ISG Provider Lens™

Cybersecurity – Solutions and Services

Extended Detection and Response

Uma análise do mercado de segurança cibernética, comparando a atratividade do portfólio de provedores e suas fortalezas competitivas

Customized report courtesy of:

kaspersky

QUADRANT REPORT | JUNHO DE 2024 | BRASIL

Índice

Autor do Relatório:
Christian Horst Alves Reis,
Gowtham Sampath (SSE), and
Dr. Maxime Martelli (XDR)

As empresas devem redobrar os esforços de proteção e resiliência em um cenário de crescimento de ataques cibernéticos

Em 2023 observamos, novamente, um significativo aumento em notificações de incidentes de ataques cibernéticos, indicando um descasamento entre a velocidade e eficácia da adoção de boas práticas e ferramentas pelas empresas e a proliferação de ameaças e agentes criminosos que, de forma impune, buscam ganhos fáceis, rápidos e em todos os setores da economia. Podemos notar que, após o pico de ataques cibernéticos em 2020 e a importante queda em 2021, temos um cenário preocupante, confirmando a tendência indicada no estudo anterior. Os constantes danos financeiros e reputacionais indicam que empresas podem estar ainda adotando posturas reativas quando o assunto é a priorização de investimentos na área. O risco deste comportamento, além do efeito imediato das perdas decorrentes de uma ação criminosa, é de, ao se concentrarem apenas na correção pontual das falhas exploradas no ataque, as empresas percam a oportunidade de estabelecer um plano abrangente de segurança da informação, amparado por fornecedores experientes, em jornadas que requerem alguns anos até a maturidade adequada.

Com o estabelecimento da Lei Geral de Proteção de Dados, em vigor desde 2020, esperava-se que empresas e órgãos governamentais adotassem medidas profundas de revisão e proteção de dados sensíveis e, com isso, elevassem a maturidade geral em segurança cibernética. O que vemos, contudo, é a proliferação de casos de subtração de dados pessoais para os mais variados usos e o enriquecimento de bases de dados na dark web, a serviço de novas ondas de ataques e danos aos consumidores.

Exemplificando a extensão preocupante destes vazamentos, tornou-se notória a existência na dark web de um repositório intitulado MOAB ("mother of all breaches" ou "mãe de todos as violações"), com 26 bilhões de registros

No Brasil, segurança cibernética deve estar na **pauta do board**, com **prioridade no budget**.

disponíveis de empresas do mundo todo. Apenas de grandes empresas brasileiras, são estimados 350 milhões de registros, que devem ser acrescentados aos vazamentos globais de credenciais de brasileiros em sites de e-commerce e redes sociais.

Nesta corrida cruel, na qual os criminosos se organizam em grupos cada vez mais poderosos contra alvos frágeis, se aproveitando de brechas conhecidas ou novos caminhos, as empresas precisam fazer o dever de casa com urgência e com visão 360 graus, protegendo seus dados através de soluções de criptografia, as identidades de forma efetiva e evoluírem na resiliência de seus ambientes críticos. A adoção de um framework, como NIST ou ISO, está ao alcance de todos e não deve ser subestimada, sendo um excelente guia mestre nas ações estruturantes.

Se de um lado temos hackers modernos, incansáveis, bem-preparados e motivados, do outro lado precisamos de disciplina, inteligência, parceiros bem selecionados, pessoas com olhar crítico e senso de urgência diferenciados. Vejamos o ritmo de adoção de postura zero trust em países mais desenvolvidos, onde o tema é considerado como prioridade, em comparação à dificuldade em nosso mercado para a conquista de recursos iniciais. Ao mantermos os atrasos na adoção dos novos antídotos, atraímos uma comunidade hacker mundial cada vez melhor instrumentada.

Phishing: observamos um aumento expressivo em tentativas de phishing no Brasil, tanto para e-mails corporativos, quanto para pessoas físicas que passam a ter suas contas repletas de mensagens cada vez melhor formuladas para a obtenção de vantagens, como o pagamento de contas falsas e o fornecimento de dados pessoais para então efetuarem os ataques.

O phishing é uma técnica de fraude online usada por criminosos para induzir indivíduos a revelarem informações pessoais, como senhas e detalhes de cartões de crédito, fingindo ser uma entidade confiável em comunicação eletrônica. Normalmente realizado por email, o ataque também pode ocorrer via mensagens de texto, redes sociais ou chamadas telefônicas. Os phishers criam mensagens e sites falsos que imitam organizações legítimas, induzindo as vítimas a fornecerem dados sensíveis ou clicar em links maliciosos que podem instalar softwares prejudiciais ou roubar informações. Reconhecer e evitar esses ataques é crucial para a proteção da segurança online.

As empresas devem adotar estratégias e práticas para se protegerem tanto das tentativas de phishing quanto do uso de dados já expostos, de forma multifacetada, incluindo:

- Controles de acessos, de forma que os funcionários e terceiros possuam apenas os privilégios minimamente necessários para suas atividades, compatíveis com os conceitos de segurança de confiança zero.
- Autenticação multifator, adicionando uma camada extra de segurança ao processo de login, mesmo que as credenciais sejam comprometidas.
- Filtros avançados de e-mails, com verificação de links, anexos e indicação de e-mail externo, para bloqueio de comunicações fraudulentas.
- Proteções robustas dos equipamentos, com atualizações constantes e atuação automática em casos suspeitos, impedindo a proliferação de malwares para a rede ou comprometimento de dados do end-point em qualquer lugar.
- Treinamento regular para a educação dos funcionários e terceiros na identificação de mensagens suspeitas, em todos os níveis da organização, e a realização de simulações de phishing para teste da resposta e reforço de conceitos.
- Segregação de uso corporativo e pessoal em dispositivos móveis.

Ransomware: continuamos a observar a evolução dos ataques de ransomware e a confirmação desta ameaça como uma das maiores e potencialmente mais lucrativas. Algumas tendências mais relevantes incluem o foco em alvos mais específicos, como organizações governamentais, sistemas de saúde, instituições educacionais e grandes corporações com exposição pública, de forma a maximizar impacto e o potencial de pagamento de resgate. Vemos também que hackers menos experientes cada vez mais possuem acesso à contratação de ransomware como serviço (RaaS), compartilhando os lucros e o resultado de extrações de dados.

