ISG Provider Lens™

Cybersecurity – Solutions and Services

Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)

Comparando pontos fortes, desafios e diferenciais competitivos dos fornecedores do país

Customized report courtesy of:

kaspersky

QUADRANT REPORT | JULHO DE 2022 | BRASIL

Table of Contents

Autor do Relatório: Sergio Rezende

Cibersegurança traz eficiência para os ambientes de tecnologia

Cibersegurança no Brasil, continua apresentando crescimento acima da média nestes últimos anos, acompanhando os demais países onde este mesmo estudo é realizado anualmente.

Temos acompanhado que a maioria dos provedores de serviços e de produtos tem reportado forte crescimento em volume de vendas, aumento do número de profissionais utilizados em tempo integral e, em muitos casos, o fortalecimento de seu portifólio com o lançamento de novos itens de produtos e serviços.

Alguns provedores continuam a reforçar sua presença e acelerar seu crescimento neste mercado através das parcerias comercias, enquanto muitos outros diversificam suas composições estratégicas com seus parceiros de tecnologia buscando cobrir novas áreas de atuação no mercado. Parte dessa demanda é explicada através dos investimentos realizados pelas empresas em produtos e serviços necessários para aumentar a proteção contra o acesso externo às redes corporativas ou mesmo aos seus serviços hospedados em nuvem.

Outro ponto importante e ainda presente foi a migração dos profissionais que trabalhavam nos escritórios e passaram a exercer suas funções em regime de home office o que exigiu novos investimentos das empresas. Ainda temos a LGPD, que demanda das empresas procurar por serviços estratégicos de segurança para planejar e implementar seus projetos garantindo a adequação às novas leis neste segmento.

Os Provedores cresceram no **mercado através de** aquisições

A soma destes fatores mudou paradigmas e criou novos desafios. De um lado, o encaminhamento dos funcionários para suas casas, provocado pela pandemia. Do outro, a necessidade de proteger a saúde de seus colaboradores e seus familiares ajudou a preservar a continuidade das operações das empresas. Assim, é importante ressaltar que o deslocamento de grande número de funcionários para casa criou enormes desafios para as equipes de infraestrutura e cibersegurança. Entre os principais, proporcionar conexões rápidas e confiáveis para todos os profissionais deslocados, assim como acesso seguro às redes locais corporativas e aos recursos em nuvem. Da mesma forma, o início da vigência da LGPD impôs um prazo final aos projetos e implementações de adequação elevando assim a pressão para que nas empresas para estarem em conformidade logo no início da vigência da lei.

Dentro da nova condição de trabalho em home office e da necessidade do cumprimento de suas tarefas diárias, sem acesso aos seus equipamentos instalados nos escritórios corporativos, os funcionários das empresas viram-se obrigados a utilizar seus dispositivos pessoais fixos ou móveis, e consequentemente de acessos à internet domésticos.

A utilização de dispositivos pessoais, às vezes compartilhados entre o funcionário e outros membros de suas famílias, normalmente estão desprovidos da maioria dos recursos de segurança disponíveis nos endpoints fornecidos pelas empresas aos seus funcionários. Esta, sem dúvida, foi uma das principais causas de elevação do risco de segurança. Assim como, o uso dos acessos de internet domésticas, em geral pouco ou nada protegidas, tornava o risco cibernético ainda mais elevado, colocando as empresas diante da necessidade inevitável de investir imediatamente para proteger todos esses itens buscando evitar impactos na continuidade dos negócios. Em contrapartida, no ambiente corporativo os endpoints estariam sob o controle das equipes de segurança e de TI e protegidos por redes no geral fortificadas e bem vigiadas.

Dentro deste cenário de ausência de proteção de acessos e endpoints foram detectados, em diversas regiões do planeta, atividades de cibercriminosos iniciando ataques cibernéticos de forma massiva, por meio de diferentes vetores, com o objetivo de contaminar esses dispositivos e, assim, obter não só informações e dados relevantes como, se possível, acesso para explorar redes e servidores. Na Dark Web, surgiram operações de comércio eletrônico especializadas na revenda de credenciais de acesso a redes corporativas, um crime que permite fácil evolução para outro ainda mais grave, que é o ataque de ransomware.

Devido a estes riscos e de possíveis desdobramentos na amplitude dos ataques, somados à necessidade de compliance com a LGPD, que as necessidades de investimento em cibersegurança se tornaram latentes e exigiram ações rápidas, conforme relatado pelos provedores no Brasil.

As empresas brasileiras responderam a esses desafios de várias maneiras, entre as quais acelerando sua digitalização, antecipando projetos de migração para soluções em nuvem, adiantando ou incentivando projetos de cibersegurança e também investindo em serviços e produtos capazes de ampliar ou complementar a segurança de ponta a ponta no acesso dos funcionários, necessária para a continuidade dos negócios. Isso se traduziu na contratação

de serviços de consultoria para planejamento estratégico, de serviços técnicos para instalação de produtos, de serviços gerenciados para monitoramento remoto de redes e proteção contra ameaças, assim como aquisição dos mais variados produtos para a proteção de dados, identidades e endpoints, como os que foram incluídos neste estudo.

Para muitos provedores de produtos e serviços de cibersegurança, essa expansão da demanda ocorrida no último ano representou uma oportunidade de elevar a sua participação no mercado brasileiro, inclusive por meio de aquisições. Em pelo menos um caso, um provedor de nuvem reconheceu que era o momento de também oferecer serviços de cibersegurança, inclusive fazendo aquisições para consolidar sua participação no mercado com mais rapidez.

Mesmo que, no momento da publicação deste relatório, estejamos em processo de controle da pandemia em que várias empresas já estejam adotando medidas de retorno total, parcial ou em modelo hibrido de seus funcionários aos escritórios, a expectativa geral dos provedores é de que o crescimento dos negócios continue nos próximos anos. Visto que os problemas não se resumem somente às grandes empresas, pequenas e medias também estão preocupadas e trabalhando forte para elevar seu nível de maturidade em segurança. Novas ferramentas e processos para acelerar o processo de detecção e resolução de ataques como o XDR estão sendo disponibilizados em defesa de seus clientes, sem contar com o aprofundamento da necessidade de entrega dos serviços baseados nos conceitos de Zero Trust e SASE estão gerando novos os projetos em seus pipelines. Porém, mesmo aqueles provedores que não contam com projetos de longo prazo têm boa quantidade de trabalho para curto e médio prazos em andamento e em negociação, acreditando que o mercado brasileiro de cibersegurança continuará vigoroso por muito tempo.

