DOCUMENTOS SiC
Nº 21
JUNIO 2016

Ciberseguridad para la transformación digital

ENTREVISTA

Karen Gaines
Directora General de HPE Security Services para Iberia

Servicios profesionales:

- Diagnósticos de CMR
- Simulación avanzada de ataques
- Diagnóstico de cuentas privilegiadas

Evolución de amenazas y escenarios:

- Cyber Risk Report 2016
- Securing Internet of Things

HPE Diagnostics, servicios avanzados de evaluación del estado de seguridad de la información

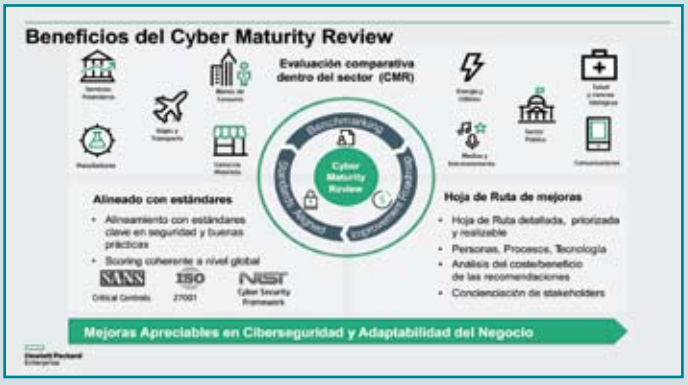
Con departamentos especializados en aspectos tan cruciales como la seguridad de información, HPE Security Services dispone de una oferta de servicios de consultoría muy extensa y de extremo-a-extremo, de soporte de TI para diseñar, implementar y optimizar los activos tecnológicos de cualquier tipo de proyecto que una organización pueda demandar, sea cual sea su sector de actividad. Además, la multinacional, también puntera en esta área, ha lanzado una serie de servicios para determinar su estado en las diferentes áreas de su seguridad. A través de los servicios de "Diagnostics", HPE Security Services evalúa el estado de la seguridad de sus clientes convirtiéndose en un partner de confianza para evolucionar la ciberdefensa de cualquier organización.

De esta manera, HPE Security Services completa su oferta de consultoría TI con servicios y soluciones de ciberseguridad, que permiten contar con un enfoque totalmente integral de cualquier proyecto. La cartera de HPE Security Services se compone de siete servicios de consultoría interconectados, creados sobre un enfoque común que cubre todo el ciclo de vida para la entrega de servicios de seguridad de la información de forma eficiente y eficaz como parte de un trabajo conjunto con el cliente, proporcionando soluciones a medida. El desarrollo de los servicios "Diagnostics" de HPE Security Services completan esta extensa oferta acercándose aún más a los requerimientos de sus clientes en seguridad de la información, evaluando y proporcionando un diagnóstico detallado y real de sus capacidades de ciberseguridad. La oferta "Diagnostics" la conforman, principalmente, los servicios de análisis de madurez de seguridad cibernética, servicios de simulación avanzada de ataques, diagnósticos de seguridad de cuentas privilegiadas, así como servicios de evaluación del compromiso.

Para ello, HPE Security Services dispone de un equipo de expertos formado por 3.000 profesionales en todo el mundo con una gran experiencia práctica que se adapta a las peculiaridades de las diferentes industrias, y que han dado servicios a más de 10.000 clientes, han protegido más un millón de aplicaciones con 2,6 billones de líneas de código, han gestionado más de 500.000 dispositivos de seguridad y han detectado y puesto en cuarentena más de 45 millones de software malicioso.