Em resposta à crescente ameaça, as organizações precisam priorizar investimentos em medidas de prevenção, como o hardening

de seus ativos, a criptografia de seus dados chave, o controle rigoroso de acesso, a adoção de tecnologias mais avançadas de detecção e resposta, backups robustos, a segmentação de rede e não menos importante na revisão e proteção de seus ativos tecnológicos de operação, com ou sem dispositivos de IoT.

A orquestração destas frentes de trabalho, cada vez mais sofisticadas, encontra barreiras importantes nos negócios além da questão orçamentária, especialmente na dificuldade de se estabelecer um time próprio especializado num ambiente tão competitivo e dinâmico. Com isso, o papel do ecossistema de fornecedores de solução e de serviços ganha maior relevância e responsabilidade. Ferramentas são essênciais, desde que bem-posicionadas, num contexto integrado à estratégia de cada empresa, ao seu apetite de riscos, à sua jornada de amadurecimento e à sua cultura organizacional. Neste cenário, as empresas devem tomar a iniciativa na construção de um ambiente seguro, não apenas adotando tecnologias e práticas recomendadas, mas também desenvolvendo uma mentalidade de segurança em todos os níveis da organização e, especialmente, no C-level. Isso inclui a capacitação contínua de colaboradores, a participação ativa na definição de políticas de segurança e a prática constante de exercícios de simulação de incidentes. Assegurar que as medidas de segurança estejam alinhadas com os objetivos de negócio é fundamental, pois a segurança cibernética não é somente uma questão de TI, mas um diferencial competitivo que protege a marca, a confiança dos clientes e o valor acionário da empresa.

A adoção de uma postura proativa significa rever e reforçar as práticas existentes e antecipar-se às novas tendências de ataques, adaptando-se rapidamente às mudanças no cenário de ameaças. Com uma estratégia de segurança bem definida e executada, as empresas podem operar de forma mais linear e explorar novos negócios e oportunidades digitais com maior confiança, garantindo a continuidade e o sucesso em um mundo digital mais interconectado.

O panorama atual indica um caminho importante com tendências que destacamos abaixo, relacionadas aos quadrantes deste estudo:

Identity and Access Management (IAM)

O gerenciamento de identidades e acessos passou a ser a nova fronteira de perímetro de uma empresa e, desta forma, a adoção de modelos de segurança de confiança zero é uma realidade em mercados mais sofisticados e deve se tornar foco no Brasil, especialmente com a escalada nos ataques cibernéticos baseados em credenciais expostas. As soluções, antes restritas a atividades básicas de credenciamento, agora possuem sofisticação crescente com o uso de inteligência artificial para entendimento de contextos de acesso, fundamental para se conferir acessos seguros. Com isso, as empresas já maduras, com aplicações federadas com controles centralizados de usuários, poderão usufruir mais facilmente deste modelo, enquanto as demais empresas precisarão de aceleradores para conseguirem adotar alguns conceitos iniciais e reduzirem a exposição. Contudo, a lacuna entre estes grupos de empresa tende a aumentar, assim como o investimento necessário para a recuperação do tempo perdido. Ao ser combinada a outras boas práticas, como os modelos de prevenção a perda de dados e defesa e resposta avançadas, a nova geração de soluções IAM se torna uma aliada essêncial de proteção.

Extended Detection and Response (XDR)

O XDR, em nossa visão, se tornou rapidamente peça chave no intrincado conjunto de práticas e soluções e deve ser entendido com a plataforma evolutiva de um centro de comando de segurança cibernética, dado o seu potencial de utilização intensiva de inteligência artificial para automatizar a análise de ameaças críticas. E neste caso, a busca é pela, até recentemente, utópica busca pela detecção e resposta imediata. Trata-se de um caminho sem volta, que ganhará grande sofisticação a cada ano, a cada salto na capacidade e na engenhosidade dos modelos de linguagem de larga escala, adotados de forma massiva como antídoto para a escalada e sofisticação das ameaças cibernéticas. Em algum momento, esta batalha ocorrerá em nanosegundos amparados por computação quântica e devemos acompanhar de perto esta revolução.

Technical Security Services (TSS)

O papel das empresas fornecedoras de serviços técnicos de segurança continuará a ganhar

relevância no mercado, amparado por fatores como a escassez de recursos nas empresas, ao aumento da complexidade e interdependência das soluções e do leque mais completo de fornecedores, cada um com seus pontos fortes e gaps. Aliadas a estes fatores, as empresas clientes devem passar a exigir mais do que serviços pontuais de venda e instalação, tendência esta já confirmada neste estudo e que, com isso, passa a distanciar players com abordagem tradicional daqueles que atuam num contexto mais amplo e estratégico junto aos seus clientes, ao mesmo tempo que se destacam nos quesitos técnicos.

Strategic Security Services (SSS)

Os serviços estratégicos de segurança são o alicerce de qualquer programa de longo prazo de segurança da informação, especialmente com o avanço gradual no nosso mercado dos modelos de acesso com confiança zero (ZTNA) e suas complexidades de adoção, com o crescente interesse e necessidade de adoção de práticas integradas de gerenciamento de riscos e conformidade, com os desafios e oportunidades postas por IA generativa permeando as organizações além da TI, com a criação e atualização de planos de resiliência cibernética e recuperação de desastres, tema este em muito negligenciado pelas empresas locais, e com o seu papel preponderante de efetivamente aproximar o tema de segurança cibernética da líderança executiva das organizações.

Managed Security Services (MSS/SOC)

O centro nervoso de monitoramento de segurança das empresas passas por desafios de grande relevância. De um lado, observamos empresas ancoradas em serviços tradicionais e tempos de resposta, notificação e resposta considerado reativos. Do outro, estão embarcadas na revolução contínua promovida pela grande sofisticação do XDR descrito anteriormente. São perspectivas completamente distintas que devem promover reflexões de todos os profissionais interessados no tema e em executivos e membros de conselhos de administração, afinal, esta linha de defesa deve representar o batalhão de elite de uma organização conectada aos desafios modernos. Vemos um movimento relevante de fornecedores em busca desta transição, enquanto outros direcionam esforços a clientes com menor grau de sofisticação e exigência. Vale ressaltar que, este mercado, de forma massificada, é relativamente novo e hoje praticamente não se discute a necessidade de adoção de serviços de SOC. O que vem adiante é ainda mais interessante e desafiador.

