ISG Provider Lens™

Cybersecurity – Solutions and Services

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

QUADRANT REPORT | JULHO DE 2022 | BRASIL

Customized report courtesy of:

LOGICALIS
Architects of Change

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

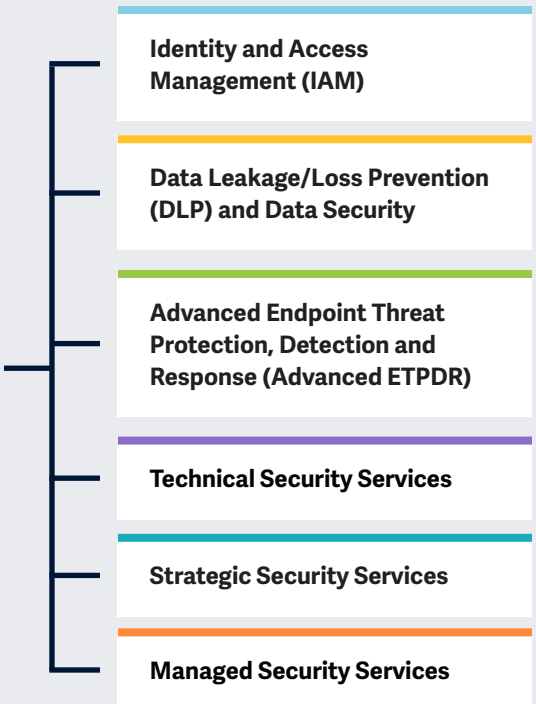
Posicionamento do Provedor

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.

Identity and Access Management (IAM)

Quem deve ler este relatório

Este relatório é relevante para empresas de todos os setores do Brasil, visando avaliar as soluções dos fornecedores que integram diversos recursos de segurança cibernética e que lidam com as preocupações causadas por mudanças nos padrões de trabalho e aumento da digitalização.

Neste relatório, o ISG destaca o posicionamento atual do mercado de fornecedores de soluções de gerenciamento de identidade e acesso (IAM) que reduzem as ameaças de segurança para empresas no Brasil, avaliando como cada fornecedor lida com os principais desafios.

Serviços financeiros, varejo, telecomunicações e mídia são os principais setores do Brasil que adotam soluções de segurança. Os fornecedores de IAM que permitem o controle de acesso adaptável, sensível ao contexto e uma arquitetura *zero trust*, são os preferidos pelas empresas.

As jornadas de migração para a nuvem de muitas empresas foram aceleradas pela pandemia da Covid-19, uma vez que o número de funcionários trabalhando de forma remota aumentou drasticamente neste período. Como os colaboradores precisavam de acesso além do perímetro de rede convencional, diversas companhias que dependiam de sistemas de IAM locais foram obrigadas a considerar opções baseadas em nuvem. Para atender às demandas do ambiente de trabalho moderno, as empresas se concentram nos recursos de IAM gerenciados em nuvem, exigindo a implantação de produtos que funcionam em várias instalações remotas.

Diretores de segurança da informação devem ler este relatório para entender como os fornecedores de soluções de IAM lidam com os desafios significativos de conformidade e segurança, ao mesmo tempo em que mantêm a experiência perfeita para clientes corporativos

Diretores Executivos de dados/ Diretores de Privacidade de dados (CDO/DPO) devem ler este relatório para entender como o fornecedor oferece proteção e privacidade de informações, governança de informações, qualidade de dados e gerenciamento do ciclo de vida de dados

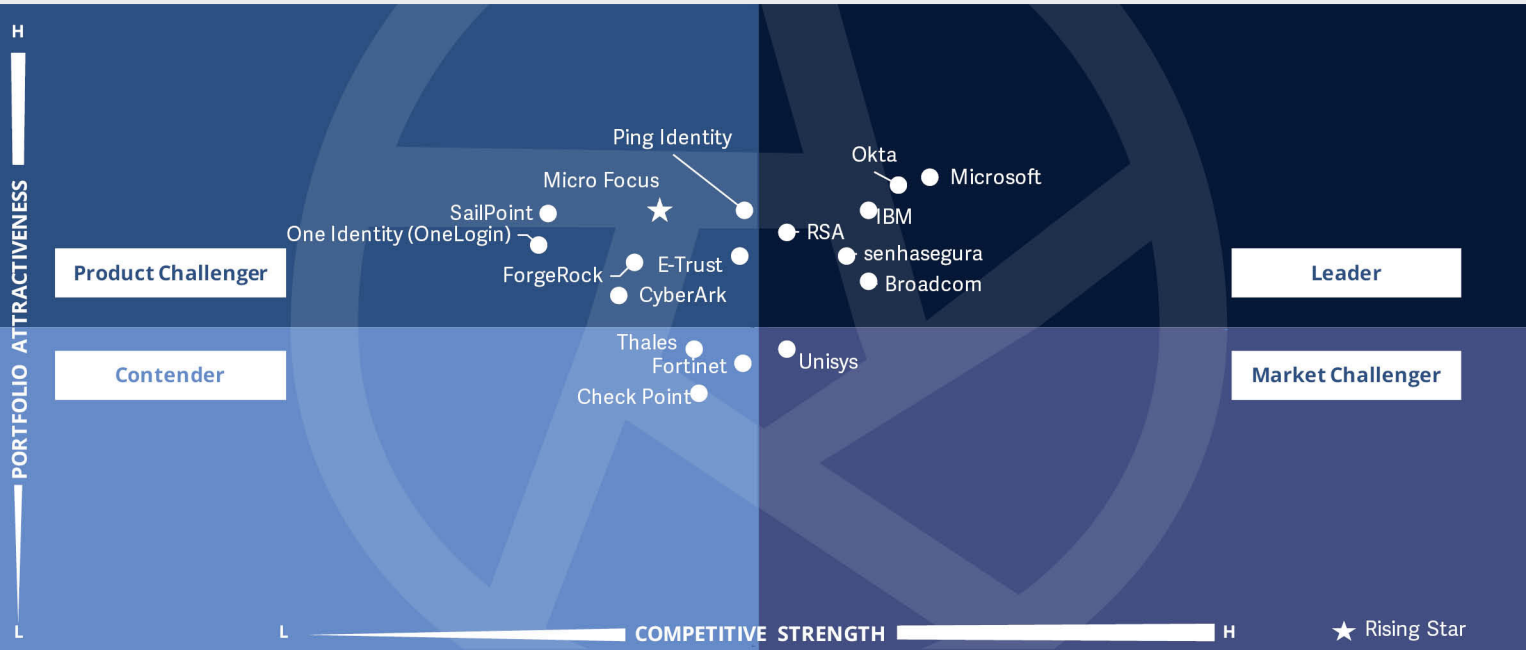
Diretores de estratégia devem ler este relatório para entender o vasto potencial dos fornecedores de soluções para diferenciá-los, atendendo melhor às crescentes demandas dos clientes.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity - Solutions and Services
Identity and Access Management (IAM)

Brazil 2022



Este quadrante avalia os fornecedores de soluções de IAM caracterizados por sua capacidade de oferecer software e serviços associados para **atender à demanda de gerenciamento seguro de identidades, dispositivos e usuários.**

Sergio Rezende

Definição

Os fornecedores e provedores de soluções de IAM são caracterizados por sua capacidade de oferecer software proprietário e serviços associados para atender à demanda exclusiva de gerenciamento seguro de identidades e dispositivos de usuários corporativos. Este quadrante também inclui software como serviço baseado em software proprietário. Provedores de serviços puros que não oferecem um produto IAM (on-premises e/ou nuvem) baseado em software autodesenvolvido não estão incluídos aqui. Dependendo dos requisitos organizacionais, essas soluções podem ser implantadas de várias maneiras, como local, na nuvem (gerenciada pelo cliente), modelo como serviço ou uma combinação dos dois.

As soluções IAM visam coletar, registrar e administrar identidades de usuários e direitos de acesso relacionados, bem como acesso especializado a ativos críticos, incluindo gerenciamento de acesso privilegiado (PAM). Eles garantem que os direitos de acesso sejam concedidos com base em políticas definidas. Para lidar com os requisitos de aplicativos novos e existentes, as soluções de IAM são cada vez mais incorporadas a mecanismos, estruturas e automação seguros (por exemplo, análises de risco) em seus conjuntos de gerenciamento para fornecer funcionalidades de perfil de ataque e usuário em tempo real. Os provedores de soluções também devem fornecer recursos adicionais relacionados a mídias sociais e usuários móveis para atender às suas necessidades de segurança que vão além do gerenciamento tradicional de direitos relacionados à Web e ao contexto. O Machine Identity Management também está incluído aqui.