Diagnósticos de CMR (revisión de cibermadurez)

La diversificación de la naturaleza y la motivación de los delincuentes cibernéticos, el complejo entorno regulativo actual que ejercen las recientes modificaciones normativas y los cambios en la entrega y consumo de servicios TI provocada por la transformación digital, están generando una gran preocupación en torno a la seguridad de la información y la protección de activos digitales en las organizaciones. Ante esta situación, HPE ha creado un servicio capaz de determinar el grado de madurez en materia de ciberseguridad de una organización, adaptándose a sus necesidades y ayudando al cliente a detectar y responder a los fallos de seguridad más críticos y a gestionar el riesgo ante incidentes, en base a tres objetivos principales:

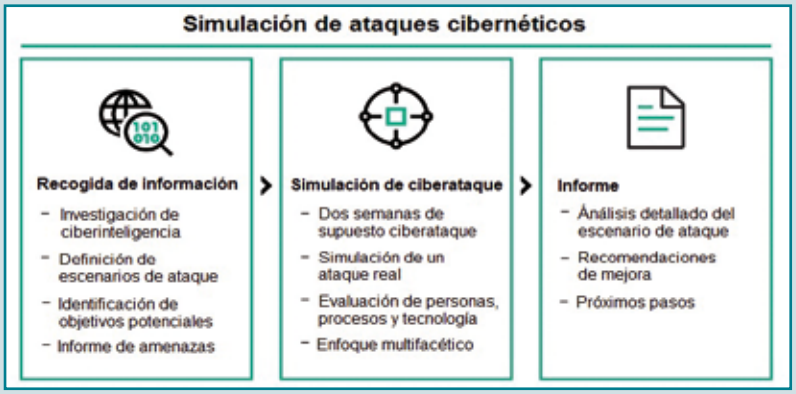


- **Evaluación de controles y procesos de seguridad**: entre los que se incluyen estándares, normas y certificaciones como SANS, NIST, ISO 27001, así como CMMI, entre otras.
- **Definición de una hoja de ruta de mejoras**: donde se procede a la identificación de áreas de mejora tanto técnicas como organizativas, a la evaluación de las prioridades y a la constitución de "Quick Wins".
- **Establecimiento de un marco de trabajo**: a través del desarrollo de objetivos de mejora, trazabilidad de avances y madurez en ciberseguridad.

Para la consecución de estos objetivos, HPE realiza una serie de entrevistas y revisiones personalizadas en las que evalúa las capacidades de gestión de vulnerabilidades, detección de anomalías, mitigación de incidentes, captura de datos, así como el nivel de conciencia de la situación. En según lugar, lleva a cabo un proceso de análisis cualitativo de resultados, estableciendo una puntuación según los niveles de madurez CMMI, y una identificación y priorización de las deficiencias clave. Por último, se entrega al cliente un informe detallado de los resultados del servicio diferenciando tres áreas clave: las personas, los procesos y la tecnología.

Simulación avanzada de ataques cibernéticos

Las ciberamenazas son cada día más difíciles de evitar y aunque algunas organizaciones están centradas en el despliegue de medidas de seguridad, éstas son insuficientes sin una sólida apuesta por la adopción de servicios especializados que mejoren la resiliencia y evalúen las verdaderas capacidades de detección y respuesta de una organización. A través de Cyber Attack Simulation, HPE ofrece un servicio avanzado de simulación de ciberataques es un escenario real, emulando herramientas, técnicas y procedimientos existentes para llevar a cabo de manera realista un ataque cibernético en la organización en el cual, los sistemas de inteligencia de HPE proceden a evaluar los diferentes actores en juego, tanto personas y procesos, como tecnologías.



En este servicio, HPE procede a la identificación de los activos críticos vulnerables y de los sistemas de ciberdefensa más ineficaces y a la validación de las capacidades de detección y respuesta a través de cinco fases:

- **Investigación:** realizando un exhaustivo análisis mediante sus sistemas de inteligencia de amenazas, centrándose en aquello que podría ser potencialmente atacado y evaluando las capacidades técnicas de seguridad perimetral de la organización.
- **Infiltración:** aplicando herramientas, técnicas y procedimientos reales haciendo *payloads* de ataques dirigidos.
- **Descubrimiento.** HPE realiza movimientos dentro de la red, burla los sistemas de protección internos, escala privilegios y descubre potenciales objetivos de alta criticidad.
- **Captura:** HPE consolida el acceso a los datos objetivo.
- **Exfiltración:** HPE extrae los datos objetivo.