Vulnerability Assessment & Pentesting (VAPT)

De forma inédita no mercado, abordamos neste estudo o tema do VAPT, pois com o maior grau de especialização dos fornecedores no mercado e demandas mais exigentes das empresas, a realização de avaliações de vulnerabilidades ganhou protagonismo e deve permanecer em ascensão pelo seu caráter isento e direcionador de esforços, sempre baseado em frameworks reconhecidos de mercado. Anteriormente, este mercado se mostrava altamente fragmentado e observamos com grande interesse os movimentos de fusões e aquisições, especialmente em 2023, constatando de que estes players adicionam grande valor em serviços de segurança para grandes empresas. Destacamos como tendência a maior recorrência de contratação destes serviços, assim como o ocorrido e estabelecido nos testes de penetração. Estes, por fim, indicam uma mudança gradativa, ainda com desafios, para a incorporação definitiva dos serviços ao longo das mudanças realizadas nas organizações, em suas APIs, sites e novos ambientes, na forma de missões complementares aos maiores eventos de testes.

Os desafios de segurança cibernética estão mais árduos com a adoção disseminada de inteligência artificial e automação pelos criminosos, atraídos por ganhos fáceis e rápidos em empresas de todos os portes e segmentos. Neste contexto, onde a postura das empresas deve ser mais rigorosa na adoção de padrões elevados de governança e na aceleração de seus planos de investimento, não há tempo a perder.

À medida que as empresas dependem cada vez mais de aplicativos em nuvem, forças de trabalho remotas e sistemas interligados, a complexidade e a sofisticação das ameaças cibernéticas aumentaram. Este ambiente dinâmico requer medidas de segurança avançadas que vão além das defesas perimetrais tradicionais. À medida que as ameaças cibernéticas continuam a crescer em sofisticação, a adoção de tais medidas de segurança de ponta será essencial para manter uma postura forte de segurança cibernética.

A necessidade de soluções avançadas de segurança cibernética, como detecção e resposta estendida (XDR) e borda de serviço de segurança (SSE), é impulsionada pelo cenário de ameaças em evolução, pelo aumento da adoção da nuvem e pela necessidade de frameworks de segurança abrangentes. Estas plataformas inovadoras abordam desafios críticos enfrentados pelas empresas, garantindo uma proteção resiliente e eficiente dos ativos digitais e das operações comerciais.

Alguns dos desafios existentes estão listados abaixo:

Complexidade em arquiteturas de segurança: O gerenciamento de ferramentas e soluções de segurança diferentes pode levar a ineficiências e lacunas na proteção, tornando plataformas integradas como XDR e SSE essenciais para operações simplificadas.

Detecção e resposta reativa a ameaças: As medidas de segurança tradicionais muitas vezes não conseguem fornecer visibilidade em tempo real e capacitações de resposta. O XDR aproveita análise avançada e automação para detectar, investigar e responder a ameaças em vários endpoints.

Privacidade e governança de dados negligentes: Garantir a privacidade e a governação dos dados num ambiente de TI descentralizado é desafiador. A SSE oferece políticas de segurança centralizadas e frameworks de governança para gerenciar a proteção de dados de forma eficaz.

Falta de escalabilidade e desempenho: À medida que as organizações crescem, as suas soluções de segurança devem ser dimensionadas de acordo, sem comprometer o desempenho operacional da TI ou dos negócios. O XDR e o SSE foram projetados para fornecer segurança escalonável e de alto desempenho em cenários de TI expansivos e em evolução.

Experiência de usuário ruim: É essencial equilibrar segurança robusta com uma experiência de usuário perfeita. As empresas exigem soluções inovadoras projetadas para serem minimamente invasivas e, ao mesmo tempo, maximizarem a proteção e a postura de segurança.

Tendências de Detecção e Resposta Estendida (XDR)

O mercado XDR está testemunhando várias tendências inovadoras para melhorar a detecção de ameaças, a resposta e a postura geral de segurança. As soluções XDR estão ganhando força devido à sua capacidade de coletar e correlacionar dados em múltiplas camadas de segurança, incluindo e-mails, endpoints, servidores, cargas de trabalho em nuvem e redes, proporcionando uma visão multifacetada da postura de segurança da organização.

As principais tendências no espaço XDR estão listadas abaixo:

Integração de IA e ML: Uma das últimas tendências em XDR é a integração de algoritmos de IA e ML para aprimorar as capacitações de detecção e resposta a ameaças. Estas tecnologias avançadas permitem que as plataformas XDR identifiquem ameaças complexas, prevejam potenciais ataques e automatizem ações de resposta, reduzindo assim a carga sobre as equipas de segurança.

Convergência com outras soluções de segurança: Outra tendência emergente é a convergência do XDR com outras soluções de segurança, como gerenciamento de informações e eventos de segurança (SIEM) e orquestração, automação e resposta de segurança (SOAR). Essa convergência cria uma arquitetura de segurança unificada, melhorando a visibilidade das ameaças, a detecção e os tempos de resposta, ao mesmo tempo que simplifica as operações de segurança.

Integração de inteligência de ameaças: As plataformas XDR integram-se cada vez mais com feeds de inteligência de ameaças para melhorar a detecção e resposta a ameaças. A combinação de dados de segurança interna com inteligência contra ameaças externas permite que as soluções XDR forneçam insights contextuais sobre ameaças potenciais. Isso ajuda as equipes de segurança a tomar decisões informadas e a priorizar seus esforços de resposta.

XDR para ambientes de nuvem e SaaS: À medida que as organizações continuam a adotar aplicativos em nuvem e SaaS, as soluções XDR estão expandindo sua cobertura para incluir esses ambientes. As plataformas XDR nativas da nuvem podem monitorar e proteger cargas de trabalho, contêineres e aplicativos sem servidor na nuvem, ao mesmo tempo que fornecem visibilidade sobre o uso de aplicativos SaaS e riscos potenciais.

Capacitações de detecção de ameaças e comprometimentos: As soluções XDR incorporam capacitações de análise de comportamento de usuários e entidades (UEBA) para detectar ameaças internas e comprometimentos de contas. A UEBA usa algoritmos de ML para analisar padrões de comportamento do usuário e identificar anomalias que possam indicar atividades maliciosas, ajudando as organizações a detectar e responder a ameaças que, de outra forma, poderiam passar despercebidas.

XDR aprimorando a segurança para ambientes ICS e OT: À medida que o cenário de ameaças para sistemas de controle industrial (ICS) e ambientes de TO continua a evoluir, os especialistas em segurança estão adaptando soluções XDR para enfrentar os desafios de segurança exclusivos desses sistemas. O XDR para ICS e OT pode monitorar e analisar dados de sistemas de controle industrial especializados, detectando ameaças antecipadamente e permitindo uma resposta rápida para minimizar possíveis danos.