Critérios de Eligibilidade

Relevância (**receita e número de clientes**) como fornecedor de produtos IAM no respectivo país.

As ofertas de IAM devem ser baseadas **em software proprietário** e não em software de terceiros. A solução deve ser capaz de ser implantada em/ou por meio de uma combinação de modelo local, na nuvem, identidade como serviço (IDaaS) e gerenciado (de terceiros).

A solução deve **ser capaz de ser compatível com autenticação** feita em/ou por uma combinação de login único (SSO), autenticação multifator (MFA), modelos baseados em risco e baseados em contexto.

A solução deve ser capaz de ser compatível com acesso baseado em função e gerenciamento de acesso privilegiado.

O fornecedor de IAM deve ser capaz de **fornecer gerenciamento de acesso** para uma ou mais necessidades corporativas, como nuvem, endpoint, dispositivos móveis, interfaces de programação de aplicativos (APIs) e aplicativos da web.

A solução deve ser **capaz de oferecer compatibilidade** com um ou mais padrões IAM herdados e mais recentes, incluindo, sem limitação: SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust e SCIM.

Para oferecer compatibilidade por meio de acesso seguro, o portfólio deve oferecer um ou mais dos seguintes: soluções de diretório, painel ou gerenciamento de autoatendimento e gerenciamento de ciclo de vida (migração, sincronização e replicação).

Observações

O risco combinado da utilização de dispositivos pessoais e de conexões de Internet domésticas colocou o gerenciamento de identidades e acessos como prioridade para muitas empresas permitirem a utilização remota das suas redes e aplicações por parte de funcionários ou parceiros. Foram muitos os projetos estratégicos que adotaram essa solução para mitigar os riscos trazidos pela adoção repentina do home office, sendo que em muitos casos a solução faz parte de uma estratégia de confiança zero, que vem sendo cada vez mais utilizada para não só limitar acessos indevidos internos como para impedir certos movimentos laterais no caso do acesso não autorizado. Além deste fator de impulso, o mercado de IAM vem ganhando força devido as políticas de BYOD, expansão do IoT e digitalização das empresas, especial-mente aquelas que estão migrando de on premises para a nuvem.

As soluções de IAM tiveram grande evolução, a ponto de as empresas anunciarem a obsolescência do uso de senhas. Anos atrás, senhas funcionavam combinadas com um nome de usuário; agora, deixaram de ser a única forma de autenticação, porque as modernas soluções têm a possibilidade de utilizar múltiplos fatores de autenticação para os usuários.

Estratégias ainda mais sofisticadas podem se utilizar das mais diversas variáveis que caracterizam, definem e identificam um usuário em particular - incluindo aquelas associadas à sua biometria.

Dos 101 fornecedores de produtos e de serviços avaliados neste estudo, 17 se qualificaram para este quadrante, sendo que seis foram nomeados Líderes e um foi nomeado Rising Star.

Broadcom

Broadcom, forte provedor da solução por meio do portifólio de produtos Symantec. Seus parceiros comerciais estão treinados e habilitados para garantir níveis elevados de suporte e rapidez no atendimento aos clientes.

IBM

IBM, com forte portfólio baseado no Security Verify, sua plataforma de identity-as-a service, atende identidades de usuários privile¬giados. A empresa vem progressivamente implantando novos recursos e acrescentando suporte com a ampliação do número de colaboradores.

Microsoft

Microsoft apresenta progresso neste espaço ao apostar em estratégias de autenticação, inclusive sem senha, para seu sistema operacional, plataformas de nuvem e aplicações de escritório, desenvolvendo soluções que podem ser utilizadas por usuários, aplicativos e dispositivos.

Okta

Okta, presente em gerenciamento de identidade de força de trabalho e agora com a aquisição da Auth0, especializada em IAM para consumidores, se torna forte em ambos mercados.

RSA

RSA, entrega solução de IAM para milhões de clientes e ganhou força nos últimos anos, depois de ser vendida pela Dell. A empresa continua recebendo investimentos da sua empresa holding, o ClearLake Capital Group.

senhasegura

senhasegura, fornece soluções PAM e evoluiu seu produto para IAM, de modo poder fornecer acesso remoto seguro dentro do conceito zero trust e sem a necessidade de utilização de VPN aos seus clientes.

Micro Focus

Micro Focus, entrega solução em uma única estrutura que atende todas as necessidades de autenticação com administração simplificada e aplicação de políticas. Estende o MS Azure MFA com liberdade para adotar ampla variedade de tipos de autenticação e acesso seguro em todo um mix de aplicativos e serviços.

Data Leakage/Loss Prevention (DLP) and Data Security

Quem deve ler este relatório

Este relatório é relevante para empresas de todos os setores do Brasil, visando avaliar as soluções dos fornecedores que integram diversos recursos de segurança cibernética e que lidam com as preocupações de segurança causadas por mudanças nos padrões de trabalho e aumento da digitalização.

Neste relatório, o ISG destaca o posicionamento atual do mercado de fornecedores de soluções de prevenção de perda de dados (DLP) e de segurança de dados que reduzem as ameaças para empresas no Brasil, e de que forma cada fornecedor lida com os principais desafios.

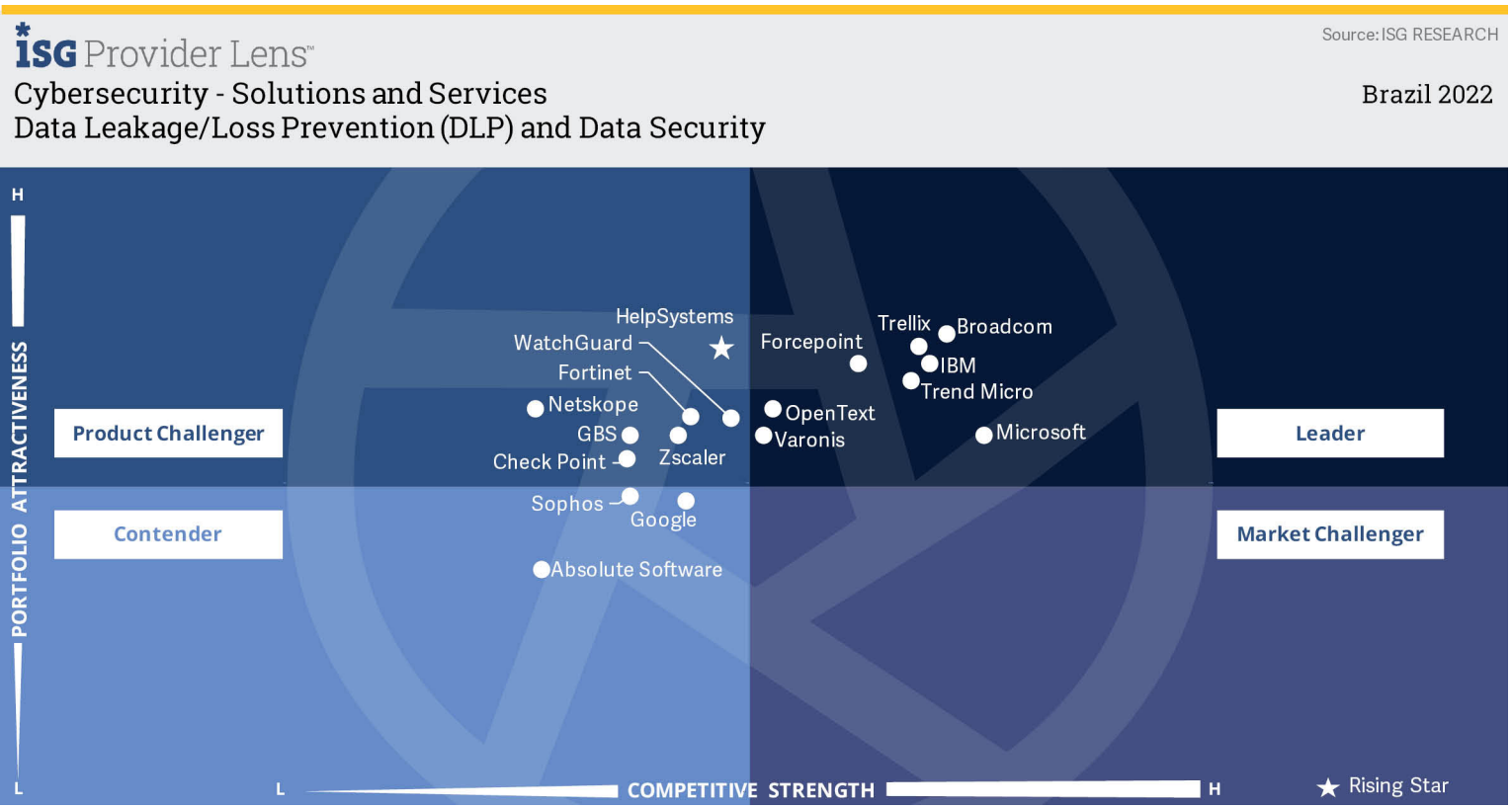
Com a migração para um ambiente de trabalho remoto em decorrência da pandemia, as empresas ao redor do mundo aumentaram o investimento em serviços em nuvem. As organizações continuam a adotar soluções DLP para proteger seus dados e cumprir medidas de segurança.

