Creado por:
Pedro Palandrani
Analista investigador

Fecha: 2 de febrero de 2021
Tema: Temática

INVESTIGACIÓN DE GLOBAL X ETF

Cuatro empresas que lideran el auge de la ciberseguridad

Hoy en día, probablemente sea solo una cuestión de tiempo para que una empresa deba hacer frente a un evento cibernético de gran magnitud. A la empresa de gestión de software SolarWinds le llegó ese momento en diciembre de 2020. En lo que algunos describen como el ciberataque más grande de la historia de los EE. UU., los perpetradores introdujeron una vulnerabilidad en el software Orion de la empresa que podría llegar a permitir a un atacante poner en peligro el servidor en el que se ejecuta el software. Lo más aterrador es que el ataque golpeó a las principales agencias y organizaciones federales, poniendo quizá en peligro la seguridad nacional. Las primeras estimaciones indican que aproximadamente 250 organizaciones se vieron afectadas.

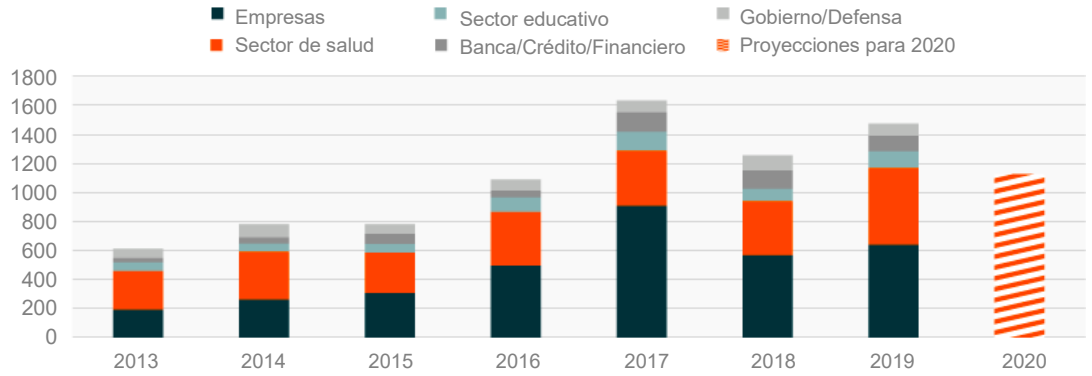
Los eventos de ciberamenazas en los EE. UU. y en todo el mundo son cada vez más generalizados y sofisticados. Se prevé que la tendencia ascendente en el número de ciberataques aumente el gasto en seguridad mundial de aproximadamente 125 000 millones de dólares en 2020 a 175 000 millones de dólares para 2024.[1] La creciente migración hacia la nube está acelerando este crecimiento. Actualmente, solo un tercio de la cantidad total del trabajo utiliza tecnología de informática en la nube. A medida que aumenta ese número, se necesitará más gasto en ciberseguridad para ayudar a prevenir ataques maliciosos.[2] De forma similar, la rápida adopción de más dispositivos habilitados para Internet también crea nuevos objetivos para los hackers que desean robar o rescatar datos valiosos.

En este artículo, destacamos cuatro empresas que son actores clave en el tema de la ciberseguridad:

- CrowdStrike: Una plataforma líder en la protección de los puntos de conexión
- Zscaler: Una plataforma nativa en la nube que ofrece puertas de enlace de web seguras
- Okta: Un actor clave en el segmento de la administración de identidad y acceso
- Mimecast: Uno de los principales proveedores de soluciones que detectan y bloquean correos electrónicos maliciosos

Se prevé que más de 380 millones de personas vieron sus datos comprometidos en 2020[3]

NÚMERO DE FILTRACIONES DE DATOS EN LOS EE. UU.
Fuente: Identity Theft Resource Center, 2020.