Conformidade e suporte regulatório: Com o foco crescente na privacidade de dados e nas regulamentações de segurança, as organizações estão aprimorando as soluções XDR para atender aos requisitos de conformidade.

As empresas estão navegando em um cenário dinâmico caracterizado pela crescente adoção de ambientes de nuvem e pela evolução das ameaças cibernéticas, necessitando de soluções de segurança escaláveis, flexíveis e robustas. As soluções SSE abordam esses desafios fornecendo visibilidade centralizada, detecção avançada de ameaças alimentada por IA e ML e aplicação contínua de políticas em todos os endpoints. Ao adotar a SSE, as organizações podem garantir o acesso seguro a aplicativos e dados a partir de qualquer local, manter a conformidade com as normas regulamentares e proteger-se contra violações de dados e ameaças internas, apoiando assim a continuidade e a resiliência dos negócios face a um cenário de ameaças em constante mudança.

Os desafios abordados pelas soluções SSE estão listados abaixo:

Segurança de aplicativos em nuvem: A proliferação de serviços de nuvem cria complexidades de segurança. A SSE centraliza as políticas de segurança e impõe controle de acesso consistente em todos os aplicativos em nuvem.

Segurança da força de trabalho remota: Com mais empregados trabalhando remotamente, os modelos tradicionais de segurança baseados em perímetro tornam-se menos eficazes. O SSE fornece acesso seguro a aplicativos em nuvem de qualquer local, independentemente do dispositivo.

Prevenção contra perda de dados (DLP): Violações e vazamentos de dados são grandes preocupações. A SSE ajuda a evitar a exfiltração de dados confidenciais, aplicando políticas de DLP e criptografia de dados em serviços de nuvem.

Sombra de TI: Os empregados costumam usar aplicativos em nuvem não autorizados. O SSE fornece visibilidade do uso de shadow IT e permite controle de acesso seguro mesmo para aplicativos não aprovados.

Complexidade do gerenciamento de segurança: Gerenciar diversas soluções de pontos de segurança pode ser complexo e demorado. SSE oferece uma plataforma unificada para gerenciar políticas de segurança em todos os aplicativos em nuvem.

O mercado SSE está a registar um crescimento significativo devido à crescente adoção de aplicativos em nuvem, forças de trabalho remotas e à necessidade de uma abordagem de segurança consolidada.

As principais tendências que moldam o mercado estão listadas abaixo:

Arquiteturas nativas da nuvem: À medida que as empresas migram para ambientes de nuvem, elas adotam soluções de segurança nativas da nuvem que se adaptam às cargas de trabalho e suportam configurações dinâmicas e distribuídas.

Convergência de segurança e rede: Há uma tendência crescente de integrar funções de rede e segurança em uma única plataforma, simplificando as operações e reduzindo a complexidade do gerenciamento da segurança e do desempenho da rede.

Integração de SWGs e CASBs: Gateways web seguros (SWGs) e corretores de segurança de acesso à nuvem (CASBs) estão convergindo para soluções SSE abrangentes, fornecendo proteção unificada contra ameaças, DLP e controle de acesso para serviços de nuvem.

Ênfase na segurança de confiança zero: As soluções SSE incorporam cada vez mais princípios de confiança zero, concedendo acesso baseado em privilégios mínimos e verificação contínua, melhorando a segurança ao minimizar a superfície de ataque e o movimento lateral dentro da rede.

Adoção SASE: SSE é um elemento fundamental das arquiteturas de borda de serviço de acesso seguro (SASE), que integram segurança de rede e segurança de acesso à nuvem em um serviço unificado fornecido pela nuvem.

Integração de IA e ML: As soluções SSE aproveitam IA e ML para automatizar a detecção de ameaças, melhorar a identificação de anomalias e personalizar políticas de segurança com base no comportamento do usuário.

Concentre-se na experiência do usuário: Equilibrar segurança com UX é crucial. As soluções SSE são projetadas para serem transparentes para os usuários, garantindo interrupção mínima no workflow e mantendo uma segurança robusta.

Consoles de gerenciamento unificados: Há uma tendência de desenvolvimento de interfaces de gerenciamento unificadas que consolidem diversas funções de segurança em um único painel, simplificando a administração e fornecendo uma visão holística do cenário de segurança.

Análise de comportamento de usuários e entidades (UEBA): As ferramentas da UEBA analisam o comportamento dos usuários e entidades para identificar potenciais ameaças à segurança. Ao estabelecer linhas de base e detectar desvios, a UEBA ajuda a identificar atividades anómalas.

Segurança centrada na identidade: A ênfase na gestão de identidade e acesso (IAM) está se tornando central nas estratégias de segurança, garantindo que apenas usuários autenticados e autorizados possam acessar os recursos.

À medida que as empresas dão prioridade à segurança cibernética robusta e navegam pelas complexidades do ambiente digital, a procura de soluções inovadoras, como XDR e SSE, estará na vanguarda da salvaguarda dos seus ativos digitais. À medida que as ameaças cibernéticas se tornam mais sofisticadas e as empresas dependem cada vez mais de serviços de nuvem, o XDR e o SSE serão cruciais para proteger a segurança empresarial.

Posicionamento do Provedor

Página 1 de 11

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Extended Detection and Response	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Vulnerability Assessment and Penetration Testing
Accenture	Not In	Not In	Not In	Not In	Leader	Leader	Leader	Not In	Leader
Agility Networks	Not In	Not In	Not In	Not In	Leader	Not In	Product Challenger	Leader	Not In
Asper	Not In	Not In	Not In	Not In	Product Challenger	Not In	Rising Star ★	Not In	Product Challenger
Atos	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Not In	Product Challenger
Berghem	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
Bitdefender	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
BlackBerry	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Blaze Info Sec	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Market Challenger
BluePex	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In

Posicionamento do Provedor

Página 2 de 11

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Extended Detection and Response	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Vulnerability Assessment and Penetration Testing
Broadcom	Leader	Leader	Product Challenger	Leader	Not In	Not In	Not In	Not In	Not In
Capgemini	Not In	Not In	Not In	Not In	Leader	Leader	Rising Star ★	Not In	Product Challenger
Cato Networks	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Check Point Software	Contender	Product Challenger	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Cipher	Not In	Not In	Not In	Product Challenger	Contender	Market Challenger	Not In	Product Challenger	Leader
Cirion	Not In	Not In	Not In	Not In	Not In	Not In	Contender	Not In	Not In
Cisco	Not In	Market Challenger	Leader	Contender	Not In	Not In	Not In	Not In	Not In
Claranet	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In	Product Challenger	Contender
Clavis	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger