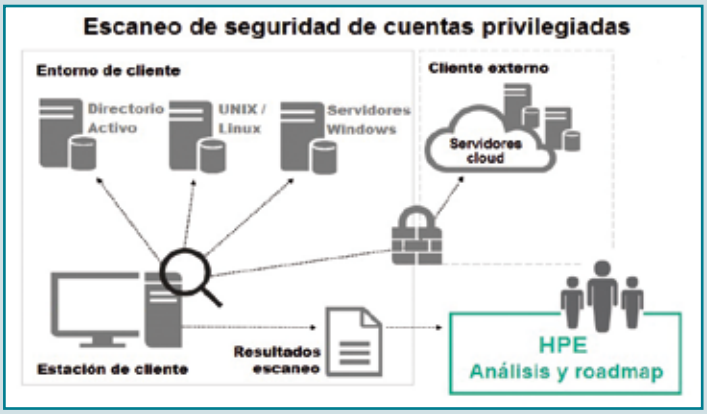
Posteriormente, la compañía procede a la creación de un informe detallado sobre el nivel de resiliencia a los ataques cibernéticos de la organización y ofrece recomendaciones, que proporcionan competencias de seguridad completas.

Diagnóstico de seguridad de cuentas privilegiadas

Una gestión incorrecta de las identidades privilegiadas puede poner a cualquier organización en peligro. Esta vulnerabilidad podría causar potencialmente enormes pérdidas financieras y perjudicar muy seriamente la reputación de las empresas. En 2015, el 100% de las violaciones de las cuentas privilegiadas dio lugar a la pérdida de datos y el coste de cada brecha de seguridad alcanzó los 174 dólares –alrededor de 157 euros–.

En 2017 se prevé que se produzca un incremento del 40% de las multas a las organizaciones con un ineficiente sistema de control de cuentas privilegiadas.

El servicio de seguridad de cuentas privilegiadas de HPE permite a las organizaciones identificar el riesgo potencial mediante el descubrimiento de cuentas y credenciales privilegiadas y su estado, comprensión de las vulnerabilidades específicas en escaladas de privilegios y las cuentas comprometidas, y la ejecución y entrega de un plan de trabajo de los pasos a seguir que abordan la visibilidad, y la gestión y el control de las cuentas con privilegios.



Como parte de este servicio HPE ofrece:

- **Evaluación cuantitativa y cualitativa**, a través de un escaneo completo del directorio de las cuentas con privilegios, compartidas y genéricas, en estaciones de trabajo y servidores sin necesidad de instalar software o hardware en la red.
- **Recogida de datos detallados y cuantificables,** utilizados para presentar una "única versión de la verdad" de las vulnerabilidades de las cuentas privilegiadas, contraseñas, SSH y Pass-the-Hass de los dispositivos explorados de la organización.

El servicio de diagnóstico de seguridad de cuentas privilegiadas de HPE permite así aplicar visibilidad a las cuentas con privilegios existentes, quién tiene acceso a ellas, gestionar y administrar las credenciales, y controlar las actividades que se derivan de las cuentas privilegiadas, así como conocer y entender todo el conjunto de controles y satisfacer los requisitos de cumplimiento (por ejemplo, SOX y PCI DSS).

Karen Gaines Cordero

Directora General de HP Enterprise Security Services para Iberia

Karen Gaines, Licenciada en Ciencias por la Universidad Internacional de Florida y MBA por la Escuela Europea de Negocios, fichó por HPE en 2013, responsabilizándose de las líneas de servicios de ciberseguridad de la compañía en Iberia. Hoy, tres años después, esta experta y su equipo están obteniendo unos resultados envidiables en el mercado especializado.

"Tenemos la capacidad de adaptar de modo granular los servicios de ciberseguridad a los requisitos de nuestros clientes"

– ¿Está respondiendo positivamente la demanda española de ciberseguridad empresarial a la oferta de servicios de HPE?

– Definitivamente sí. HPE ha sido capaz de captar el interés del cliente español en materia de ciberseguridad gracias a un claro enfoque de adaptación granular a las necesidades reales del negocio y a su casuística concreta. Un indicador es el rápido crecimiento de nuestro equipo Advisory, debido al aumento de la demanda de nuestros servicios Diagnostics. Se ve claramente que los clientes requieren de un socio de confianza para guiarles en la ciberdefensa.

Otra muestra de nuestro éxito es el rápido incremento del número de clientes a los que prestamos servicio desde nuestro Centro de Competencia de Seguridad.