CrowdStrike: Una plataforma líder en la protección de los puntos de conexión

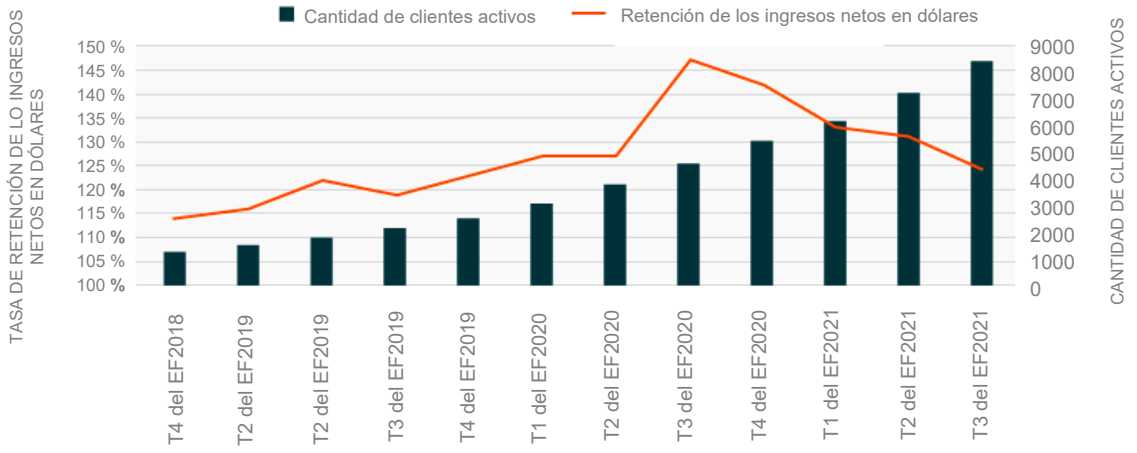
CrowdStrike es una de las principales empresas de ciberseguridad en plataformas de protección de los puntos de conexión (endpoint protection platforms, EPP), que ayuda a los clientes a proteger los dispositivos del usuario final como dispositivos móviles, computadoras portátiles y servidores. La solución de CrowdStrike es un software como servicio (software-as-a-service, SaaS) que trabaja continuamente para detectar y analizar amenazas. La solución es una arquitectura 100 % basada en la nube, que proporciona a CrowdStrike una ventaja competitiva frente a los softwares anteriores no en la nube. La empresa puede configurar su solución de forma rápida y eficaz en muchos entornos de TI diferentes. Por ejemplo, en el año fiscal del cuarto trimestre de 2020 de la empresa, la empresa incorporó a Target como nuevo cliente en apenas 10 días.

En el pasado, el software antivirus local evitaba los ciberataques mediante el control y el análisis de amenazas conocidas en archivos de punto de conexión. Pero esa capa de seguridad es en gran medida reactiva. Las mejores ofertas actuales aprovechan la inteligencia artificial (IA) La oferta de IA de CrowdStrike se llama Threat Graph, el cerebro detrás de las soluciones de ciberseguridad habilitadas para IA de la empresa. El gráfico de amenazas puede ayudar a CrowdStrike a gestionar 4 billones de eventos cibernéticos por semana y tomar 50 millones de decisiones por minuto.[4] Los conjuntos de datos se procesan en la nube de CrowdStrike, creando un efecto de red donde, cuanto más datos se analizan entre los clientes, mejor es la tecnología de IA de Threat Graph.

Las soluciones basadas en la nube pueden traducirse en sólidos ingresos constantes. A partir del cuarto trimestre del ejercicio fiscal (EF) 2020, el 92 % de los ingresos totales de CrowdStrike provino de sus suscripciones.[5] También es destacable que CrowdStrike haya mantenido una tasa de retención de ingresos netos en dólares superior al 120 % desde el primer trimestre de EF2019.[6] Una tasa superior al 100 % significa la base de clientes existente tiene un crecimiento neto, ya sea a través de aumentos de precios o de oportunidades de ventas adicionales.