Posicionamento do Provedor

Página 3 de 11

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Extended Detection and Response	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Vulnerability Assessment and Penetration Testing
Cloudflare	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
CrowdStrike	Not In	Leader	Not In	Leader	Not In	Not In	Not In	Not In	Not In
CyberArk	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Cybereason	Not In	Product Challenger	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Deloitte	Not In	Not In	Not In	Not In	Leader	Leader	Product Challenger	Not In	Not In
DXC Technology	Not In	Not In	Not In	Not In	Product Challenger	Not In	Contender	Not In	Not In
Edge UOL	Not In	Not In	Not In	Not In	Not In	Not In	Market Challenger	Leader	Not In
Ericom Software	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
ESET	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In

Posicionamento do Provedor

Página 4 de 11

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Extended Detection and Response	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Vulnerability Assessment and Penetration Testing
E-TRUST	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
EY	Not In	Not In	Not In	Not In	Not In	Leader	Not In	Not In	Not In
FastHelp	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Contender	Contender
Forcepoint	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Fortinet	Contender	Leader	Product Challenger	Product Challenger	Not In	Not In	Not In	Not In	Not In
GC Security	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Leader
GoCache	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
HackerSec	Not In	Not In	Not In	Not In	Not In	Contender	Not In	Not In	Not In
Hakai	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Market Challenger

Posicionamento do Provedor

Página 5 de 11

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Extended Detection and Response	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Vulnerability Assessment and Penetration Testing
HPE (Aruba)	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Huge Networks	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
IBLISS	Not In	Not In	Not In	Not In	Not In	Contender	Not In	Not In	Product Challenger
IBM	Leader	Leader	Not In	Leader	Leader	Leader	Leader	Not In	Not In
iboss	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
ISH Tecnologia	Not In	Not In	Not In	Not In	Leader	Leader	Leader	Leader	Leader
iT.eam	Not In	Not In	Not In	Not In	Contender	Not In	Not In	Leader	Not In
Italtel	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Contender	Contender
Kaspersky	Not In	Product Challenger	Not In	Leader	Not In	Not In	Not In	Not In	Not In

Posicionamento do Provedor

Página 6 de 11

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Extended Detection and Response	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Vulnerability Assessment and Penetration Testing
KPMG	Not In	Not In	Not In	Not In	Contender	Rising Star ★	Contender	Not In	Not In
Kryptus	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger	Contender
Kyndryl	Not In	Not In	Not In	Not In	Rising Star ★	Product Challenger	Not In	Not In	Not In
Logicalis	Not In	Not In	Not In	Not In	Leader	Leader	Leader	Not In	Leader
Lookout	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Microsoft	Leader	Leader	Market Challenger	Leader	Not In	Not In	Not In	Not In	Not In
NAVA	Not In	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In
NEC	Not In	Not In	Not In	Not In	Not In	Contender	Not In	Not In	Not In
Netskope	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In

Posicionamento do Provedor

Página 7 de 11

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Extended Detection and Response	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Vulnerability Assessment and Penetration Testing
NTT DATA	Not In	Not In	Not In	Not In	Leader	Product Challenger	Leader	Not In	Not In
Okta	Leader	Not In	Not In	Not In	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	Not In	Not In	Not In
Open Systems	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
OpenText	Product Challenger	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In	Not In
Oracle	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Palo Alto Networks	Not In	Leader	Leader	Rising Star ★	Not In	Not In	Not In	Not In	Not In
Perimeter 81	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Ping Identity	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In

Posicionamento do Provedor

Página 8 de 11

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Extended Detection and Response	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Vulnerability Assessment and Penetration Testing
Pride Security	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Contender
Proofpoint	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
PwC	Not In	Not In	Not In	Not In	Product Challenger	Leader	Not In	Not In	Not In
Rapid7	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
RSA	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
SailPoint	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Scunna	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Contender	Not In
Secureworks	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
SEK	Not In	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In	Leader

Posicionamento do Provedor

Página 9 de 11

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Extended Detection and Response	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Vulnerability Assessment and Penetration Testing
senhasegura	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
SenseOn	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
SentinelOne	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Service IT	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
Skyhigh Security	Not In	Not In	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In
SONDA	Not In	Not In	Not In	Not In	Market Challenger	Not In	Not In	Market Challenger	Not In
Sophos	Not In	Product Challenger	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Stefanini	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Leader	Rising Star ★
TCS	Not In	Not In	Not In	Not In	Product Challenger	Contender	Not In	Not In	Not In

Posicionamento do Provedor

Página 10 de 11

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Extended Detection and Response	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Vulnerability Assessment and Penetration Testing
TDec Network	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Contender	Not In
TEHTRIS	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Teltec Solutions	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Contender	Not In
Thales	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Think IT	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Contender	Contender
TIVIT	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In	Rising Star ★	Market Challenger
Trellix	Not In	Rising Star ★	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Trend Micro	Not In	Leader	Not In	Leader	Not In	Not In	Not In	Not In	Not In
T-Systems	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Not In	Not In

Posicionamento do Provedor

Página 11 de 11

	Identity and Access Management	Extended Detection and Response (Global)	Security Service Edge (Global)	Extended Detection and Response	Technical Security Services	Strategic Security Services	Managed Security Services - SOC (Large Accounts)	Managed Security Services - SOC (Midmarket)	Vulnerability Assessment and Penetration Testing
Unisys	Contender	Not In	Not In	Not In	Not In	Product Challenger	Leader	Not In	Not In
Versa Networks	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Vortex Security	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Market Challenger	Not In
Wipro	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Not In	Not In
YSSY	Not In	Not In	Not In	Not In	Contender	Not In	Not In	Leader	Contender
Zscaler	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In

Key focus areas for the Cybersecurity – Solutions and Services 2024.