As razões para isso aparecem nos seis quadrantes estudados.

- No mercado de Identity and Access Management (IAM ou gerenciamento de identidade e acesso) parece viver in viés de consolidação, sendo a mais importante a da Auth0 por parte da Okta, por um valor de US$ 6,5 bilhões. Ela se mantem como Líder desse quadrante no estudo, ao lado de Broadcom, IBM, Microsoft, RSA e senhasegura. A empresa classificada como Rising Star foi a Micro Focus.
- Aquisições também no mercado de Data Leakage/Loss Prevention (DLP) and Data Security onde a Broadcom adquiriu a Bay Dynamics e a HelpSystems comprou Titus e Boldon James. Outro destaque foi que a McAffee se tornou a Trellix neste segmento. Este quadrante mostrou como Líderes a Broadcom, Forcepoint, IBM, Trellix, Microsoft, OpenText, Trend Micro e Varonis, sendo Rising Star a HelpSystems.
- No mercado de Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR) temos a chegada da Crowdstrike e da VMware Carbon Black como as novas lideranças no estudo. Assim, os Líderes nesse quadrante foram Broadcom, Crowdstrike, Microsoft, Trend Micro, VMware Carbon Black e Kaspersky, sendo Rising Star a Trellix.
- Na área de Technical Security Services tivemos a chegada da NTT Ltd. como player de segurança do mercado nacional. Nesse quadrante os Líderes

foram Agility Networks, Capgemini, Deloitte, IBM, ISH Tecnologia, Logicalis, NTT Ltd e o Rising Star foi a Accenture.

- Nos serviços estratégicos, analisados no quadrante de Strategic Security Services, destacamos a entrada da Tempest como um novo player do estudo. Nesse quadrante os Líderes foram Accenture, Capgemini, Deloitte, EY, IBM, ISH Tecnologia, Logicalis e PwC e o Rising star foi a Tempest.
- Para finalizar, no mercado de Managed Security Services ou serviços gerenciados de segurança destaco a Accenture que mostrou seu crescimento passando de Rising Star em 2021 para Lider este ano juntamente como Agility Networks, Edge UOL, IBM, ISH Tecnologia, Logicalis, Lumen, Stefanini Rafael, Unisys e Wipro, sendo NTT Ltd. a Rising Star.

As pequenas e medias empresas também estão elevando seu nível de maturidade em segurança

Posicionamento do Provedor

Page 1 of 6

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Absolute Software	Not In	Contender	Contender	Not In	Not In	Not In
Accenture	Not In	Not In	Not In	Rising Star ★	Leader	Leader
Agility	Not In	Not In	Not In	Leader	Not In	Leader
Ativy	Not In	Not In	Not In	Contender	Product Challenger	Contender
Atos	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Broadcom	Leader	Leader	Leader	Not In	Not In	Not In
Capgemini	Not In	Not In	Not In	Leader	Leader	Product Challenger
Check Point	Contender	Product Challenger	Product Challenger	Not In	Not In	Not In
Cipher	Not In	Not In	Product Challenger	Not In	Contender	Product Challenger
Cisco	Not In	Not In	Contender	Not In	Not In	Not In
Claranet	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Compugraf	Not In	Not In	Not In	Contender	Not In	Not In

Posicionamento do Provedor

Page 2 of 6

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
CrowdStrike	Not In	Not In	Leader	Not In	Not In	Not In
CyberArk	Product Challenger	Not In	Not In	Not In	Not In	Not In
Cybereason	Not In	Not In	Product Challenger	Not In	Not In	Not In
Deloitte	Not In	Not In	Not In	Leader	Leader	Product Challenger
DXC Technology	Not In	Not In	Not In	Product Challenger	Contender	Contender
Edge UOL	Not In	Not In	Not In	Product Challenger	Not In	Leader
E-Trust	Product Challenger	Not In	Not In	Not In	Not In	Not In
EY	Not In	Not In	Not In	Not In	Leader	Not In
FastHelp	Not In	Not In	Not In	Contender	Not In	Contender
Forcepoint	Not In	Leader	Not In	Not In	Not In	Not In
ForgeRock	Product Challenger	Not In	Not In	Not In	Not In	Not In

Posicionamento do Provedor

Page 3 of 6

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Fortinet	Contender	Product Challenger	Product Challenger	Not In	Not In	Not In
GBS	Not In	Product Challenger	Not In	Not In	Not In	Not In
GoCache	Not In	Not In	Contender	Not In	Not In	Not In
Google	Not In	Contender	Not In	Not In	Not In	Not In
HelpSystems	Not In	Rising Star ★	Not In	Not In	Not In	Not In
Huge Networks	Not In	Not In	Contender	Not In	Not In	Not In
IBLISS	Not In	Not In	Not In	Not In	Product Challenger	Not In
IBM	Leader	Leader	Product Challenger	Leader	Leader	Leader
ISH	Not In	Not In	Not In	Leader	Leader	Leader
Kaspersky	Not In	Not In	Leader	Not In	Not In	Not In
Kryptus	Not In	Not In	Not In	Not In	Contender	Not In

Posicionamento do Provedor

Page 4 of 6

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Logicalis	Not In	Not In	Not In	Leader	Leader	Leader
Lumen	Not In	Not In	Not In	Not In	Not In	Leader
Micro Focus	Rising Star ★	Not In	Not In	Not In	Not In	Not In
Microsoft	Leader	Leader	Leader	Not In	Not In	Not In
NEC	Not In	Not In	Not In	Product Challenger	Market Challenger	Contender
Netskope	Not In	Product Challenger	Not In	Not In	Not In	Not In
Nextios	Not In	Not In	Not In	Contender	Not In	Not In
NTT	Not In	Not In	Not In	Leader	Product Challenger	Rising Star ★
Okta	Leader	Not In	Not In	Not In	Not In	Not In
One Identity (OneLogin)	Product Challenger	Not In	Not In	Not In	Not In	Not In
OpenText	Not In	Leader	Not In	Not In	Not In	Not In