Com o preocupante aumento no número de casos de vazamento de dados das organizações, as empresas nacionais buscam por soluções DLP em nuvem que protejam seus dados, assim como os dados de seus clientes, e que estejam de acordo com a Lei Geral de Proteção de Dados.

Diretores de segurança da informação devem ler este relatório para entender como os fornecedores de soluções de DLP lidam com os desafios significativos de conformidade e segurança, ao mesmo tempo em que mantêm a experiência perfeita para clientes corporativos

Diretores Executivos de dados/ Diretores de Privacidade de dados (CDO/DPO) devem ler este relatório para entender como o fornecedor oferece proteção e privacidade de informações, governança de informações, qualidade de dados e gerenciamento do ciclo de vida de dados

Diretores de estratégia devem ler este relatório para entender o vasto potencial dos fornecedores de soluções para diferenciá-los, atendendo melhor às crescentes demandas dos clientes.



Este quadrante avalia os fornecedores de soluções de DLP caracterizados por sua capacidade de **oferecer software e serviços associados para identificar e monitorar dados confidenciais, fornecer acesso apenas para usuários autorizados e evitar vazamento de dados.**

Sergio Rezende

Definição

Os fornecedores e provedores de soluções de DLP 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 DLP (local ou baseado na nuvem) com base em software desenvolvido por conta própria não estão incluídos aqui. As soluções DLP são ofertas que podem identificar e monitorar dados confidenciais, fornecer acesso apenas para usuários autorizados e evitar vazamento de dados. As soluções de fornecedores no mercado são caracterizadas por uma combinação de produtos capazes de fornecer visibilidade e controle sobre dados confidenciais que residem em aplicativos em nuvem, endpoint, rede e outros dispositivos.

Essas soluções devem ser capazes de descobrir dados confidenciais, aplicar políticas, monitorar o tráfego e melhorar a conformidade dos dados. Elas estão ganhando uma importância considerável à medida que ficou mais difícil para as empresas controlar as movimentações e transferências de dados. O número de dispositivos, inclusive móveis, que são usados para armazenar dados está aumentando nas empresas. Quase sempre, esses dispositivos estão equipados com conexão à Internet e podem enviar e receber dados sem passar por um gateway central de Internet. Os dispositivos contam com várias interfaces, como portas USB, Bluetooth, rede local sem fio (WLAN) e comunicação de campo próximo (NFC), que permitem o compartilhamento de dados. As soluções de segurança de dados protegem os dados contra acesso não autorizado, divulgação ou roubo.

Critérios de Eligibilidade

1. Relevância (**receita e número de clientes**) como fornecedor de produtos DLP no respectivo país.
2. A oferta de DLP deve ser baseada em **software proprietário** e não em software de terceiros.
3. A solução deve ser **compatível com DLP em qualquer arquitetura**, como nuvem, rede, arma¬zenamento ou endpoint.
4. A solução deve ser capaz de lidar com a proteção de dados confidenciais em **dados estruturados ou não estruturados, texto ou dados binários.**
5. A solução deve ser oferecida com **compatibilidade com gerenciamento básico,** incluindo sem limitação: relatórios, controles de política, instalação e manutenção e funcionalidades avançadas de detecção de ameaças.

Observações

A tecnologia de DLP é utilizada para gerenciar todos os tipos de dados que se encontram em um determinado ambiente, permitindo que sejam identificados e classificados segundo políticas objetivas e nítidas, que definem quem pode acessá-los, manuseá-los ou transferi-los, por exemplo. Para isso, todos os arquivos, pastas e bancos de dados são vasculhados pelas soluções de DLP para a localização de ativos que só possam ser utilizados com a obediência a regras de segurança rígidas, e cujas tentativas de violação, além de serem bloqueadas, produzem alertas para as áreas interessadas. O objetivo é impedir qualquer possibilidade de acesso não autorizado a dados críticos, que possam de alguma forma comprometer a companhia, seus usuários, clientes ou parceiros, seja de forma acidental ou intencional.

Atualmente, existe grande variedade de soluções de DLP. Entre as mais utilizadas estão as de fornecedores que vêm oferecendo recursos avançados como Aprendizado de Máquina (ML) e Inteligência Artificial (IA). Esses novos recursos ajudam os gestores a mapear e classificar os dados, assim como a definir melhor os processos que devem ser utilizados em cada caso. Ter um geren¬ciamento centralizado, independentemente do tipo de ambiente (cloud ou on premises) também ajuda o responsável a administrar as políticas necessárias dentro do âmbito de DLP. Outra característica dessas ferramentas é que elas oferecem facilidade de integração para trabalharem em conjunto com outras soluções de segurança.

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

Broadcom

Broadcom: ao adquirir a empresa Bay Dynamics, a Broadcom mais uma vez ampliou seu portfólio de segurança e de prevenção de perda de dados. O software de análise comportamen¬tal de riscos da nova empresa adquirida complementa as soluções da linha Symantec para Data Loss Prevention (DLP).

Forcepoint

Forcepoint: recém adquirida pela firma de private equity Francisco Partners, a Forcepoint redesenhou sua operação no Brasil e ampliou seu quadro de funcionários, tendo agora quase o triplo do que havia antes da aquisição. O reforço resultou na conquista de novas contas e numa previsão de 50% de aumento da receita para 2021.

IBM

IBM: a empresa aprimorou suas estratégias de prevenção da perda de dados, especialmente com o fornecimento de novos serviços criptográficos, aumentando assim o grau de privacidade e a segurança de conformidades regulatórias. Sua receita em serviços e produtos de segurança está em crescimento.

Microsoft

Microsoft: no último ano, apresentou sua solução de DLP, inicial¬mente para os ambientes de nuvem e aplicações como o Office 365. Dois anos atrás, já havia ampliado o alcance da solução para todos os produtos Microsoft, incluindo Exchange, Sharepoint, Teams e compartilhamentos locais do Windows.

OpenText

OpenText: fortificou sua posição de mercado ao adquirir no início de 2020 a empresa Xmedius. A OpenText já fez 44 aquisições e permanece como um sólido fornecedor de soluções de segurança, com 14 mil funcionários e receita de US$ 3,15 bilhões em 2020.

Trend Micro

Trend Micro: reforçou sua posição como fornecedor de soluções de segurança em DLP, ampliando o número de logos no Brasil e a receita em relação ao ano fiscal anterior, num mercado que ganhou força por causa do início de vigência da Lei Geral de Proteção de Dados no país.

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, que foi ampliada com a aquisição da Lightpoint Security, empresa que desenvolveu um browser com segurança aprimorada.

Varonis

Varonis: é um fornecedor cuja presença cresce graças à sua rede de parceiros no país e à divulgação do seu conceito de gestão da segurança em 360 graus. Também ganhou novos clientes que buscam proteção contra a perda de dados, impulsionados pelas exigências da nova legislação brasileira.

HelpSystems

HelpSystems: ganhou mais espaço no setor de proteção de dados ao adquirir as empresas Titus e Boldon James. Nos últimos anos a HelpSystems já fez outras dez aquisições, tornando-se um robusto fornecedor de soluções de segurança para redes em ambientes híbridos.

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.