– ¿Qué tipo de proyectos han realizado en el 2015 y en lo que llevamos de 2016?

"HPE lleva más de 40 años prestando servicios de seguridad gestionada y más de 20 años con la función de consultoría de seguridad establecida. Hace aproximadamente tres años decidió realizar una inversión importante en España, potenciando el equipo local, que ha ido doblando su crecimiento desde entonces"

– Nos sentimos muy orgullosos de estar desarrollando y expandiendo nuestra actividad en todas las prácticas dentro del área de seguridad, como son: 1) Estrategia de Seguridad y Gestión de Riesgos, 2) Inteligencia de Seguridad y Gestión de Incidentes. 3) Gestión de Amenazas y Vulnerabilidades, 4) Seguridad en Infraestructura y Redes, 5) Protección de Datos y Privacidad, 6) Gestión de Identidades y Accesos y 7) Seguridad en Aplicaciones.

– ¿Cuántas personas iniciaron bajo su dirección los servicios de HPE Security Services y cuántas forman parte hoy de su equipo?

– Hewlett Packard Enterprise lleva más de 40 años prestando servicios de seguridad gestionada y más de 20 años con una consultoría de seguridad establecida. Hace aproximadamente 3 años Enterprise Services decidió realizar una inversión importante en España, potenciando el equipo local. El equipo de Enterprise Services de Seguridad en España, ha doblado su crecimiento cada año. Creemos que nuestro equipo está cada vez más consolidado y que tiene un *expertise* al que pocos pueden aspirar; contamos con especialistas en cada una de las áreas, permitiendo ofrecer resultados excepcionales para todos nuestros clientes y que nos vean como el socio de su transformación en materia de seguridad.

– HPE es un tradicional proveedor de servicios de ciberseguridad para las estructuras de la Defensa de EE.UU. ¿Han tenido contactos con las estructuras españolas en la materia?

– La casuística en el ámbito de Defensa entre EEUU y España es muy diferente. Localmente, hemos participado en varios eventos en los que había representación de Defensa y HPE, y estamos muy interesados en incrementar nuestra relación con el MCCD.

– ¿En qué direcciones están evolucionando el portafolio de servicios de HPE Security Services?

– Nuestros servicios están orientados a aportar el máximo valor para cada cliente concreto. Esto se traduce en un enfoque de Advisory para la consultoría, y en unos servicios gestionados totalmente adaptados al negocio, siempre aportando nuestro *expertise* en el ámbito tecnológico de la seguridad, ya sea con soluciones muy consolidadas o innovando con las nuevas tendencias.

– Una última cuestión: ¿disponen HPE Security Services de servicios específicos para dar soporte a compañías privadas del sector industrial?

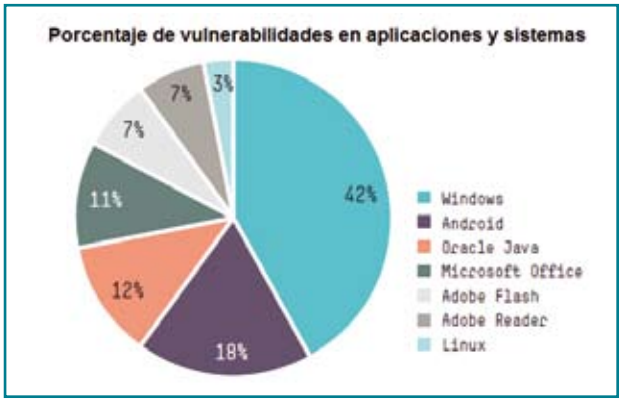
– En HPE Security Services identificamos dos áreas de servicios principales para el sector industrial, SCADA, que ya es un requerimiento actual de nuestros clientes, e IoT, que es nuestra apuesta por la innovación. Con estos dos servicios estamos seguros que podremos ofrecer los resultados que las organizaciones necesitan para su negocio. ●

La vulnerabilidad de aplicaciones, los parches y la monetización del *malware* representan los principales riesgos para las empresas

HPE ha dado a conocer recientemente el denominado "Cyber Risk Report 2016", un informe que recoge de forma esclarecedora toda la información vinculada al panorama de amenazas que afectaron a las empresas a lo largo del pasado año 2015, así como los recursos que pueden ayudar a minimizar los riesgos de seguridad.