Posicionamento do Provedor

Page 5 of 6

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Palo Alto Networks	Not In	Not In	Contender	Not In	Not In	Not In
Ping Identity	Product Challenger	Not In	Not In	Not In	Not In	Not In
PwC	Not In	Not In	Not In	Not In	Leader	Not In
RSA	Leader	Not In	Not In	Not In	Not In	Not In
SailPoint	Product Challenger	Not In	Not In	Not In	Not In	Not In
senhasegura	Leader	Not In	Not In	Not In	Not In	Not In
SONDA	Not In	Not In	Not In	Contender	Not In	Contender
Sophos	Not In	Contender	Product Challenger	Not In	Not In	Not In
Stefanini Rafael	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader
TDeC	Not In	Not In	Not In	Contender	Not In	Not In
Tempest	Not In	Not In	Not In	Product Challenger	Rising Star ★	Product Challenger

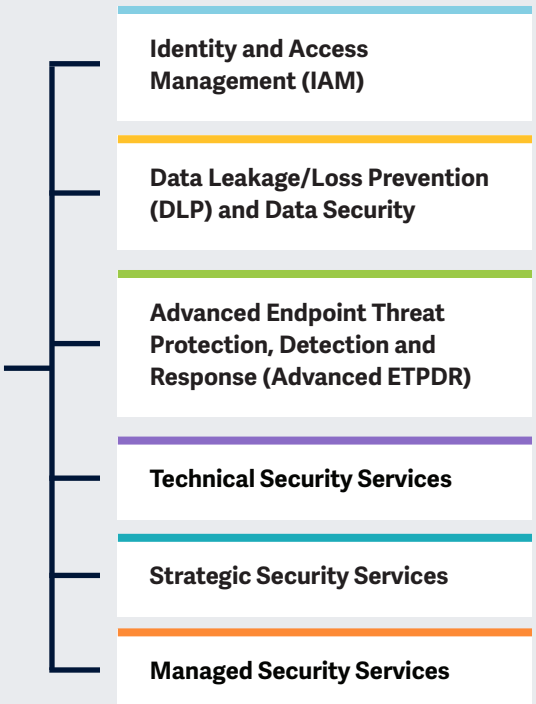
Posicionamento do Provedor

Page 6 of 6

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Thales	Contender	Not In	Not In	Not In	Not In	Not In
TIVIT	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger
Trellix	Not In	Leader	Rising Star ★	Not In	Not In	Not In
Trend Micro	Not In	Leader	Leader	Not In	Not In	Not In
T-Systems	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger
Unisys	Market Challenger	Not In	Not In	Not In	Product Challenger	Leader
Varonis	Not In	Leader	Not In	Not In	Not In	Not In
VMware Carbon Black	Not In	Not In	Leader	Not In	Not In	Not In
WatchGuard	Not In	Product Challenger	Not In	Not In	Not In	Not In
Wipro	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader
Zscaler	Not In	Product Challenger	Not In	Not In	Not In	Not In

Este estudo foca no que a ISG classifica como fundamental em Cibersegurança.

Simplified Illustration Source: ISG 2022



Definição

Soluções de Segurança:

- Gerenciamento de identidade e acesso (IAM);
- Prevenção contra vazamento/perda de dados (DLP) e segurança de dados;
- Proteção, detecção e resposta avançada a ameaças de endpoint (ETPDR avançado).

Serviços de Segurança:

- Serviços de Segurança Estratégica;
- Serviços Técnicos de Segurança;
- Serviços Gerenciados de Segurança.

As empresas estão absorvendo novas tecnologias para embarcar em sua jornada de transformação digital para se manterem competitivas e se alinharem às necessidades dos usuários finais em constante evolução. A crescente adoção dessas tecnologias, juntamente com novas ferramentas para fornecer eficiência e velocidade, levou a um aumento na exposição e a uma crescente superfície de ataque de ameaças. Ransomware, ameaças persistentes avançadas e ataques de phishing permanecem como algumas das principais ameaças cibernéticas.

Os invasores estão sempre procurando maneiras novas e ingênuas de violar os mecanismos de defesa. Isso levou a um aumento em sua sofisticação, pois esses invasores acessam diferentes pontos em um ecossistema de TI corporativo, como redes de cadeia de suprimentos. Este último ano testemunhou vários outros ataques cibernéticos de alto perfil. Os ataques visavam propriedade intelectual, informações de identificação pessoal (PII) e registros confidenciais e informações de clientes de empresas

de saúde, hospitalidade, TI, finanças e outros setores, juntamente com dados pertencentes a estados-nação. Além de causar danos operacionais, esses ataques afetaram o valor da marca, os sistemas de TI e a saúde financeira das organizações visadas.

O cenário global ficou mais exacerbado com a pandemia da Covid-19, que resultou em grandes massas trabalhando remotamente, principalmente em casa. Esse novo modelo de trabalho levou a um aumento no uso de ferramentas e plataformas de colaboração e redes públicas, expondo os usuários a hackers por meio de vetores de ataque como phishing e outras ameaças maliciosas. Com esse cenário de ameaças em constante mudança, as empresas precisaram adotar uma abordagem detalhada e inclusiva de segurança cibernética para proteger seus negócios, implementando uma combinação de produtos e serviços de segurança em áreas como gerenciamento de identidade e acesso (IAM), DLP e serviços de segurança gerenciados (MSS) para obter uma estrutura segura robusta que se alinhasse às suas necessidades e visão.

À medida que a natureza e a complexidade das ameaças de segurança cibernética continuam a aumentar, os hackers estão constantemente pesquisando e atacando fontes vulneráveis e infraestruturas de TI. Algumas ameaças, como phishing, spear phishing e ransomware, visam se beneficiar da ignorância dos usuários e de seu comportamento online. Os altos níveis de atividade online, liderados por comércio eletrônico e transações online, ampliaram a postura de vulnerabilidade e expuseram os usuários finais a cibercriminosos que procuram por qualquer vestígio digital deixado para trás. Isso torna os usuários e sistemas de endpoint de TI com baixa postura de segurança e mecanismos de defesa fracos presas fáceis para ataques cibernéticos.