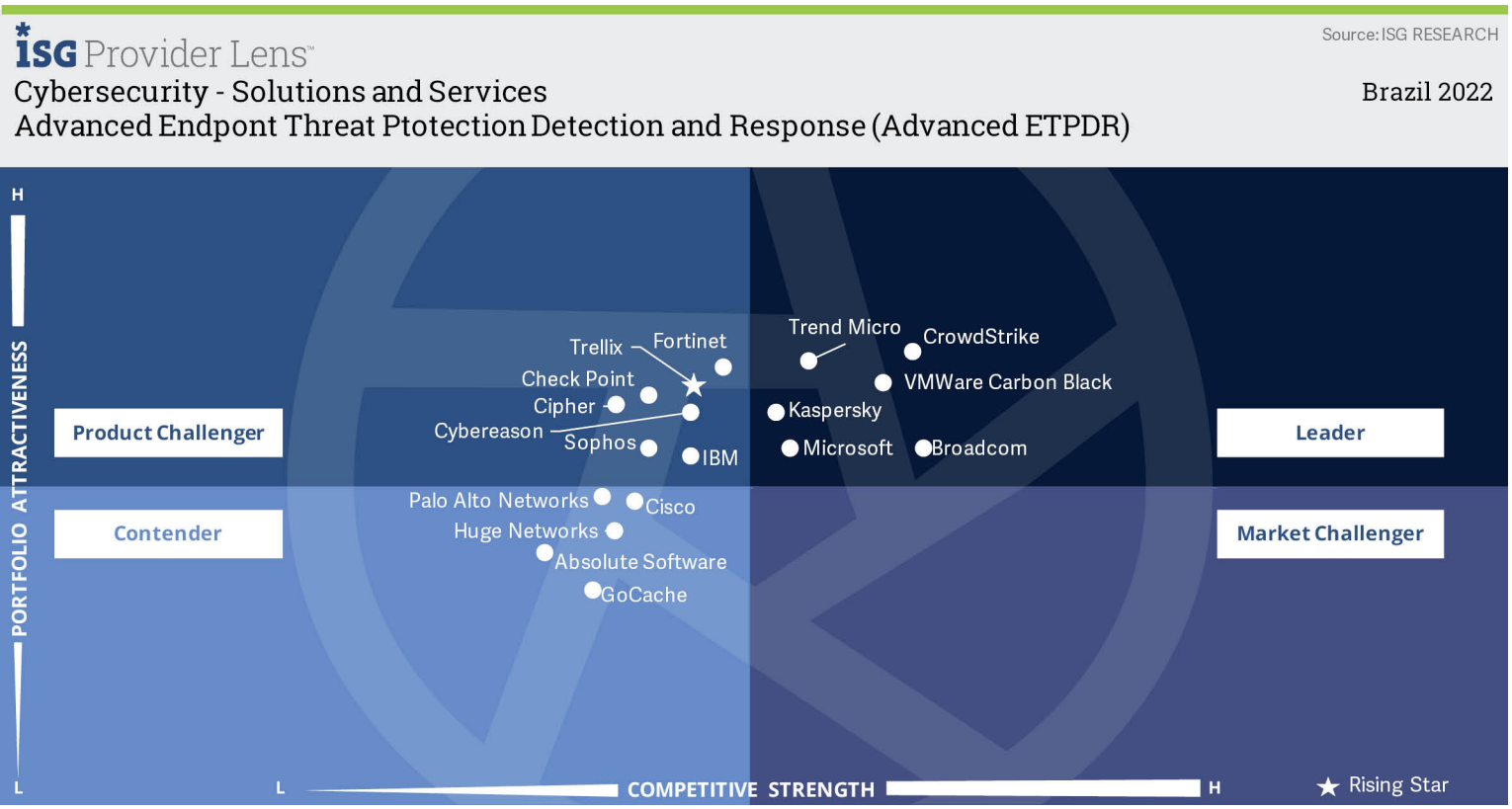
Neste relatório, o ISG destaca o posicionamento de mercado atual dos fornecedores de produtos avançados para ameaça de *endpoint* voltado às empresas no Brasil, e como cada fornecedor lida com os principais desafios enfrentados na região.

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.

Technical Security Services

Quem deve ler este relatório

Este relatório foi elaborado para ajudar empresas do Brasil de todos os setores a avaliar fornecedores que não têm foco exclusivo em seus respetivos produtos proprietários e que, em vez disso, implementam e integram produtos ou soluções de outros fornecedores de serviços de segurança de TI.

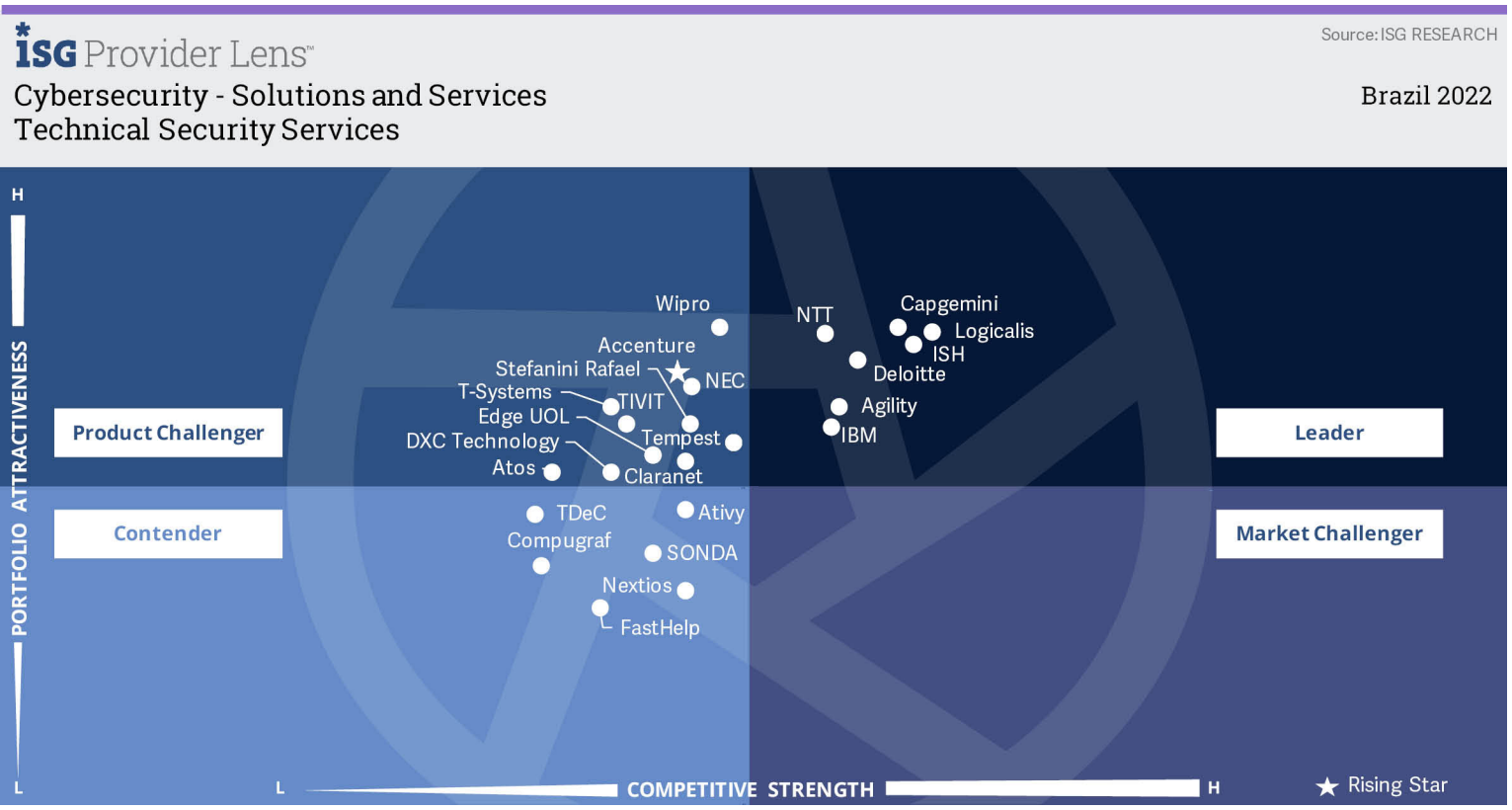
Neste relatório, o ISG define o atual posicionamento de mercado dos fornecedores que implementam e integram serviços de segurança de TI no Brasil, descrevendo como cada fornecedor lida com os principais desafios. Especificamente, as empresas avaliam se a implementação do serviço pode combater as técnicas de ataque mais recentes. Usando os conjuntos de serviços oferecidos pelos fornecedores, as organizações podem se preparar para se defender de ataques e responder rapidamente a ameaças que colocam em risco suas informações confidenciais.

As principais tarefas de implementação ou integração incluem proteção contra ransomwares e malwares e, considerando o aumento drástico das ameaças cibernéticas, os serviços técnicos de segurança estão em alta demanda no Brasil. No entanto, cada cliente tem suas prioridades em relação a estruturas, segurança, escalabilidade, entre outros. As empresas no Brasil estão vulneráveis a ameaças virtuais devido a seus frágeis sistemas de segurança, a falta de recursos qualificados e de preparação das empresas para lidar com as ameaças. Para prever e combater as ameaças cibernéticas, há a necessidade de investir em treinamento contínuo, identificação e implementação de serviços em potencial.

