresariales de Juniper. Las capacidades de seguridad avanzadas de J-SRX ofrecen protección de aplicaciones y de red integral que evita que una amplia gama de amenazas de seguridad como gusanos, virus, troyanos, spyware y demás malware entre en la red.

Se entrega por medio de un dispositivo integrado simple que también ofrece enrutamiento y conmutación de alto rendimiento, con procesamiento dedicado para evitar los cuellos de botella, permitiendo que las pequeñas y medianas empresas cambien sus dispositivos firewall/VPN heredados por un dispositivo mucho más funcional, de costo y complejidad reducidos.

Tal como sugiere Oltsik, J-SRX fue diseñado pensando en las pequeñas y medianas empresas. Incluye asistentes y una interfaz web que facilita su configuración e implementación. Su firewall basado en zonas hace que la creación de políticas para aislar invitados, redes inalámbricas, computadoras de escritorio, servidores o bases de datos sea simple. También viene en tres versiones y permite que las pequeñas y medianas empresas elijan entre los modelos, desde el que le sea conveniente para sus sitios más pequeños hasta el que cuenta con 16 puertos Gigabit Ethernet y rendimiento de firewall hasta de 1,5 Gbps; todo a un precio adecuado para las pequeñas y medianas empresas.

Conclusión

Con su enfoque de varios niveles de seguridad creado pensando en las pequeñas y medianas empresas, Dell está simplificando drásticamente lo que una vez fue un desafío complejo: brindar seguridad de nivel empresarial a las pequeñas y medianas empresas.

Con el agregado de Dell J-SRX Services Gateways, la línea de Dell incluye todos los componentes principales de una estrategia de seguridad por niveles firme. Pero debido a la naturaleza cambiante del panorama de la amenaza, Dell agregará de manera continua a su gama de servicios de seguridad para abordar los requisitos adicionales de las pequeñas y medianas empresas. Por ejemplo, Dell está expandiendo su sociedad con Juniper para brindar soluciones de seguridad de red integradas e integrales que protejan las redes de las pequeñas y medianas empresas ante gusanos, troyanos y las amenazas de seguridad que surgirán.

Dell, en reconocimiento de que es difícil para las pequeñas y medianas empresas mantenerse al tanto sobre la volatilidad de la seguridad, ha desarrollado una arquitectura directa que les facilita garantizar que todas sus bases de seguridad estén cubiertas. Ya sea que una pequeña o mediana empresa opte por implementar las soluciones de Dell por su cuenta o decida aprovechar los servicios de seguridad de Dell, puede descansar teniendo la certeza de que obtiene seguridad de nivel empresarial a un nivel de simplicidad y precio creados pensando en las pequeñas y medianas empresas.

Haga clic aquí para leer más acerca de **las soluciones de seguridad por niveles de Dell.**