El intenso trabajo realizado por el equipo de HPE confirma un aumento significativo de los ataques directos a aplicaciones móviles que, en la actualidad, se están convirtiendo en la ruta más fácil para acceder a los datos más sensibles de las empresas. En este sentido, el informe señala que el 75% de las aplicaciones móviles analizadas presenta al menos una vulnerabilidad de seguridad crítica o de alta severidad, en comparación con el 35% del resto de aplicaciones.

La explotación de vulnerabilidades en el software también sigue siendo un vector primario para el ataque y las explotaciones móviles ganan terreno. Al igual que en 2014, las diez principales vulnerabilidades explotadas en 2015 tenían más de un año, con un 68% con tres años o más. En 2015, Microsoft Windows fue la plataforma de software más atacada, con el 42% de las 20 principales vulnerabilidades descubiertas.



El 75% de las aplicaciones móviles analizadas presenta al menos una vulnerabilidad de seguridad crítica o de alta severidad.

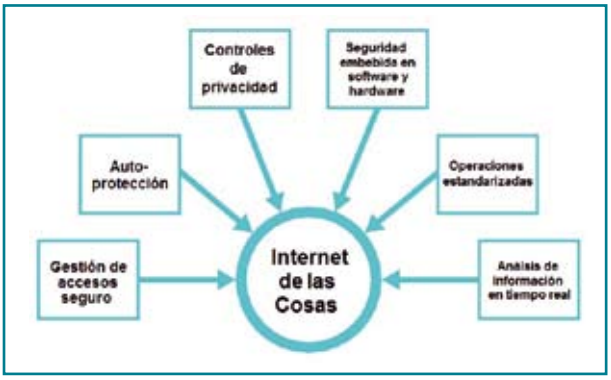
Por otro lado, el *malware* ha asumido un nuevo enfoque, dejando de ser simplemente perjudicial a convertirse en una actividad generadora de ingresos para los atacantes, desarrollándose cada vez más *ransomware* y caballos de Troya bancarios.

HPE recomienda a las empresas defender no sólo el perímetro sino también las interacciones entre usuarios, las aplicaciones y los datos independientemente de la ubicación o el dispositivo. Las organizaciones han de vigilar mejor la aplicación de parches, tanto en la empresa como en el nivel del usuario. Asimismo, la mejor protección contra el *ransomware* es una política de copia de seguridad consecuente con la importancia de los archivos de los sistemas.

Control de accesos, privacidad y seguridad embebida, las claves para reforzar la protección de los dispositivos IoT

La rápida expansión de dispositivos conectados ofrece nuevas formas de comunicarse, nuevos modelos de negocio y una mayor visibilidad de los procesos existentes; pero los enormes volúmenes de datos de los dispositivos IoT deben protegerse de robo, modificación y explotación desde el momento de su creación.

En su estudio "Securing the Internet of Things", HPE explora la seguridad y privacidad en un mundo interconectado, identificando una serie de aspectos fundamentales en materia de seguridad que las organizaciones deben de tener en cuenta en su proceso de adopción del IoT.



Los dispositivos IoT deben protegerse de robo, modificación y explotación desde el momento de su creación.

• **Seguridad en la gestión de accesos**. Todos los componentes del ecosistema del IoT deben estar identificados y gestionados con sistemas avanzados de identificación, autenticación y autorización.

• **Autoprotección.** Los dispositivos IoT carecen de un perímetro definido por lo que será de vital importancia crear mecanismos de protección que proporcionen seguridad a nivel de dispositivo.

• **Controles de privacidad.** Dado que los datos se generarán en cantidades cada vez mayores y se localizarán en cualquier parte, es imperativo que la seguridad y la privacidad sean directamente proporcionadas en toda la cadena –sensores, dispositivos e intermediarios– así como en cada transacción y comunicación del mismo.

• **Seguridad embebida**. La seguridad necesitará ser integrada en cada capa que conforma tanto el hardware como el software del dispositivo IoT.