Diretores de segurança de informações devem ler este relatório para terem uma visão dos principais fornecedores de serviços do mercado que ajudam na integração de serviços de segurança de TI. Com a transformação digital na vanguarda dos negócios de hoje, os executivos devem encontrar um equilíbrio entre segurança de dados, experiência do cliente e privacidade.

Diretores de Estratégia devem ler este relatório para entender o posicionamento relativo e os recursos dos fornecedores de serviços, colaborando para desenvolver um serviço de segurança cibernética eficaz. Este relatório contém informações que podem ser usadas para implementar uma estratégia de proteção de dados.

Analistas de segurança devem ler este relatório para entenderem como os fornecedores aderem às leis de segurança e proteção de dados no Brasil, mantendo-se à frente das próximas tendências do mercado e para se prepararem para utilizar todos os serviços disponíveis.



Este quadrante avalia os fornecedores de soluções de Serviços Técnicos de Segurança (TSS) caracterizados por **sua capacidade de implementar e integrar produtos ou soluções de outros fornecedores.**

Sergio Rezende

Definição

Este quadrante examina os provedores de serviços que não têm um foco exclusivo em seus respectivos produtos proprietários e podem implementar e integrar produtos ou soluções de outros fornecedores.

Os TSS cobrem integração, manutenção e suporte para produtos ou soluções de segurança de TI. Os TSS abordam todos os produtos de segurança, incluindo antivírus, nuvem e segurança de data center, IAM, DLP, segurança de rede, segurança de ponto de extremidade, gerenciamento unificado de ameaças (UTM) e outros.

Critérios de Eligibilidade

1. Demonstrar **experiência na implementação** de soluções de segurança para empresas no respectivo país.
2. Não focado exclusivamente em **produtos proprietários**.
3. Autorizado por fornecedores para distribuir e **oferecer suporte** a soluções de segurança.
4. **Especialistas certificados** para apoiar suas tecnologias de segurança.
5. Capacidade de participar (desejável, não obrigatório) em **associações de segurança locais e agências de certificação**.

Observações

O mercado brasileiro pode ser considerado maduro em termos de quantidade e qualidade dos prestadores de serviços técnicos de segurança: eles existem em grande quantidade em todo o país, disponíveis em grande variedade de especialidades e estrutura de atendimento.

Os serviços são prestados em muitas modalidades, que incluem desde instalações de software e dispositivos, abrangendo ainda atualizações e treinamentos, por exemplo, mas que podem se estender para outras atividades, entre elas alocação de mão de obra para o dia-a-dia de segurança cibernética ou serviços específicos, como testes de penetração. Serviços de análise de maturidade e de resistência ou resiliência da empresa são também prestados e enriquecidos com a alocação de "blue teams" (para defesa) e "red teams" (para os ataques), e com a organização de cursos, workshops e simulações para elevar o nível de alerta dos funcionários, reduzindo assim a possibilidade de que sejam vítimas de ataques de phishing ou fraudes.

As empresas que prestam os serviços técnicos de segurança são em geral parceiras dos fornecedores de soluções e serviços estratégicos, sendo muitas vezes o principal ponto de contato do provedor com o cliente, quando não parcialmente responsáveis pelas vendas, contando com mão de obra qualificada e certificada para atender empresas mais exigentes ou cuja atividade esteja sujeita a supervisão de agências reguladoras.

Dos 101 fornecedores de produtos e serviços avaliados neste estudo, 24 se qualificaram para este quadrante, sete foram nomeados Líderes e um foi nomeado Rising Star.

Agility Networks

Agility Networks: com mais de 30 anos de operação e com uma carteira de mais de 180 clientes, sendo metade em contratos de receita recorrente – estando entre esses clientes os principais Bancos e as maiores operadoras brasileiras de telecomunicações. Tem uma equipe de 180 pessoas e 25 premiações recebidas de vendors de primeira linha.

Capgemini

Capgemini: apresentou crescimento de receitas oriundas de serviços principalmente no segundo semestre de 2020, após re¬tração no primeiro semestre devido à pandemia da Covid-19. Muitos negócios foram impulsionados pela vigência da nova lei de proteção de dados pessoais, que levaram a um aumento de 20% no número de funcionários full time do time de segurança no Brasil.

Deloitte

Deloitte: a consultoria continua com forte atuação em segurança no país, graças a serviços técnicos diferenciados para corporações, como cyber wargaming e resposta a incidentes cibernéticos, que incluem a investigação de crimes e incidentes. Adquiriu em 2020 a empresa SecurePath, especializada em segurança de dados com blockchain.

IBM

IBM: o time de serviços da empresa cresceu nos últimos 12 meses para reforçar o atendimento dos clientes em projetos de hardening de segurança, entre eles os de implementação de estratégias críticas como zero trust e outsourcing de serviços por meio do IBM Security Services.

ISH Tecnologia: a empresa havia feito uma previsão de crescimento de receita de 20% para 2020, mas o crescimento alcançou 41% em relação a 2019, com acréscimo de novos clientes, aumento de 40% no número de funcionários e ampliação nas iniciativas de educação corporativa para retenção de talentos.

NTT Ltd

NTT Ltd: ampliou a equipe de segurança cibernética com novos talentos, opera com alto volume de certificações, equipe multidisciplinar e obteve novos clientes nos setores finan-ceiro, de telecomunicações, utilities, saúde e varejo.

Logicalis: agora com mais de 500 clientes no Brasil, tem presença em todo o país e continua forte em parcerias de tecnologia. Mesmo durante a recessão econômica causada pela pandemia da Covid-19, obteve novos clientes e pôde anunciar crescimento.

Accenture: o time em serviços de implementação e integração também cresceu, acompanhando as áreas de SSS e MSS em 2021 para entrega da segurança cibernética no Brasil. O crescimento tem suporte nas parcerias globais com os principais provedores de segurança e os maiores CSPs do mercado.

Logicalis

Leader

"A Logicalis entrega soluções de cibersegurança aos seus clientes atuando com os maiores parceiros e principais especialistas do mercado."

Sergio Rezende

Visão Geral

A Logicalis está sediada em Slough, Reino Unido, e opera em 27 países. Como prestadora de serviços, possui mais de 6.400 funcionários em 76 escritórios globais. No FY21, a empresa gerou US$ 1,4 bilhão (-13,8% A/A) em receita, com o produto como seu maior segmento. A Logicalis é uma empresa global especializada em serviços de consultoria na tecnologia para negócios, computação em nuvem, cibersegurança, internet das coisas (IoT), analytics & big data / inteligência artificial e gerenciamento de serviços.

Pontos Fortes

Serviços: adaptáveis e fáceis de gerenciar, este é a abordagem dos serviços de segurança para a empresa. Metodologia, processos, gestão de risco fazem parte da estratégia de segurança e trabalham sincronizadamente em benefício do cliente.

Integrações: a Logicalis tem a capacitação de integrar soluções multivendor através de seus profissionais qualificados. Estes são orientados por planejamento e definições de arquitetura tornando-os viáveis para os desdobramentos da tecnologia.

Estratégia: planejamento estratégico de segurança da informação através de avaliações de todo o ambiente de TI com gerenciamento de risco, avaliação de vulnerabilidades e testes de penetração da Logicalis. Aplicação de melhores práticas, mapeamento processos de negócio conectados com a tecnologia do cliente.

Ponto de Atenção

Engajada na jornada de transformação digital de seus clientes, a Logicalis precisa estar alinhada com as estratégias de tecnologia de seus parceiros para o crescimento conjunto das empresas.

Strategic Security Services

Quem deve ler este relatório

Este relatório é relevante para empresas de todos os setores do Brasil, avaliando fornecedores de consultoria para segurança de TI e TO que não se concentram exclusivamente em produtos ou soluções proprietárias.

Neste relatório de quadrantes, a ISG define o posicionamento atual do mercado de fornecedores de serviços de segurança estratégica no Brasil e como cada fornecedor lida com os principais desafios enfrentados na região. Os serviços estratégicos auxiliam as empresas na transformação de segurança cibernética por meio de auditorias, consultorias e treinamentos.