TASA DE RETENCIÓN DE LOS INGRESOS NETOS EN DÓLARES (IZQ.) Y CLIENTES ACTIVOS (DER.) DE CROWDSTRIKE

Fuente: ETF de Global X, CrowdStrike Company Filings.



Zscaler: Una de las principales empresas en materia de puertas de enlace web seguras

Zscaler es otra plataforma de ciberseguridad 100 % basada en la nube, por lo que no hay que comprar ni administrar ningún hardware, y la plataforma siempre está actualizada. Zscaler realiza 175 000 actualizaciones de seguridad en la nube por día.[7] Las soluciones de puertas de enlace de web seguras (Secure Web Gateways, SGW) de Zscaler se centran principalmente en proporcionar a los clientes acceso seguro a aplicaciones administradas internamente, como correos electrónicos corporativos, a través de su acceso privado de Zscaler (Zsclar Private Access, ZPA). También proporcionan soluciones para

aplicaciones externas, como el software de gestión de relaciones con el cliente (customer relationship management, CRM), a través del acceso a Internet de Zscaler (Zscaler Internet Access, ZIA). Una puerta de enlace web segura evita que el tráfico no seguro entre en una red interna a través de aplicaciones web externas. Zscaler es como un intermediario, que conecta a los usuarios directamente a las aplicaciones sin pasar por su red.

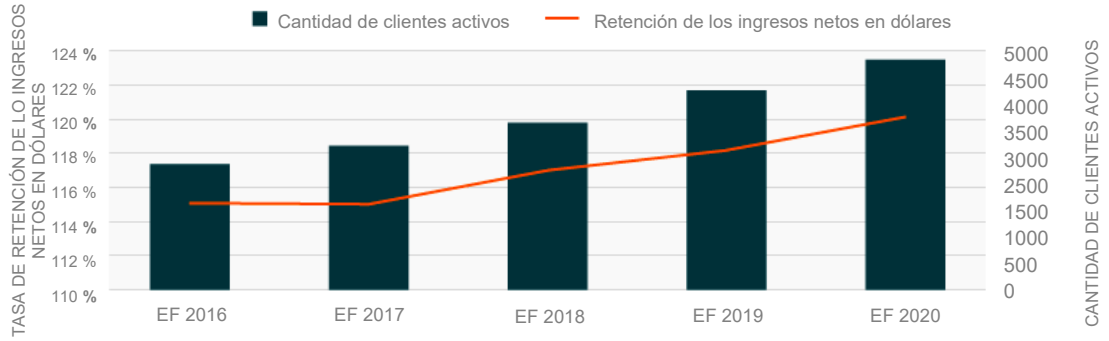
Zscaler ofrece capacidades que podrían dejar obsoleto el uso de tecnologías de red privada virtual (VPN). La solución empresarial de ZPA es más fácil de implementar, más fácil de administrar y más segura que las soluciones VPN tradicionales. ZPA proporciona a los usuarios acceso a aplicaciones internas, sin necesidad de conectarse a la red de una empresa o exponer a esos usuarios a Internet. Esta arquitectura también limita completamente la capacidad de un ciberataque para moverse horizontalmente por la red durante una filtración. La empresa describe esta arquitectura como “Zero Trust Network” (que no debe confiarse en ninguna red), que nunca extiende la red a todos los usuarios. Básicamente, se aparta a la red y la Internet se convierte así en la nueva red corporativa.[8]

Asegurar el acceso a aplicaciones internas y externas en portátiles, teléfonos inteligentes y otros dispositivos de Internet de las cosas es ahora una prioridad principal para las organizaciones, especialmente con el trabajo remoto y semipresencial que se está volviendo algo cada vez más común. Según la empresa de investigación Gartner, para 2023, el 60 % de las empresas eliminarán gradualmente la mayoría de sus VPN de acceso remoto y lo reemplazarán por redes Zero Trust Networks como la de Zscaler.[9]

Zscaler alcanzó un tasa de retención de los ingresos netos del 120% a finales del año fiscal 2020, lo que indica un crecimiento constante entre su base de usuarios existente.[10] Cabe destacar que la empresa cree que con sus productos ZIA y ZPA tiene una oportunidad de venta 6 veces superior solo con sus clientes existentes solamente.[11]

TASA DE RETENCIÓN DE LOS INGRESOS NETOS EN DÓLARES (IZQ.) Y CLIENTES ACTIVOS (DER.) DE ZSCALER

Fuente: Los ETF de Global X, información presentada por Zscaler Company.