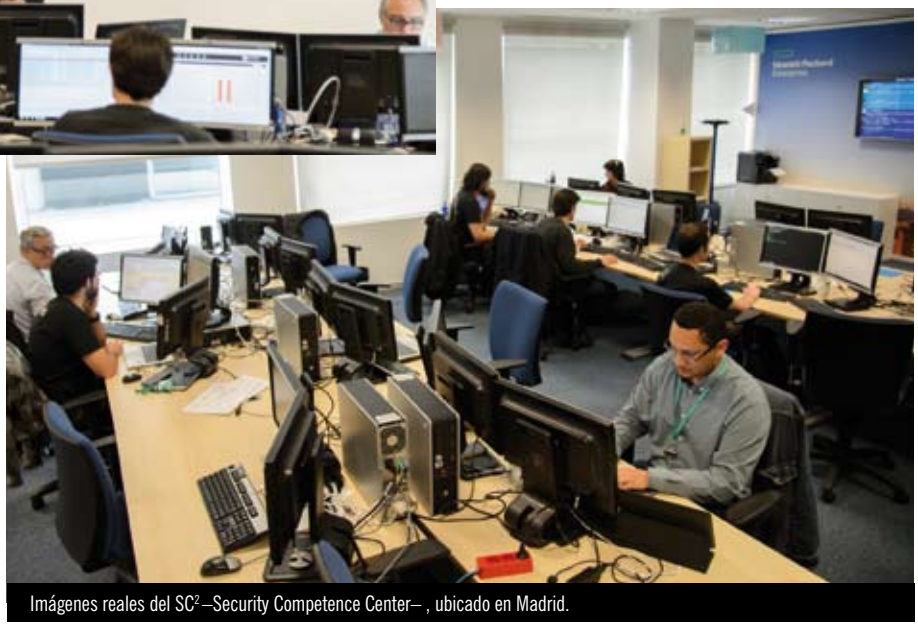
• **Operaciones estandarizadas**. Los dispositivos IoT también necesitarán procesos de gestión ITIL estandarizados para operar con eficacia y seguridad. Los procesos deben incluir inventario, gestión de seguridad, monitorización y actualizaciones.

• **Procesos de información en tiempo real.** El análisis de información en los dispositivos IoT tendrá que ser predictivo, proactivo y en tiempo real para aumentar su resiliencia y contar con una rápida capacidad de recuperación.

HPE SC², el valor de la gestión ininterrumpida de la seguridad de la información

La demanda de servicios de gestión externalizada de la seguridad de la información lleva creciendo a un ritmo muy elevado en los últimos años, considerándose en la actualidad como un complemento equilibrado, eficaz y eficiente en los procesos de seguridad de la información de grupos empresariales de todo tipo.

Correspondiendo a la demanda de las organizaciones, HPE dispone de un Centro de Gestión de Seguridad –SC²– destinado a la prestación de servicios gestionados de seguridad y ubicado en Madrid. HPE Security Services tienen un objetivo claro: conseguir el mayor grado de satisfacción del cliente a través de la personalización de los servicios ofertados.



Imágenes reales del SC²–Security Competence Center– , ubicado en Madrid.

Servicios personalizados

Los principales servicios que se ofrecen desde SC² corresponden a los más demandados por los clientes, aunque, como gran valor añadido HPE Security Services realiza una personalización muy granular de los servicios ofertados para cada organización. Esto supone que se puede estudiar la prestación de casi cualquier servicio de ciberseguridad requerido por el cliente en el Security Competence Center de Madrid. Además, HPE Security Services es una firma agnóstica en la prescripción de tecnología, lo cual implica, a su vez, que ninguno de los servicios que se ofrecen está limitado por el fabricante tecnológico.

Tipologías de servicios

- Monitorización y gestión de alertas de seguridad (SIEM).
- Consolidación y retención de *logs* (SEM).
- Gestión de identidades.
- Gestión de identidades privilegiadas.
- Seguridad en aplicaciones (análisis de código en aplicaciones).
- Gestión de vulnerabilidades.
- Administración de elementos de seguridad: WAF, DLP, IDS/ IPS, Next Gen FW, Proxy, *endpoint*…
- Protección contra APT.
- Protección anti-DDoS.
- Vigilancia digital.
- Auditorías recurrentes de seguridad (*ethical hacking*).
- Respuesta a incidentes.
- Análisis forense.