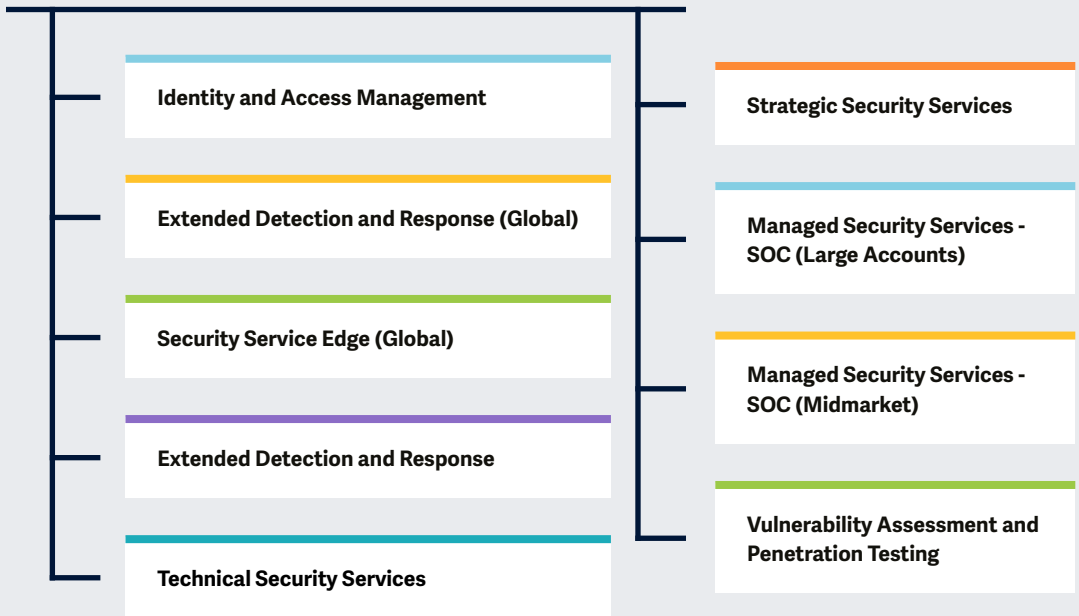


Ilustração simplificada Fonte: ISG 2024

Definição

O relatório ISG Provider Lens™ Cybersecurity – Solutions and Services oferece o seguinte aos tomadores de decisão de negócios e de TI:

- Transparência sobre os pontos fortes e fracos dos fornecedores relevantes;
- Um posicionamento diferenciado de fornecedores por segmentos, sobre seus pontos fortes competitivos e atratividade de portfólio;
- O foco em diferentes mercados, incluindo EUA, Reino Unido, Alemanha, Suíça, França, Brasil, Austrália e Setor Público dos EUA. Os tópicos sobre SSE e XDR serão analisados quanto ao mercado global;
- Para considerar as características específicas dos países neste estudo global, a análise de XDR se estende ao Brasil, enquanto, para a Alemanha, analisa-se a DLP. A introdução da DFIR será testada nos EUA e na França. O novo tópico de Avaliação de Vulnerabilidade e Teste de Penetração será lançado no Brasil.

Introdução

Nosso estudo serve como uma importante base de tomada de decisão para o posicionamento de relacionamentos chave e considerações de estratégia de vendas. Consultores e clientes corporativos do ISG usam informações desses relatórios para avaliar seus relacionamentos com fabricantes atuais e novos relacionamentos em potencial.

Escopo do Relatóriot

Este relatório do quadrante ISG Provider Lens™ abrange os nove quadrantes seguintes (indique o número de quadrantes, não utilize um dígito) para serviços/soluções: Gestão de Identidades e Acessos , Defesa e Resposta Alargadas , Serviços Técnicos de Segurança , Serviços Estratégicos de Segurança , Serviços Geridos de Segurança - SOC - (Grandes Contas), Serviços Geridos de Segurança -SOC (Midmarket) , Avaliação de Vulnerabilidades e Pentesting , Os fornecedores que oferecem soluções de Segurança de Borda de Serviços e de Deteção e Resposta Alargadas são analisados e posicionados a partir de uma perspetiva global e não de regiões individuais.

Este estudo ISG Provider Lens™ oferece aos decisores de TI:

- Transparência sobre os pontos fortes e fracos dos fornecedores de software e serviços relevantes;
- Um posicionamento diferenciado dos fornecedores por segmentos (quadrantes);
- Foco no mercado regional.

Nosso estudo serve como base para a tomada de decisões importantes sobre posicionamento, relações-chave e considerações de entrada no mercado. Os consultores e clientes corporativos da ISG também utilizam as informações contidas nestes relatórios para avaliar suas relações existentes com fornecedores e possíveis compromissos.

Classificações do Provedor

A posição de fornecedor reflete a adequação dos fornecedores de TI/fornecedores de software para um segmento de mercado definido (quadrante). Sem mais acréscimos, a posição sempre se aplica a todas as classes e indústrias de todos os tamanhos de empresas. Caso as exigências de serviços de TI de clientes empresariais sejam diferentes e o espectro dos fornecedores de TI que operam no mercado local seja suficientemente amplo, uma diferenciação adicional dos fornecedores de TI por desempenho é feita de acordo com o grupo-alvo de produtos e serviços. Ao fazer isso, a ISG considera as exigências do setor ou o número de funcionários, assim como as estruturas corporativas dos clientes e posiciona os fornecedores de TI de acordo com sua área de foco. Como resultado, a ISG os diferencia, se necessário, em dois grupos-alvo de clientes que são definidos como segue:

- **Mercado Intermediário:** Empresas com 100 a 4.999 funcionários ou receitas entre US$20 milhões e US$999 milhões com sede central no respectivo país, geralmente de propriedade privada.
- **Grandes Empresas:** Empresas multinacionais com mais de 5.000 funcionários ou receita acima de US$ 1 bilhão, com atividades em todo o mundo e estruturas de tomada de decisão distribuídas globalmente.

Segundo o ISG Provider Lens™, os quadrantes são criados usando uma matriz de avaliação contendo quatro segmentos (Leader, Product & Market Challenger e Contender), e os fornecedores estão posicionados de acordo. Cada quadrante de Lentes de Fornecedores ISG pode incluir um prestador(es) de serviços que a ISG acredita ter forte potencial para se mover para o quadrante dos Líderes. Este tipo de fornecedor pode ser classificado como uma Estrela em Ascensão.

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

Classificação dos Provedores: Quadrantes Chave

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.

Classificação dos Provedores: Quadrantes Chave

★ 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.

Extended Detection and Response

Quem Deve Ler Isto

Este relatório é relevante para empresas de todos os setores no Brasil, visando avaliar fornecedores de produtos de detecção e resposta estendida (XDR), que são projetados para fornecer segurança do espaço de trabalho, segurança da rede ou segurança de workloads.

Neste relatório, o ISG destaca o posicionamento de mercado atual dos fornecedores de produtos XDR, que atuam na detecção e resposta de ameaças nas empresas do Brasil, e como cada fornecedor lida com os principais desafios enfrentados na região.