Essas sérias implicações de ameaças de phishing e ransomware deram origem ao surgimento de serviços para combater essas ameaças avançadas. Esses serviços e soluções vão além do perímetro básico e das medidas de segurança convencionais para monitoramento, inspeção e proteção profundos e contínuos, juntamente com uma abordagem estruturada de resposta a incidentes. Além da necessidade de autoproteção, leis e regulamentos, como o Regulamento Geral de Proteção de Dados (GDPR) na Europa, obrigaram as empresas a implementar medidas de proteção mais fortes para combater ataques cibernéticos. Legislação semelhante existe em outros países, como Brasil e Austrália, para proteger os usuários de ameaças e ataques cibernéticos.

A cibersegurança tornou-se uma área de prática importante para as empresas devido ao seu impacto nos negócios e processos. No entanto, os executivos de TI muitas vezes lutam para justificar os investimentos em segurança para as partes interessadas nos negócios, principalmente os CFOs. Ao contrário de outros projetos de TI, nem sempre é possível medir e demonstrar o ROI, bem como quantificar os riscos relacionados a ameaças. Portanto, as medidas de segurança geralmente são de baixo nível e não são adequadas para lidar com ameaças sofisticadas. Por outro lado, a disponibilidade de tecnologia adequada nem sempre resulta na eliminação de vulnerabilidades; muitos incidentes de segurança, como ataques de Trojan e phishing, são causados devido à ignorância dos usuários finais. Aspectos relacionados à conscientização entre usuários finais podem resultar em ataques direcionados, como ameaças

persistentes avançadas e ransomware. Isso afeta a reputação da marca, causa perdas financeiras e de dados e leva a interrupções operacionais. Assim, a consultoria e a formação dos utilizadores continuam a desempenhar um papel fundamental, juntamente com uma infraestrutura de TIC atualizada. Há também um foco maior em serviços de monitoramento, detecção e resposta para proteger as empresas além do perímetro com proteção baseada em assinatura e outros serviços de segurança.

O estudo ISG Provider Lens™ Cybersecurity – Solutions and Services 2022 visa apoiar os tomadores de decisão de TIC a fazer o melhor uso de seus orçamentos de segurança apertados, oferecendo o seguinte:

- Transparência sobre os pontos fortes e fracos dos fornecedores relevantes;
- Posicionamento diferenciado dos provedores por segmentos de mercado;
- Perspectiva sobre os mercados locais.

Para provedores e fornecedores de TI, este estudo serve como uma importante base de tomada de decisão para posicionamento, relacionamentos-chave e considerações de entrada no mercado (GTM). Os consultores e clientes corporativos da ISG também aproveitam as informações dos relatórios ISG Provider Lens™ enquanto avaliam seus relacionamentos atuais com fornecedores e possíveis novos compromissos.

Escopo do Relatório

Neste estudo de quadrante ISG Provider Lens™, o ISG inclui os seguintes quadrantes: IAM, DLP, ETPDR avançado e Serviços de Segurança Estratégica, Serviços Técnicos de Segurança e Serviços Gerenciados de Segurança.

Este estudo ISG Provider Lens™ oferece aos tomadores de decisão de TI:

- Transparência sobre os pontos fortes e fracos dos fornecedores/fornecedores de software relevantes;
- Posicionamento diferenciado de fornecedores por segmentos
- Foco no mercado regional

Nosso estudo serve como base para importantes tomadas de decisão em termos de posicionamento, relacionamentos-chave e considerações de entrada no mercado. Consultores ISG e clientes corporativos também usam as informações desses relatórios para avaliar seus relacionamentos com fornecedores existentes e possíveis compromissos.

Classificações do Provedor

A posição do provedor reflete a adequação dos provedores de TI/fornecedores de software para um segmento de mercado definido (quadrante). Sem mais adições, a posição sempre se aplica a todas as classes e setores de porte de empresa. Caso os requisitos de serviços de TI dos clientes corporativos sejam diferentes e o espectro de provedores de TI que operam no mercado local seja suficientemente amplo, uma diferenciação adicional dos provedores de TI por desempenho é feita de acordo com o grupo-alvo de produtos e serviços. Ao fazer isso, o ISG considera os requisitos do setor ou o número de funcionários, bem como as estruturas corporativas dos clientes e posiciona os fornecedores de TI de acordo com sua área de foco. Como resultado, o ISG os diferencia, se necessário, em dois grupos-alvo de clientes que são definidos da seguinte forma:

Midmarket/Mercado Intermediário: Empresas com 100 a 4.999 funcionários ou faturamento entre US$ 20 milhões e US$ 999 milhões com sede central no respectivo país, geralmente de propriedade privada.

Large Accounts/Grandes contas: empresas multinacionais com mais de 5.000 funcionários ou receita acima de US$ 1 bilhão, com atividades em todo o mundo e estruturas de tomada de decisão globalmente distribuídas.

Os quadrantes ISG Provider Lens™ são criados usando uma matriz de avaliação contendo três segmentos (Leader, Product & Market Challenger e Contender), e os fornecedores estão posicionados de acordo. Cada quadrante ISG Provider Lens pode incluir um provedor de serviços que a ISG acredita ter forte potencial para entrar no quadrante Líder. Esse tipo de provedor pode ser classificado como Rising Star.

Número de prestadores em cada quadrante: o ISG classifica e posiciona os prestadores mais relevantes de acordo com o escopo do relatório para cada quadrante e limita o máximo de prestadores por quadrante a 25 (exceções são possíveis).

(Continua na próxima página)

Classificações do Provedor: Quadrantes principais

Product Challengers:
Os Product Challengers oferecem um portfólio de produtos e serviços que fornece uma cobertura acima da média dos requisitos corporativos, mas não são capazes de fornecer os mesmos recursos e força de atuação que os Leaders em relação às categorias e mercados individuais. Freqüentemente, isso se deve ao tamanho do respectivo fornecedor ou uma trajetória mais fraca dentro do respectivo segmento-alvo.