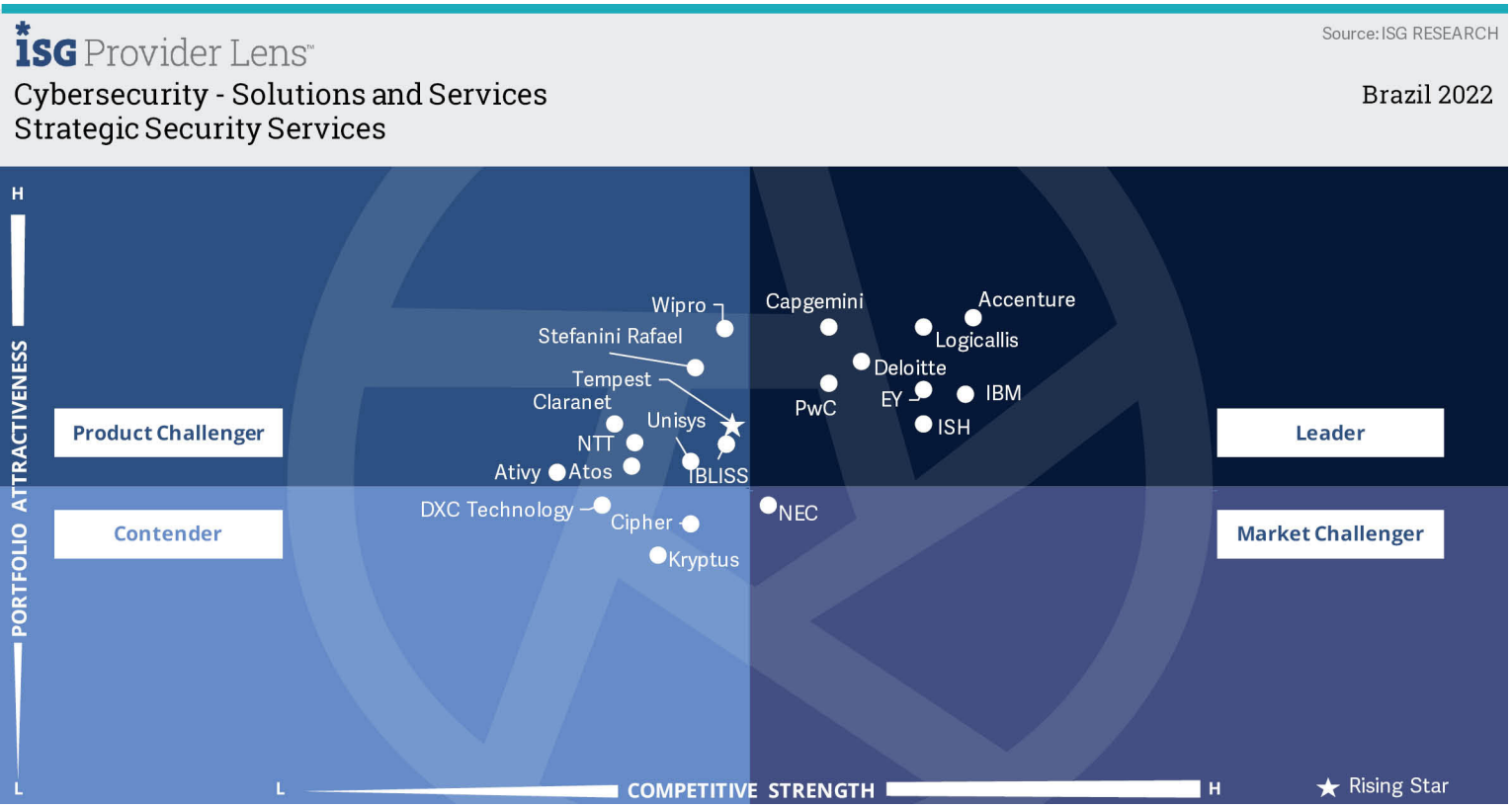
Com o crescimento do trabalho remoto por conta da Covid-19 e a crescente onda de ataques cibernéticos, as empresas têm buscado se proteger de maneira proativa e não apenas reativa. Assim, o volume de serviços estratégicos de segurança cibernética tem aumentado consideravelmente no Brasil.

Tratando-se de segurança cibernética, as empresas buscam por um fornecedor em que possam confiar. Para o mercado intermediário, que geralmente não possui uma equipe dedicada exclusivamente à segurança cibernética, a contratação de consultorias em segurança é uma maneira de criar essa relação de confiança com o fornecedor que, por sua vez, busca conscientizar seus clientes sobre a necessidade de serviços de segurança cibernética. Por outro lado, grandes empresas buscam por fornecedores que supram suas necessidades com uma equipe grande e altamente qualificada, recursos avançados, vastos portfólios e presença global.

Diretores de Segurança da Informação devem ler este relatório para 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, o relatório 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 serviços de segurança estratégica 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 Serviços Estratégicos de Segurança (SSS) caracterizados por sua capacidade de **oferecer serviços de consultoria** para segurança de TI.

Sergio Rezende

Definição

Os SSS cobrem principalmente consultoria para segurança de TI. Alguns dos serviços cobertos neste quadrante incluem auditorias de segurança, serviços de consultoria de conformidade e risco, avaliações de segurança, consultoria de arquitetura de solução de segurança e conscientização e treinamento. Esses serviços são usados para avaliar a maturidade da segurança, postura de risco e definir a estratégia de segurança cibernética para empresas. Este quadrante examina os provedores de serviços que não têm foco exclusivo em produtos ou soluções proprietários. Os serviços aqui analisados abrangem todas as tecnologias de segurança.

Critérios de Eligibilidade

1. Os provedores de serviços devem demonstrar habilidades em áreas de SSS, como avaliação, apurações, seleção de fornecedores, **consultoria de arquitetura e consultoria de risco**.
2. Os provedores de serviço devem oferecer pelo menos um dos SSS acima no respectivo país.
3. A execução de serviços de **consultoria de segurança usando frameworks** será uma vantagem.
4. Sem foco exclusivo em produtos ou **soluções proprietárias**.

Observações

A segurança da informação está hoje no topo da lista de prioridades dos CEOs e dos conselhos de administração. Na era da conectividade e do consumo digital, ela se tornou determinante no rumo e no futuro das corporações, deixando de ser um assunto da área de tecnologia da informação para se tornar um tema estratégico, que viabiliza, garante e potencializa o negócio. Não é à toa que se vê, cada vez mais, áreas de segurança se tornando independentes da área de TI, com os CISOs e CSOs cada vez mais se reportando direto ao conselho das empresas ou ao CEO.

A resposta a esse desafio está vindo sob a forma de projetos estratégi¬cos e planos diretores de segurança cibernética: as consultorias têm atualmente boa quantidade de projetos em andamento, auxiliando cli¬entes antigos e novos no processo de adequação a essa nova realidade, algumas vezes em meio a uma transformação digital acelerada.

As próprias consultorias, especialmente as grandes, fizeram no último ano investimentos bilionários em transformações para agregar valor e novos serviços em combinação com os seus projetos.

O mercado de serviços estratégicos de segurança sofreu super¬aquecimento no primeiro semestre de 2020, por causa da intensa migração de funcionários para o trabalho em home office.

Esse conjunto de desafios disparou uma demanda não só por projetos como também pelas ações necessárias à implantação de cada um, o que pode ser traduzido em serviços técnicos e aquisição de novos produtos e serviços.

Dos 101 fornecedores de produtos e de serviços avaliados neste estudo, 21 se qualificaram para este quadrante, oito foram nomeados Líderes e um foi nomeado Rising Star.

accenture

Accenture: cresceu seu time em serviços de consultoria em 250% em 2021 e agora conta com 42 funcionários em tempo integral para segurança cibernética no Brasil, fornecendo serviços de consultoria fortes, crescendo dois dígitos por ano desde então (incluindo os últimos 12 meses).

Capgemini

Capgemini: obteve novos clientes para projetos de proteção de dados e serviços de segurança estratégica, impulsionados principalmente pela nova lei de proteção de dados do Brasil, a LGPD, que entrou em vigor em 2020.

Deloitte

Deloitte: manteve-se como uma das grandes consultorias e como provedora de variados serviços de segurança cibernética, também agregando projetos de segurança estratégica graças à vigência da Lei Geral de Proteção de Dados.

EY

EY: a empresa anunciou para 2021 investimentos no Brasil da ordem de US$ 1,5 bilhão, principalmente para inovação e qualidade em todos os seus serviços (consultoria, soluções, pessoas) e estabe¬lecimento de um ecossistema mais amplo de alianças estratégicas.

IBM

IBM: a empresa mantém crescente o número de funcionários para serviços estratégicos, apoiando projetos de transformação digital com mapa estratégico de segurança e mantendo especialistas disponíveis para projetos de todos os portes.