Okta: Una empresa de rápido crecimiento en la administración de identidad y acceso

Okta es una empresa líder en ciberseguridad en el segmento de la administración de identidad y acceso (Identity Access Management, IAM). Este segmento de mercado se centra en permitir que las personas y los empleados adecuados accedan a los recursos adecuados en los momentos adecuados por los motivos adecuados.[12] La autenticación multifactor (Multi-factor authentication, MFA), la gestión de acceso a la interfaz de programación de aplicaciones (application programming interface, API) y el inicio de sesión único (single sign-on, SSO) son algunas soluciones de identidad que las empresas aprovechan cada vez más para garantizar que los usuarios adecuados estén autorizados para acceder a las diferentes aplicaciones.

También se prevé que las empresas en el mercado de IAM se beneficien del cambio hacia entornos de trabajo remotos e híbridos. Con empleados trabajando desde múltiples ubicaciones y conectándose desde

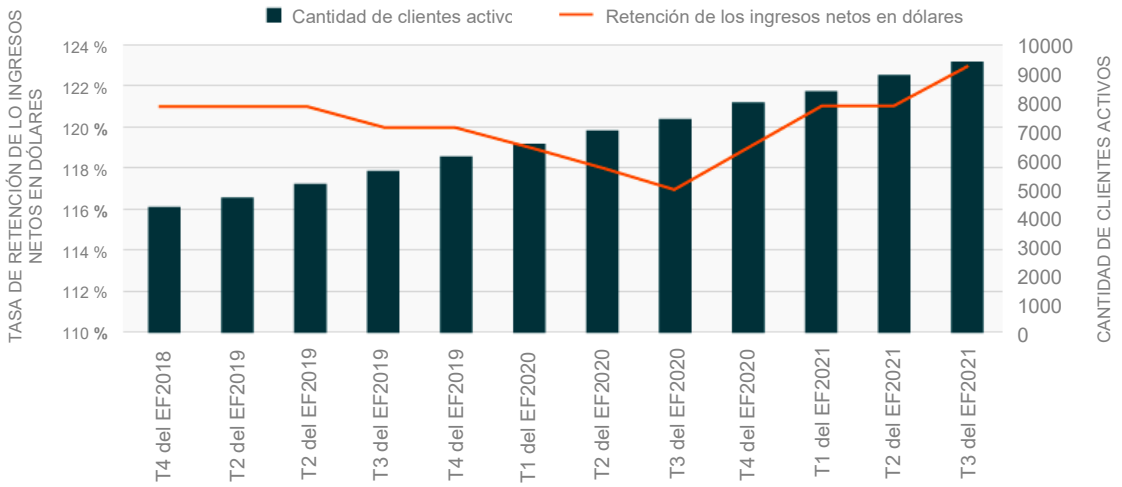
diferentes dispositivos, la administración de identidad y acceso permite a los departamentos de TI supervisar quién accede a aplicaciones específicas en un momento dado. La administración de identidad y acceso también ayuda a las empresas a supervisar y dar seguridad a los puntos de acceso dados a contratistas o clientes que deben acceder a determinadas aplicaciones internas.