Leaders:
Os Leaders entre os fornecedores / provedores têm uma oferta de produtos e serviços altamente atraente e um mercado e posição competitiva muito fortes; eles cumprem todos os requisitos para uma atuação bem-sucedida no mercado. Eles podem ser considerados formadores de opinião, impulsionando estrategicamente o mercado. Eles também garantem estabilidade e resistência inovadoras.

Contenders:
Os concorrentes que se encontram neste quadrante ainda carecem de produtos e serviços maduros ou profundidade e amplitude suficientes em sua oferta, mas também mostram alguns pontos fortes e potencial de melhoria em seus esforços de atuação no mercado. Esses fornecedores geralmente são generalistas ou participantes de nicho.

Market Challengers:
Os Market Challengers também são muito competitivos, mas ainda há um potencial de melhoria significativa no portfólio e eles ficam claramente atrás dos Leaders. Freqüentemente, os Market Challengers são fornecedores estabelecidos que levam mais tempo para lidar com novas tendências devido ao seu tamanho e estrutura da empresa e, portanto, têm algum potencial para otimizar seu portfólio e aumentar sua atratividade.

Classificações do Provedor: Quadrantes principais

★ Rising Stars
Os Rising Stars são geralmente os Product Challengers com alto potencial no futuro. As empresas que recebem o prêmio Rising Star têm um portfólio promissor, incluindo o roadmap necessário e o foco adequado nas principais tendências do mercado e requisitos do cliente. Os Rising Stars também possuem uma excelente gestão e compreensão do mercado local. Este prêmio é concedido apenas a fornecedores ou prestadores de serviços que fizeram um progresso significativo em direção a suas metas nos últimos 12 meses e devem alcançar o quadrante Leader nos próximos 12-24 meses devido ao seu impacto acima da média e força para inovação.

Not in
O provedor de serviços ou fornecedor não foi incluído neste quadrante. Pode haver um ou vários motivos pelos quais essa designação foi aplicada: O ISG não conseguiu obter informações suficientes para posicionar a empresa; a empresa não fornece o serviço ou solução relevante conforme definido para cada quadrante de um estudo; ou a empresa não se qualificou devido à sua participação no mercado, receita, capacidade de entrega, número de clientes ou outras métricas de escala a serem comparadas diretamente com outros fornecedores no quadrante. A omissão no quadrante não significa que o provedor ou fornecedor do serviço não ofereça esse serviço ou solução, nem confere qualquer outro significado.

Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)

Quem deve ler este relatório

Este relatório é relevante para empresas de todos os setores no Brasil, visando avaliar fornecedores de produtos de proteção, detecção e resposta a ameaças de *endpoints* avançados.

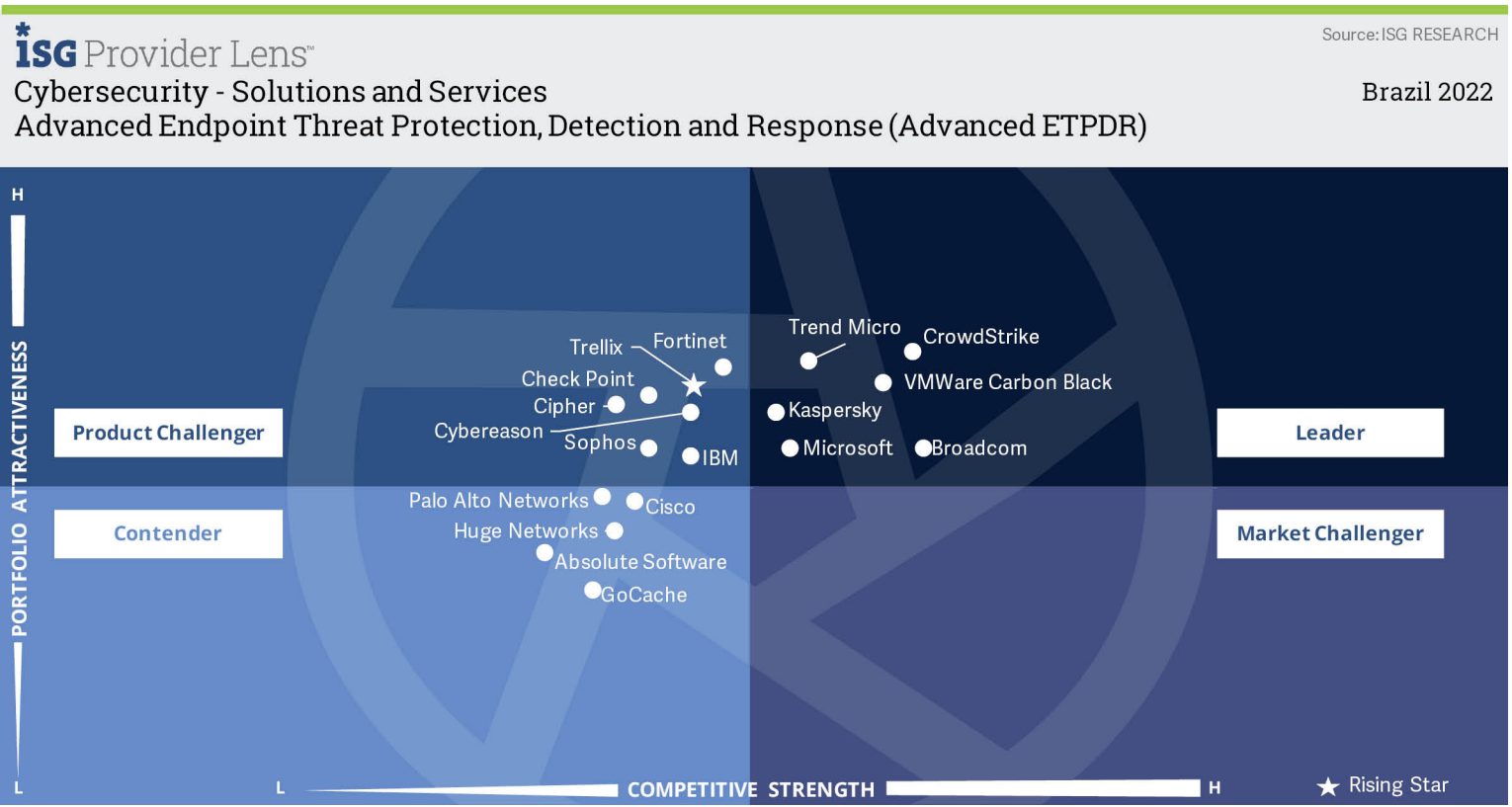
Neste relatório, o ISG destaca o posicionamento de mercado atual dos fornecedores de produtos avançados para ameaça de *endpoint* voltado às empresas no Brasil, e como cada fornecedor lida com os principais desafios enfrentados na região.