As empresas brasileiras estão oferecendo plataformas de XDR que utilizam ferramentas de inteligência artificial e automação para reduzir o tempo médio de detecção e resposta a ameaças, pois a agilidade é essencial nesse processo. Isso ocorre porque o tempo de permanência de um cibercriminoso no ambiente está diretamente relacionado aos danos causados.

Os fornecedores locais estão investindo na integração de suas plataformas XDR com feeds de inteligência para enfrentar as crescentes ameaças, como novos golpes, ataques de engenharia social e táticas de ransomware. Essas preocupações são constantes para as organizações, que buscam maneiras eficazes de lidar com os desafios emergentes.

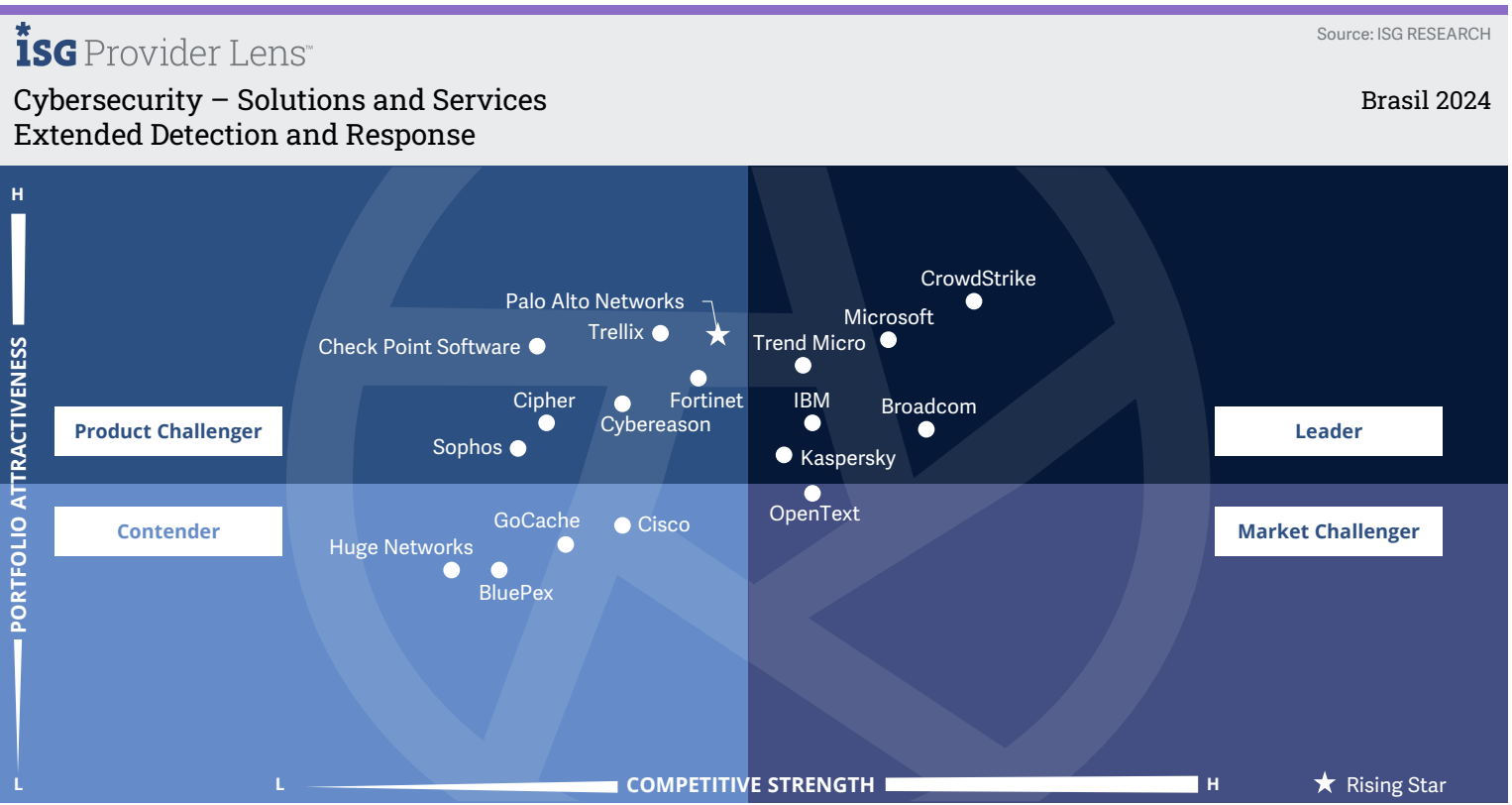
Por fim, as empresas brasileiras estão ampliando o uso de modelos de linguagem de larga escala em tecnologias XDR para melhorar suas defesas cibernéticas, uma vez que esses modelos são capazes de processar grandes volumes de dados de forma eficiente e identificar padrões sutis, que podem indicar atividades maliciosas. Isso é fundamental para lidar com ameaças digitais crescentes, permitindo uma resposta eficaz aos ataques.

Líderes de segurança da informação devem ler este relatório para entender como os fornecedores de soluções de XDR se atualizam para enfrentar novos tipos de ataques.

Diretores de tecnologia devem ler este relatório para entender a capacidade dos fornecedores de soluções XDR e como podem ajudá-los na estratégia de segurança cibernética da empresa.

Profissionais de privacidade de dados devem ler este relatório para entender o posicionamento relativo dos fornecedores de soluções XDR e como eles auxiliam na resposta a incidentes envolvendo dados.

Profissionais de produtos digitais devem ler este relatório para entender como os fornecedores de XDR podem ajudar na estabilização de produtos para aumentar a segurança de seus clientes.



Este quadrante avalia fornecedores de **soluções defesa e resposta estendida, com software e serviços** de monitoramento total de **próxima geração baseados em correlações múltiplas de eventos**, permitindo respostas mais rápidas e precisas.

Christian Horst Alves Reis

Definição

Os fornecedores de soluções XDR avaliados neste quadrante são caracterizados pela capacidade de oferecer uma plataforma que integra, correlaciona e contextualiza dados e alertas de múltiplos componentes de prevenção, detecção e resposta a ameaças. XDR é uma tecnologia em nuvem com soluções de múltiplos pontos. Com análises avançadas, ela correlaciona alertas de diversas fontes, incluindo sinais individuais fracos, para permitir detecções precisas.