ISH: novos clientes na área de serviços estratégicos de segurança ajudaram a empresa a quase dobrar sua receita com serviços de consultoria, levando-a a expandir seu quadro de funcionários e iniciar atividades de trein¬amento através de uma universidade corporativa.

Logicalis: ganhou mercado com serviços estratégicos que podem ser conectados a serviços de implantação e operação, recomendando aos clientes tecnologia de acordo com as necessi-dades deles e expandindo essa metodologia para computação em nuvem. Espera crescer 25% em 2022.

PwC

PwC: a empresa presta serviços de elevada qualidade em consultoria estratégica de segurança e anunciou investimentos de US$ 3 bilhões para a qualificação de seu pessoal.

Tempest

Tempest: vem crescendo 30%, em média, por período, nos últimos cinco anos e tornou-se uma das maiores do país especializada em crimes cibernéticos. Atualmente tem 450 funcionários, sendo 150 deles contratados durante a pandemia. A previsão de faturamento em 2021 foi de R$ 180 milhões.

Logicalis

Leader

"As aquisições realizadas pela Logicalis permitem que ela implemente novas soluções oferecendo uma estratégia de cibersegurança 360º para seus clientes."

Sergio Rezende

Visão Geral

A Logicalis está sediada em Slough, Reino Unido, e opera em 27 países. Como prestadora de serviços, possui mais de 6.400 funcionários em 76 escritórios globais. No FY21, a empresa gerou US$ 1,4 bilhão (-13,8% A/A) em receita, com o produto como seu maior segmento. A Logicalis é uma empresa global especializada em serviços de consultoria na tecnologia para negócios, computação em nuvem, cibersegurança, internet das coisas (IoT), analytics & big data / inteligência artificial e gerenciamento de serviços.

Pontos Fortes

Crescimento: a Logicalis acelera seu crescimento de serviços de segurança. Adquiriu a Kumulus para complementar o seu portfólio de soluções com a expertise em modernização de aplicações e gestão de ambientes de nuvem híbrida. Também realizou a aquisição de participação majoritária da Áudea que provê soluções para clientes nos setores financeiro, automotivo, transporte, hotelaria, bens de consumo, comércio e educação reforçando a capacidade da Logicalis de oferecer um amplo portfólio de serviços para garantir a proteção de dados críticos para os clientes.

Projetos: oferece soluções customizadas para desenho e implementação de projetos de segurança para proteção de redes, dados e aplicativos focando na abordagem focada nas ameaças digitais. Avaliação da Arquitetura de Segurança e criação de roadmap para um cenário seguro também são serviços que diferenciam a empresa.

Parceiras Estratégicas: A Logicallis possui parcerias com os principais fornecedores de tecnologias globais e as utiliza em seus clientes de acordo com sua necessidade e escala. Este fator contribui para construção e robustez de seu Portifólio de serviços.

Ponto de Atenção

O processo de aquisições e integrações de novas empresas não devem reduzir o foco da Logicalis na jornada de transformação digital de seus clientes, buscando sempre criar valor sustentável.

Managed Security Services

Quem deve ler este relatório

Este relatório é relevante para empresas de todos os setores do Brasil, visando avaliar os serviços dos fornecedores que integram diversos recursos de segurança cibernética que abordam as preocupações com a segurança causadas por mudanças nos padrões de trabalho e aumento da digitalização.

Neste relatório, o ISG se concentra no posicionamento atual do mercado de fornecedores de serviços de segurança gerenciados que reduzem as ameaças para empresas no Brasil e como cada fornecedor lida com os principais desafios.

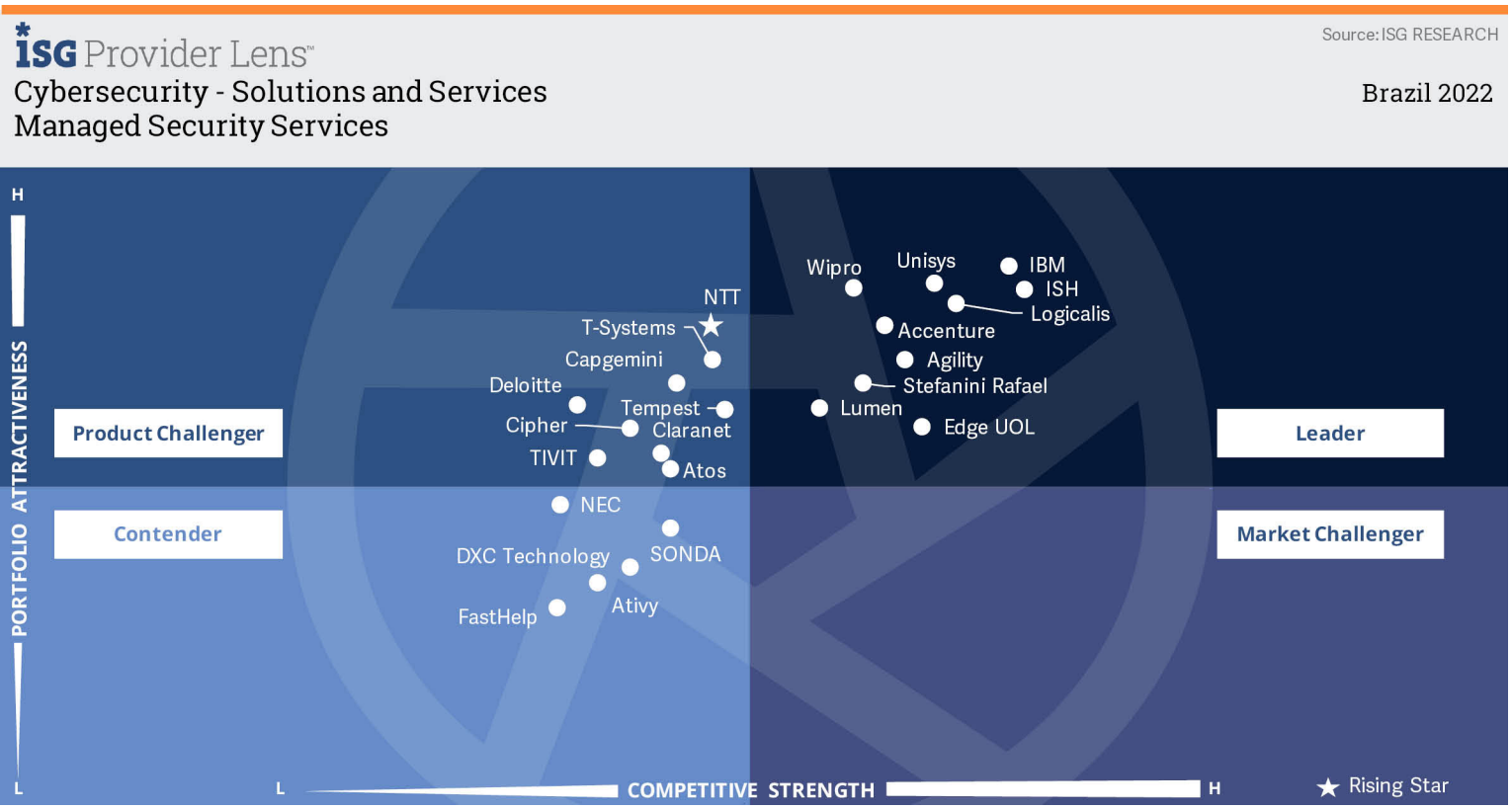
Os problemas de segurança estão afetando as empresas todos os dias, com novas ameaças surgindo com tanta frequência que maneiras mais inteligentes precisam ser implementadas para melhorar e gerenciar as preocupações de segurança. Atualmente, as empresas estão aproveitando as mais recentes tendências de segurança no mercado para aumentar a eficácia e, ao mesmo tempo, reduzir os riscos.

O mercado de serviços de segurança gerenciados no Brasil está crescendo devido ao aumento das violações de segurança, com políticas e leis adequadas sendo implementadas para evitar o aumento de problemas de segurança. No ano passado, as empresas aumentaram suas demandas por centros de operações de segurança virtual (SOC), incluindo plataformas de detecção e resposta gerenciadas (MDR), uma vez que os ataques estão evoluindo rapidamente devido à aceleração dos processos de digitalização.

Diretores de Segurança da Informação devem ler este relatório para uma visão mais ampla das últimas tendências no cenário da segurança. O relatório também 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, trazendo *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 serviços gerenciados de segurança 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 Serviços Gerenciados de Segurança (MSS) caracterizados por sua **capacidade de gerenciar e operar as melhores ferramentas de segurança do mercado**.