Uma vez que a empresa sofre um ataque cibernético, um fator crítico para minimizar qualquer ação criminosa é a velocidade de detecção e resposta ao incidente. Essa busca das empresas por um produto que permita identificar ameaças da forma mais ágil possível tem movimentado os fornecedores de soluções de proteção, detecção e resposta a ameaças de *endpoints* avançados a desenvolver e a melhorar seus *softwares* proprietários. Por isso vemos a crescente escalada no uso de inteligência artificial, machine learning e *security analytics* na detecção e resposta de incidentes. Além disso, os fornecedores seguem trabalhando no desenvolvimento de novos produtos que vão além do *endpoint*, como a detecção e resposta estendida (XDR), atuando em várias camadas de segurança.

Diretores de Segurança da Informação devem ler este relatório para adquirir uma visão mais ampla das últimas tendências no cenário da segurança. O relatório fornece uma compreensão abrangente de ameaças imediatas, das capacidades de segurança necessárias para combatê-las e auxilia na tomada de decisões estratégicas de negócios para atender às preocupações de segurança existentes. Adicionalmente, traz *insights* valiosos sobre como aumentar a produtividade e reduzir a complexidade nas operações de segurança empresarial.

Diretores de Tecnologia devem ler este relatório para acompanharem um cenário de segurança em constante mudança. Além de estabelecer objetivos estratégicos e desenvolver plataformas de segurança de acordo com as necessidades de marketing, os CTOs podem melhorar as vantagens competitivas para atrair mais perspectivas.

Diretores de estratégia devem ler este relatório para compreender o posicionamento relativo e as capacidades dos fornecedores de *endpoint* avançados no mercado brasileiro, que ajudam a empresa a definir sua visão e estratégia para a segurança cibernética



Este quadrante avalia os fornecedores de soluções de ETPDR avançado caracterizados por sua capacidade de oferecer software e serviços associados para **monitoramento contínuo e visibilidade total de todos os pontos de extremidade, e podem analisar, prevenir e responder a ameaças avançadas.**

Sergio Rezende

Definição

Os fornecedores e provedores de soluções de ETPDR avançado são caracterizados por sua capacidade de oferecer software proprietário e serviços associados. Este quadrante também inclui software como serviço baseado em software proprietário. Provedores de serviços puros que não oferecem um produto ETPDR avançado (local ou baseado na nuvem) com base em software desenvolvido por conta própria não estão incluídos aqui. Este quadrante avalia os provedores que oferecem produtos que podem fornecer monitoramento contínuo e visibilidade total de todos os pontos de extremidade, e podem analisar, prevenir e responder a ameaças avançadas.

Essas soluções vão além da simples proteção baseada em assinatura e oferecem proteção contra adversários, como ransomware, ameaças persistentes avançadas (APTs) e malware, investigando os incidentes em todo o cenário de ponto de extremidade. A solução deve ser capaz de isolar o ponto de extremidade infectado e tomar a ação corretiva/ remediação necessária. Tais soluções compreendem um banco de dados em que as informações coletadas da rede e pontos de extremidade são agregados, analisados e investigados, e um agente que reside no sistema host oferece os recursos de monitoramento e relatório para os eventos.

Critérios de Eligibilidade

1. Relevância (**receita e número de clientes**) como fornecedor avançado de produtos ETPDR no respectivo país.
2. A oferta de ETPDR avançada deve ser baseada em software proprietário e não em software de terceiros.
3. As soluções dos provedores devem fornecer cobertura abrangente e total e visibilidade de todos os terminais na rede.
4. A solução deve demonstrar eficácia no **bloqueio de ameaças sofisticadas,** como ameaças persistentes avançadas, ransomware e malware.
5. A solução deve aproveitar a inteligência de ameaças, analisar e oferecer percepções em tempo real sobre as ameaças que emanam dos pontos de

Observações

A proteção de endpoints é um dos segmentos mais disputados no mercado de segurança cibernética. Os endpoints, ou terminais, são os dispositivos por meio dos quais os usuários acessam todas as aplicações.

A proteção dos endpoints evoluiu na mesma medida em que as ameaças, exigindo dos fornecedores, em contrapartida, evolução contínua das soluções. A sofisticação da maioria colocou-as muito longe do ponto inicial, que foram os antivírus, transformando o conjunto de endpoints protegidos numa verdadeira rede de sensores que são contados às centenas de milhões.

O desenvolvimento e comercialização dessas soluções criou empresas robustas de alcance global, a maioria com forte presença no Brasil e disputando aqui um mercado que tem quase 500 milhões de dispositivos. Embora a maioria tenha começado pequena, algumas pela iniciativa de especialistas em computação que se tornaram empreendedores, aquelas que foram bem-sucedidas, se transformaram em empresas de alcance global, com faturamento, no geral, contabilizado em bilhões de dólares.

Isso implica investimentos contínuos em pesquisa e desenvolvimento de tecnologias, como as de inteligência artificial, machine learning, big data e analytics, sem as quais não existe a possibilidade de tratar os incidentes e proteger os endpoints.

Dos 101 fornecedores de produtos e de serviços avaliados neste estudo, 18 se qualificaram para este quadrante, seis foram nomeados Líderes e um foi nomeado Rising Star.

Broadcom

Broadcom: seu produto Symantec Endpoint Protection possui mais de 14 anos no mercado, sendo um dos mais vendidos pela sua ampla rede de parceiros no Brasil. Os volumes de vendas no país tendem a crescer no futuro, conforme a empresa consiga negociar um acordo de preços de itens da Symantec com o governo federal.