HPE Security Services realiza una personalización granular para cada cliente, lo que supone que se puede estudiar la inclusión de casi cualquier servicio de ciberseguridad demandado en el Security Competence Center de Madrid.

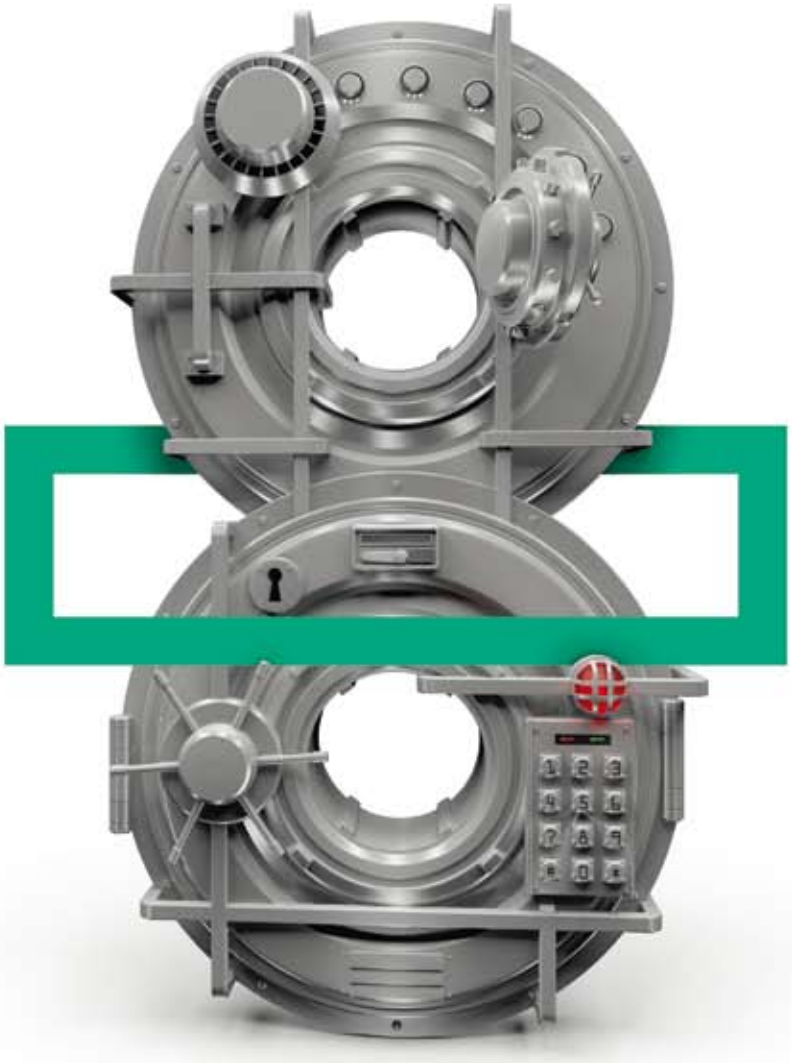
Equipo humano cualificado

El equipo humano del SC² está formado por profesionales especializados en las distintas áreas de seguridad de la información, y sus miembros poseen conocimientos avalados por certificaciones profesionales, permitiendo dar un servicio global y efectivo.

Tanto la ubicación como la dedicación de los especialistas de HPE Security Services con respecto al cliente se conforman en torno a tres modalidades de prestación de servicios:

– **Local**: especialistas dedicados y ubicados *on site* para un único cliente.
– **Híbrido**: parte de los especialistas dedicados y ubicados en la sede del cliente y parte del servicio prestado en remoto desde el SC².
– **Remoto**: todo el servicio es prestado en remoto desde el SC².

Accelerating protection



Hewlett Packard Enterprise security products and solutions help protect 8 of the top 10 Fortune Global 500 companies.

Accelerating next

Hewlett Packard Enterprise

hpe.com/protection

Source: Fortune Global 2015; HPE Customers 2013 Q3 – 2015 Q2.