Desde el punto de vista del usuario final, las soluciones de IAM de Okta proporcionan acceso a todas las aplicaciones dentro de un único portal. Esta funcionalidad reduce las llamadas al servicio de asistencia técnica relacionadas con el inicio de sesión en un 50 % y hace que sea un 50 % más rápido para los usuarios iniciar sesión y utilizar nuevas aplicaciones.[13] Okta estima que el mercado total potencial para identificación del personal es de 30 000 millones de dólares y el mercado para identificación de clientes es de 25 000 millones de dólares.[14]

Al igual que CrowdStrike y Zscaler, las soluciones de Okta son nativas de la nube. El 94 % de los ingresos de la empresa son recurrentes, ya que se generan a partir de servicios de suscripción. Okta es otra empresa con sólidas cifras de retención de ingresos netos en dólares, que para el tercer trimestre del EF2021 registrará un 123 %, lo que supone un incremento del 2% con respecto al trimestre anterior.

TASA DE RETENCIÓN DE LOS INGRESOS NETOS EN DÓLARES (IZQ.) Y CLIENTES ACTIVOS (DER.) DE OKTA

Fuente: Los ETF de Global X, información presentada por Okta Company.



Mimecast: Uno de los principales proveedores en seguridad de correos electrónicos

Mimecast es uno de los principales competidores en lo que probablemente sea el segmento más conocido en el mercado de la ciberseguridad: las puertas de enlace de correo electrónico seguras (Secure Email Gateways). El 95 % de los ciberataques utilizan el correo electróni co, lo que los convierte en el canal preferido para ataques oportunistas y con objetivo definido.[15] El conjunto de oportunidades de Mimecast es significativo, con aproximadamente 1000 millones de usuarios de correo electrónico corporativo en todo el mundo.[16] En la actualidad, la empresa tiene aproximadamente 15 millones de usuarios, lo que representa un 1,5 % de penetración del mercado mundial total.[17]

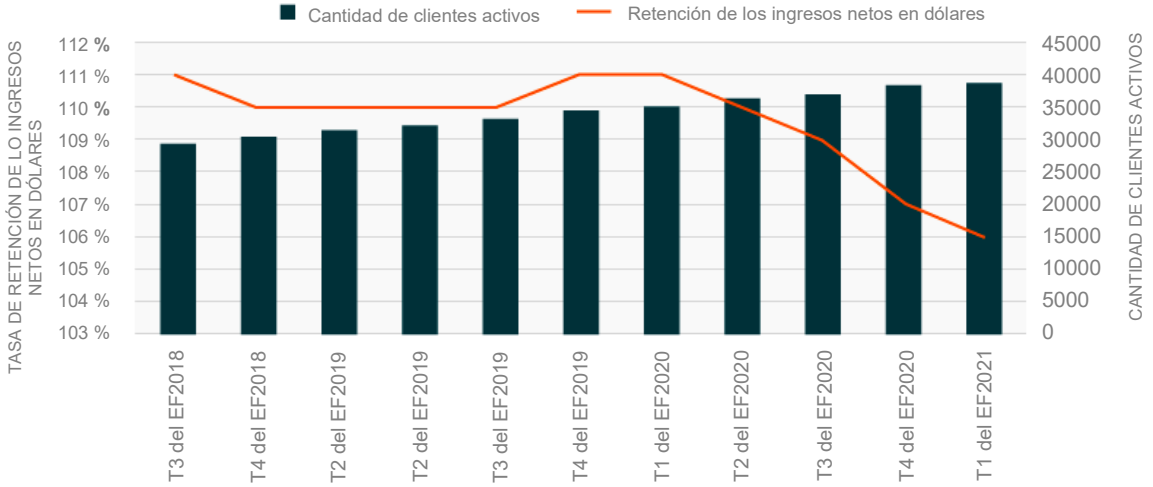
El objetivo del phishing (suplantación de identidad) masivo y de los ataques de phishing de objetivo definidos (spear-phishing) es atraer a los destinatarios con un mensaje que resuene con ellos y los coaccione para que entren en acción.[18] Los atacantes quieren robar dinero o datos importantes como la propiedad intelectual. El FBI estima que entre octubre de 2013 y mayo de 2018 se perdieron 12 000 millones de dólares por las vulnerabilidades de correos electrónicos.[19] El phishing por correo electrónico y el fraude de suplantación de identidad están presentes en la actualidad, pero la pandemia de COVID-19 hace que el ambiente sea aún más propenso los comportamientos de este tipo, con personas que pasan más tiempo en línea. De hecho, el fraude de suplantación de identidad y phishing por correo electrónico aumentó un 30 % solo en los primeros 100 días de la COVID-19.[20]