Crowdstrike

Crowdstrike: construído desde o início como uma plataforma baseada em nuvem, o CrowdStrike Falcon é um novo participante no espaço de segurança de endpoints. Seu mecanismo de detecção de ameaças combina aprendizado de máquina, identificadores comportamentais de malware e inteligência de ameaças para detectar ataques, mesmo de novos malwares.

kaspersky

Kaspersky: com crescimento de 15% YoY em receita gerada na América Latina, a Kaspersky opera no Brasil com equipe de vendas, suporte e pesquisa de ameaças, oferecendo suporte em português e espanhol estando entre os poucos provedores que investigam em detalhe ameaças criadas em território brasileiro e latino-americano.

Microsoft

Microsoft: o grande número de estações de trabalho, servidores e serviços de nuvem protegidos pelo Windows Defender coloca a Microsoft num lugar privilegiado no mercado de proteção avançada de endpoints, apoiado por uma vasta rede de parceiros para vendas, instalações e suporte no Brasil.

Trend Micro

Trend Micro: a Trend Micro continua a ser o fornecedor preferido de muitas das grandes corporações do Brasil, incluindo algumas da área financeira, o que continua a lhe proporcionar elevada reputação. Contratou novos executivos, ampliou o território de operação, conquistou novos clientes e ampliou seus programas de certificação.

VWware Carbon Black

VWware Carbon Black: Adquirida pela VMware por US$ 2.1B, é líder no fornecimento de nuvem de segurança da próxima geração e conta com mais de 5.600 clientes e 500 parceiros em todo o mundo. A inovadora plataforma de segurança nativa na nuvem da empresa aproveita a análise de dados e de comportamentos para fornecer proteção abrangente aos terminais até mesmo contra os ataques cibernéticos mais avançados.

Trellix

Trellix: tem um dos mais robustos portfólios de prevenção à perda de dados do mercado, organizado com seis produtos, e se mantém como um dos players mais vigorosos entre os fornecedores de soluções de cibersegurança, tendo feito em 2020 mais uma aquisição, a Lightpoint Security, empresa que desenvolveu um browser com segurança aprimorada.

Leader

"Através de seus Centros de Transparência, a Kaspersky visa se tornar transparente sobre suas tecnologias de proteção, infraestrutura e práticas de processamento de dados."

Sergio Rezende

Kaspersky

Visão Geral

A Kaspersky é uma empresa privada internacional sediada em Moscou, Rússia com sua holding registrada no Reino Unido e sua infraestrutura de processamento de dados localizada na Suíça. A empresa tem operações administradas por entidades locais em 30 países e possui mais de 4.000 funcionários.

A Kaspersky Ltda do Brasil, sede da América Latina para as operações na região possui 15 anos de atuação. A nível mundial no FY21, a empresa gerou US$ 752.28 milhões (+6.56% A/A) em receita, com soluções e serviços de segurança como seu maior segmento. Suas soluções estão instaladas em mais de 400 milhões de dispositivos com atuação em proteção avançada de endpoints, cloud, EDR e servidores.

Pontos Fortes

Kaspersky Transparency Centers: os centros em New Brunswick, Zurique, Madri, Kuala Lumpur e São Paulo compartilham com parceiros e governos informações sobre produtos, código fonte e desempenho.

Sensores: cada instalação de produto de segurança feita pela empresa transforma o dispositivo num sensor de detecção de ameaças, caso o usuário opte por compartilhar estas informações com a empresa. Assim que uma ameaça é detectada, os dados anonimizados associados a ela são enviados para análise; a confirmação da existência de uma nova ameaça permite a atualização da base de dados de malware da companhia e também do produto, seguida de atualização e proteção de toda a base instalada.

Foco na Região: são mais de 1.500 parceiros ativos no Brasil, totalizando uma rede de mais de 6.000 parceiros na América Latina. A Kaspersky conta com uma equipe com cerca de 50 profissionais no Brasil e mais 90 colaboradores na América Latina. Possui um centro de suporte local, com atendimento em português e espanhol para serviços de Resposta a Incidentes, Gerenciamento de SOC e Centro de Pesquisa de Ameaças.

Crescimento: a Kaspersky no Brasil continua crescendo sua receita. Em 2021 cresceu 12%, sendo que no segmento enterprise ele foi da ordem de 35%, com uma média CAGR de 2018 a 2021 de 25% durante os últimos quatro anos.

Ponto de Atenção

Manter os parceiros no Brasil atualizados com seus produtos e aptos a oferecer todo o suporte necessário de modo a evitar impactos nas operações dos clientes.

Apêndice

Metodologia e Equipe

O estudo de pesquisa "ISG Provider Lens™ Cybersecurity - Solutions and Services" analisa os fornecedores de software/ fornecedores de serviços relevantes no Brasil, com base em um processo de análise e pesquisa multifásico. Ele posiciona esses fornecedores com base na metodologia ISG Research.

Lead Author:
Sergio Rezende

Editor:
Mondoni Press

Research Analyst:
Gabriel Sobanski

Data Analyst:
Rajesh Chillappagari

Consultant Advisor:
Doug Saylors

Project Manager:
Ridam Bhattacharjee

A Information Services Group, Inc. é exclusivamente responsável pelo conteúdodeste relatório. A menos que citado de outra forma, todo o conteúdo, incluindo ilustrações, pesquisa, conclusões, afirmações e posições contidas neste relatório foram desenvolvidas por, e são de propriedade exclusiva da Information Services Group Inc.

A pesquisa e análise apresentadas neste relatório incluem pesquisas do programa ISG Provider Lens™, programas de pesquisa ISG em andamento, entrevistas com consultores do ISG, briefings com fornecedores de serviços e análise de informações de mercado publicamente disponíveis de várias fontes. Os dados coletados para este relatório representam informações que o ISG acredita serem atuais em Junho de 2022, para fornecedores que participaram ativamente, bem como para fornecedores que não participaram. O ISG reconhece que muitas fusões e aquisições ocorreram desde então, mas essas mudanças não estão refletidas neste relatório.