Sergio Rezende

Definição

Os MSS compreendem as operações e gerenciamento de infraestruturas de segurança de TI para um ou vários clientes por um centro de operações de segurança (SOC). Os serviços típicos incluem monitoramento de segurança, análise de comportamento, detecção de acesso não autorizado, aconselhamento sobre medidas de prevenção, teste de penetração, operações de firewall, operações de antivírus, serviços de operação de IAM, operações de DLP e todos os outros serviços operacionais para fornecer proteção contínua em tempo real sem comprometer desempenho dos negócios. Este quadrante examina os provedores de serviços que não se concentram exclusivamente em produtos proprietários, mas podem gerenciar e operar as melhores ferramentas de segurança. Esses provedores de serviço podem lidar com todo o ciclo de vida do incidente de segurança, desde a identificação até a resolução.

Critérios de Eligibilidade

1. Capacidade de fornecer serviços de segurança como **detecção e prevenção; segurança da informação e gerenciamento de eventos (SIEM); e consultor de segurança e suporte de auditoria,** remotamente ou localmente no cliente.
2. Relevância (**receita e número de clientes**) como fornecedor de MSS no respectivo país.
3. **Não focado exclusivamente em produtos proprietários,** mas pode gerenciar e operar as melhores ferramentas de segurança da categoria.
4. **Possui credenciamentos** de fornecedores de ferramentas de segurança.
5. Os SOCs de propriedade e **gerenciados idealmente pelo provedor** e não predominantemente por parceiros.
6. Manter uma **equipe certificada,** por exemplo, em Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Global Information Assurance Certification (GIAC), etc.

Observações

O mercado de Managed Security Services vem crescendo no mundo inteiro de maneira acelerada, quando comparado às demais áreas de serviços de segurança cibernética. Ele tem potencial para crescer ainda mais nos próximos anos, conforme indica o ritmo das fusões e aquisições ocorridas nos últimos 12 meses. Há estimativas de que ele valha atualmente US$ 22,5 bilhões e já existem projeções de que o setor fature perto de US$ 60 bilhões anualmente a partir do final de 2026. Daqui até lá, a taxa média de crescimento anual pode ser de 15%.

O fenômeno que impulsiona o crescimento dos serviços gerenciados é a complexidade cada vez maior do gerenciamento da segurança cibernética. O crescimento da variedade e do volume de ameaças exige uma quantidade tão grande de soluções e serviços que acaba produzindo dois efeitos nocivos: por um lado, faz com que a empresa seja obrigada a adquirir e acumular tecnologias que exigem diferentes especialistas, certificações, manutenções e contratos; por outro, esse acúmulo se torna motivo de sobrecarga para as equipes de segurança, porque impõe a elas uma demanda de conhecimento que geralmente é impossível de atender.

Por essa razão, muitas empresas têm optado pela contratação de serviços gerenciados para a cobertura de diversos aspectos da segurança, que vão desde a operação de firewalls e gateways até a utilização de centros de operações de segurança terceirizados.

Dos 101 fornecedores de produtos e de serviços avaliados neste estudo, 24 se qualificaram para este quadrante, dez foram nomeados Líderes e um foi nomeado Rising Star.

accenture

Accenture: depois de contratar mais 100 novos funcionários em tempo integral em 2021 e de ter obtido novos clientes, a Accenture fez no Brasil a aquisição da Real Protect, uma empresa especializada em serviços gerenciados de segurança.

Agility Networks

Agility Networks: possui uma carteira de mais de 180 clientes, estando entre esses clientes os principais Bancos e as maiores operadoras brasileiras de telecomunicações do país. Tem uma equipe de 180 pessoas e 25 premiações recebidas de vendors de primeira linha.

Edge UOL

Edge UOL: com cerca de 1.300 clientes no final do primeiro semestre de 2020, a Compasso UOL se fortaleceu com novos projetos e novos clientes. Seu número de funcionários alcançou ao final do ano o total de 2 mil pessoas, com um total superior a 1.100 certificações e acreditações.

IBM

IBM: a empresa vem adicionando mais funcionários em tempo integral à equipe de serviços gerenciados do Brasil, num time de segurança que tem agora perto de 130 pessoas; conseguiu em 2020 novos clientes e prossegue aperfeiçoando serviços como análise automatizada e a orquestração para resposta imediata a ameaças.

ISH

ISH Tecnologia: o provedor continua expandindo seus serviços gerenciados, adicionando a plataformas para detecção de ameaças, além de ter elevado em dois dígitos a sua receita em relação ao ano anterior.

LOGICALIS
Architects of Change

Logicalis: esse provedor atende uma base de grandes clientes corporativos, cresceu 10% em relação ao ano anterior e apresentou no Brasil novos cases de clientes de segurança cibernética. Seus serviços de nuvem crescem 25% ao ano no Brasil.

LUMEN®

Lumen: com a aquisição da CenturyLink no segundo semestre de 2020, a Lumen reforçou sua posição como prestadora de serviços gerenciados que têm o suporte da sua extensa rede de fibra óptica, presente em mais de 60 países.

Stefanini Rafael

Stefanini Rafael: a empresa integrou dois novos SOCs para ampliar a prestação de serviços gerenciados, inclusive na região EMEA. Sua equipe de trabalho já conta com mais de 100 funcionári¬os em tempo integral e o seu número de clientes dobrou no último ano.

Unisys

Unisys: os serviços gerenciados foram aperfeiçoados com novas ferramentas adicionadas pelos parceiros Securonix, Tenable e Nessus, que se somam ao Stealth®, um dos pilares dos serviços de segurança cibernética da companhia.

Wipro

Wipro: sua operação no Brasil completa 14 anos e foi reforçada com a aquisição da empresa Ivia para ampliar sua capacidade de entregas no país; em março de 2021 a Wipro fez a aquisição da consultoria Capco, sediada em Londres, e em maio de 2021 anunciou a abertura de um centro de inovação também em Londres.

NTT Ltd

NTT Ltd: ampliou a equipe de segurança cibernética com novos talentos, opera com alto volume de certificações, equipe multidisciplinar e obteve novos clientes nos setores finan-ceiro, de telecomunicações, utilities, saúde e varejo.

Logicalis

Leader

"A Logicalis optou por ter os profissionais mais capacitados do mercado para oferecer serviços de MSS altamente especializados aos seus clientes."

Sergio Rezende

Visão Geral

A Logicalis está sediada em Slough, Reino Unido, e opera em 27 países. Como prestadora de serviços, possui mais de 6.400 funcionários em 76 escritórios globais. No FY21, a empresa gerou US$ 1,4 bilhão (-13,8% A/A) em receita, com o produto como seu maior segmento. A Logicalis é uma empresa global especializada em serviços de consultoria na tecnologia para negócios, computação em nuvem, cibersegurança, internet das coisas (IoT), analytics & big data / inteligência artificial e gerenciamento de serviços.

Pontos Fortes

Serviços 24x7: a Logicalis possui 2 Security Operation Centers na América Latina operando em regime 24x7 com serviços de monitoramento e gerenciamento proativo. Reconhecida pelas certificações ISO e processos ITIL, apresenta também Catálogos de serviços gerenciados adaptáveis para: Next-Generation Firewall, Email Security, Web & Content Security e SIEM aos seus clientes.

Customer Success: a Logicalis disponibiliza aos seus clientes os serviços do Customer Success Manager através de uma abordagem complementar da empresa chamada de Logicalis Adoption Services. Este visa oferece práticas de adoção tecnológica e de sucesso de clientes para mapear os objetivos de negócio através de tecnologias de cibersegurança.

Modelo Hibrido: A Logicalis está capacitada para implementação de modelos de MSS onde parte da infraestrutura de hardware e software podem ser instaladas nas dependências do cliente e operar em perfeita sincronia com seu CSA – Centro de Servicos Avançados. Assim, os recursos especializados também poderão estar operando nas 2 localidades para atender as demandas dos clientes.

Ponto de Atenção

Apesar de operar com seu SOC altamente especializado, o fato de possuir apenas uma instalação no Brasil pode colocar a Logicalis em desvantagem nas disputadas por novos negócios de MSS.

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:

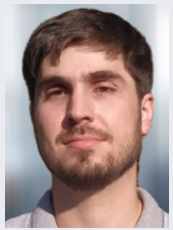
1. Definição do mercado Cybersecurity – Solutions and Services
2. Uso de pesquisas baseadas em questionários de provedores/ fornecedores de serviços em todos os tópicos de tendência
3. Discussões interativas com provedores/fornecedores de serviços sobre recursos e casos de uso
4. Uso de bancos de dados 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