Mimecast proporciona soluciones que detectan y bloquean correos electrónicos que incluyen malware conocido o desconocido, URL maliciosos y suplantación de miembros del personal sénior u organizaciones de terceros como bancos, organismos federales o incluso clientes y proveedores. Mimecast complementa sus técnicas de detección tradicionales con funciones de IA como el aprendizaje profundo para identificar imágenes y logotipos no seguros para el trabajo, el aprendizaje automático para detectar patrones anómalos de riesgo en correos electrónicos y el aprendizaje supervisado para categorizar enlaces de alto riesgo.

Mimecast también implementa una arquitectura nativa en la nube, que combina agilidad con un atractivo modelo de negocio. La empresa ha mantenido una tasa de retención de ingresos netos en dólares por encima del 100 % en los últimos años, lo que se suma a la solidez de los modelos de negocio de las empresas de ciberseguridad.[21]

TASA DE RETENCIÓN DE LOS INGRESOS NETOS EN DÓLARES (IZQ.) Y CLIENTES ACTIVOS (DER.) DE MIMECAST

Fuente: Los ETF de Global X, información presentada por Mimecast Company.



Conclusión

La ciberseguridad no solo acapara los titulares de estos días, sino que también acapara presupuestos. El creciente número de ciberataques y sus posibles implicaciones para los sectores y gobiernos de todo el mundo hace que las herramientas de ciberseguridad sean indispensables para que las organizaciones operen de forma segura en múltiples funciones empresariales. Ya sea que se trate del correo electrónico, la gestión de la identidad, el acceso a aplicaciones internas y externas o la protección de dispositivos de usuario final, las cuatro empresas aquí destacadas son actores fundamentales para mantener más seguro este mundo cada vez más digital y ejemplificar la naturaleza multifacética del sector de la ciberseguridad.

Notas al pie:

1. IDC, “Ongoing Demand Will Drive Solid Growth for Security Products and Services, According to New IDC Spending Guide”, 13 de agosto de 2020.
2. IDG, “2020 IDG Cloud Computing Survey”, 8 de junio de 2020.
3. Identity Theft Resource Center, “Identity Theft Resource Center's 2020 Q3 Data Breach Analysis and Key Takeaways”, 14 de octubre de 2020.
4. CrowdStrike, “Corporate Overview”, diciembre de 2020.
5. Ibid.
6. CrowdStrike, (n4).
7. Zscaler, “Investor Relations: Cloud Stats”, consultado el 19 de enero de 2021.
8. Zscaler, “An Introduction to Zero Trust Network Access”, consultado el 19 de enero de 2021.
9. Zscaler, “VPN Alternative”, junio de 2020.
10. Zscaler, “Zscaler 2021 Analyst Day”, 11 de enero de 2021.
11. Ibid.
12. Gartner, “Identity and Access Management (IAM)”, consultado el 19 de enero de 2021.
13. Okta, “Single Sign-On”, consultado el 19 de enero de 2021.
14. Okta, “Q3 FY 2021 Results”, 2 de diciembre de 2020.
15. Mimecast, “The 2020 Gartner Market Guide for Email Security”, consultado el 19 de enero de 2021.
16. Mimecast, “Mimecast Investor Presentation”, noviembre de 2020.
17. Ibid.
18. Mimecast, “Email Security That Protects Your Organization”, consultado el 19 de enero de 2021.
19. FBI, “Business E-mail Compromise The 12 Billion Dollar Scam”, 12 de julio de 2018
20. Mimecast, “The State of Email Security: Download Hub”, consultado el 19 de enero de 2021.
21. Mimecast, (n16)