Todas as referências de receita são em dólares americanos ($US), a menos que indicado de outra forma.

O estudo foi dividido nas seguintes etapas:

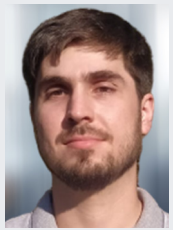
1. Definição do mercado Cybersecurity – Solutions and Services
2. Uso de pesquisas baseadas em questionários de provedores/ fornecedores de serviços em todos os tópicos de tendência
3. Discussões interativas com provedores/fornecedores de serviços sobre recursos e casos de uso
4. Uso de bancos de dados internos do ISG e o conhecimento e experiência do consultor (sempre que aplicável)
5. Uso do Star of Excellence CX-Data
6. Análise detalhada e avaliação de serviços e documentação de serviços com base nos fatos e números recebidos de fornecedores e outras fontes.
7. Uso dos seguintes critérios principais de avaliação:
   * Estratégia e visão
   * Inovação Tecnológica
   * Conhecimento e presença da marca no mercado
   * Cenário de vendas e parceiros
   * Amplitude e profundidade do portfólio de serviços oferecidos
   * CX e Recomendação

Autor

Sergio Rezende
Analista Líder

Consultor Sênior de TIC com mais de 25 anos de experiência liderando a transformação digital de clientes. Responsável pela implementação de soluções tecnológicas para resolver problemas de negócios através de projetos de cibersegurança, transformação em aplicações e infraestrutura, soluções de inovação, gerenciamento de serviços, cloud, gerenciamento de equipes em empresas como EDS e HP. Atua como consultor na aplicação de metodologia de sourcing estratégico para identificação, análise e contratação de provedores de soluções e serviços de tecnologia da informação. Atualmente como Analista Lider do ISG Provider Lens, trabalha como membro do time global nos Estudos de Pesquisas dos Provedores de Soluções e Serviços para indústria de Cibersegurança no Brasil.

Analista de Pesquisa



Gabriel Sobanski
Analista de Pesquisa

Gabriel Sobanski é analista de pesquisa do ISG e é responsável pelo suporte e coautoria dos estudos da Provider Lens™ sobre Ecossistema ServiceNow, Ecossistema Salesforce, Ecossistema Microsoft, Serviços de MarTech, Soluções e Serviços de Segurança Cibernética e Serviços de Ecossistema SAP HANA. Ele apoia os analistas líderes no processo de pesquisa e é coautor do relatório de resumo global com tendências e insights de mercado. Gabriel também desenvolve conteúdo de uma perspectiva empresarial. Gabriel está à frente de sua função atual desde 2021. Antes dessa função, trabalhou como consultor de TI, onde adquiriu experiência e capacidade técnica na coleta, análise e apresentação de dados quantitativos e qualitativos. Sua área de especialização inclui indústria, logística e pesquisa de mercado.

IPL Product Owner

Jan Erik Aase

Sócio e Chefe Global – ISG Provider Lens™

O Sr. Aase traz uma vasta experiência na implementação e pesquisa de integração de serviços e gerenciamento de processos de TI e de negócios. Com mais de 35 anos de experiência, ele é altamente qualificado em analisar tendências e metodologias de governança de fornecedores, identificar ineficiências nos processos atuais e assessorar a indústria. Jan Erik tem experiência em todos os quatro lados do ciclo de vida de sourcing e governança de fornecedores - como cliente, analista do setor, provedor de serviços e consultor. Agora, como diretor de pesquisa, analista principal e chefe global da ISG Provider Lens™, ele está muito bem posicionado para avaliar e relatar o estado da indústria e fazer recomendações para empresas e clientes de provedores de serviços.

ISG Provider Lens™

A pesquisa por quadrantes ISG Provider Lens™ é a única avaliação de prestadores de serviços de seu tipo a combinar pesquisa empírica, pesquisa orientada por dados e análise de mercado, com a experiência e observações do mundo real da equipe de consultoria global do ISG. As empresas encontrarão uma riqueza de dados detalhados e análises de mercado para ajudar a orientar sua seleção de fornecedores de serviços apropriados, enquanto os consultores do ISG utilizam os relatórios para validar seu próprio conhecimento de mercado e fazer recomendações às empresas clientes do ISG. A pesquisa atualmente abrange fornecedores que oferecem seus serviços globalmente. Para mais informações sobre a pesquisa ISG Provider Lens™, visite esta página da web.

ISG Research™

A ISG Research™ fornece pesquisa por assinatura, consultoria recomendatória e serviços de eventos executivos com foco em tendências do mercado e tecnologias disruptivas causando mudanças na computação corporativa. A ISG Research™ entrega diretrizes que ajudam negócios a acelerar o crescimento e criar mais valor comercial.

Para mais informações sobre as assinaturas da ISG Research, envie um e-mail para contact@isg-one.com, ligue para +1.203.454.3900 ou visite research.isg-one.com.

ISG

O ISG (Information Services Group) (NASDAQ: III) é uma empresa líder mundial em pesquisa e consultoria tecnológica. Um parceiro comercial confiável para mais de 800 clientes, incluindo 75 das 100 maiores empresas do mundo, o ISG está comprometido em ajudar corporações, organizações do setor público e provedores de serviços e tecnologia a alcançar excelência operacional e crescimento mais rápido. A empresa é especializada em serviços de transformação digital, incluindo automação, analytics de nuvens e dados; consultoria em sourcing; governança gerenciada e serviços de risco; serviços de operadoras de rede; estratégia tecnológica e projeto de operações; gerenciamento de mudanças; inteligência de mercado e pesquisa e análise de tecnologia. Fundado em 2006, e sediado em Stamford, Connecticut, o ISG emprega mais de 1.300 profissionais operando em mais de 20 países - uma equipe global conhecida por seu pensamento inovador, influência de mercado, profunda experiência na indústria e tecnologia, e capacidade de pesquisa e análise de classe mundial com base nos dados de mercado mais abrangentes da indústria. Para mais informações visite www.isg-one.com.

ISG Provider Lens™

JULHO 2022

REPORT: CYBERSECURITY – SOLUTIONS AND SERVICES