As soluções XDR consolidam e integram vários produtos, proporcionando segurança abrangente para espaços de trabalho, redes e cargas de trabalho. Normalmente, as soluções XDR visam melhorar significativamente a visibilidade e a compreensão do contexto das ameaças identificadas em toda a empresa. As características dessas soluções incluem telemetria e análise contextual de dados para detecção e resposta.

As soluções XDR compreendem vários produtos integrados em um único painel para recursos sofisticados de visualização, detecção e resposta. Sua alta maturidade de automação e análise contextual oferecem respostas personalizadas para sistemas afetados, priorizando alertas com base na gravidade em termos de estruturas de referência conhecidas. Este quadrante exclui **fornecedores de serviços puros que não oferecem uma solução XDR baseada em softwares exclusivos**.

As soluções XDR destinam-se a reduzir a dispersão de produtos, fadiga de alertas, desafios de integração e despesas operacionais. São particularmente adequadas para equipes de operações de segurança que precisam gerenciar diversos portfólios de soluções ou obter valor de soluções de gerenciamento de informações e eventos de segurança (SIEM) ou de orquestração, automação e resposta de segurança (SOAR).

Critérios de elegibilidade

1. Oferecer soluções XDR baseadas em **softwares exclusivos**, e não softwares de terceiros
2. Certificar-se de que uma solução XDR tenha dois componentes principais: **XDR front-end e XDR back-end**
3. Oferecer front-end com **três ou mais soluções ou sensores**, incluindo, entre outros, **detecção e resposta de endpoint, plataformas de proteção de endpoint**, proteção de rede (firewalls, IDPS), detecção e resposta de rede, gestão de identidade, segurança de e-mail, detecção de ameaças móveis, proteção de carga de trabalho na nuvem e identificação de fraude
4. Fornecer solução com **cobertura e visibilidade abrangentes e totais de todos os endpoints em uma rede**
5. Oferecer solução capaz de **bloquear ameaças sofisticadas, como ameaças persistentes avançadas, ransomware e malware**
6. Fornecer soluções usando **inteligência de ameaças e insights em tempo real** sobre ameaças provenientes de endpoints
7. Oferecer solução com **recursos de resposta automatizada**

Observações

Observamos em 2023 um movimento mais acelerado na evolução das soluções de XDR, à medida em que as abordagens tradicionais de monitoramento e os tempos de resposta se mostram cada vez menos adequados ao panorama atual de aumento nas tentativas de ataque cibernético, adoção massificada de ambientes híbridos, multicloud e, num contexto de maior, utilização de aprendizado de máquina aliado à inteligência artificial.

O papel destas soluções é de atuar como o grande processador de alertas e comportamentos em todo o ambiente computacional, relacionando-os a bases de conhecimentos constantemente enriquecidas por observações e eventos anteriores e aliado ao poder da inteligência artificial. De forma cada vez mais automática e rápida, estas soluções devem atuar com precisão na resposta e permitir a evolução contínua para novos cenários. O que vivemos atualmente é o início de uma grande revolução que mudará completamente o papel do SOC convencional, dos times técnicos e dos prestadores de serviços envolvidos.

Os recursos necessários para que estas soluções evoluam na velocidade que o mercado demanda indicam que, ao menos em uma primeira onda, os players que mais se destacam são aqueles com abordagens inovadoras para entregas em larga escala, amparados por ampla conectividade técnica e uso intensivo de IA.

O quadrante deste ano reflete o dinamismo do mercado, com movimentações mais relevantes, com o caso da IBM, que passa a figurar como líder, da Microsoft que avança com ofertas mais robustas e da Palo Alto Networks, escolhida como Rising Star do ano. Com a incorporação da VMWare pela Broadcom, esta deixa de ser mencionada no estudo.

Das 74 empresas avaliadas para este estudo, 18 se qualificaram para este quadrante, sendo 6 Líderes e uma Rising Star.

Broadcom

A solução XDR da **Broadcom**, oferecida através da Symantec Endpoint Security (SES) Complete, apresenta diversos benefícios visando simplificar, acelerar e expandir a visibilidade entre diferentes pontos de controle de segurança nas empresas.

CrowdStrike

A solução XDR da **CrowdStrike**, conhecida como Falcon XDR, oferece uma gama de benefícios significativos para equipes de segurança, visando aprimorar a visibilidade, detecção, investigação e resposta a ameaças em todo o ecossistema de TI de uma organização.

IBM

Criado com base em padrões abertos, o **IBM** Security QRadar XDR é uma solução nativa de nuvem com elevada aceitação no mercado, integrando várias fontes de dados externas e aplicando a triagem e a correlação de alertas com tecnologia de IA.

kaspersky

A **Kaspersky Lab** oferece soluções para empresas de todos os tamanhos, com as ofertas Security Foundations, Optimum Security e Expert Security, sendo esta última a sua oferta mais abrangente e avançada.

Microsoft

Com mais de 3.500 especialistas em segurança cibernética e investimentos anuais superiores a USD1 bilhão, a **Microsoft** se consolida como líder em soluções cada vez mais integradas e avançadas, através das soluções Sentinel e Defender XDR.

Trend Micro

A solução XDR da **Trend Micro**, Trend Vision One, oferece uma abordagem completa para detecção mais rápida e precisa de ameaças, investigação aprofundada e respostas mais eficientes através de uma integração nativa de dados, análises e fluxos de trabalho.

Palo Alto Networks

A soluções da Plataforma Cortex XDR da **Palo Alto Networks** atuam em todo o ambiente computacional, eliminando pontos cegos e reduzindo o tempo médio de resposta, com alta qualidade na detecção de ameaças.

Leader

"A Kaspersky Lab conta com um time próprio de especialistas no Brasil, essêncial para maior assertividade no combate a ameaças locais. Sua ampla rede de parceiros e o centro de transparência em São Paulo reforçam a posição de destaque no mercado."

Christian Horst Alves Reis

Kaspersky Lab

Visão Geral

Kaspersky Lab é uma empresa privada internacional sediada em Moscou, Rússia com sua holding registrada no Reino Unido e com sua infraestrutura de processamento de dados localizada na Suíça. A empresa tem subsidiárias em 31 países e possui cerca de 4.000 especialistas altamente qualificados. Suas soluções protegem 220.000 clientes corporativos. A Kaspersky Lab é conhecida por sua expertise em pesquisa de malware e análise de ameaças cibernéticas. Seu time de pesquisa, o Kaspersky Global Research and Analysis Team (GReAT), é responsável pela descoberta de várias campanhas de ciberespionagem e ciberataques sofisticados.

Pontos Fortes

Pesquisa e desenvolvimento: através de seu time de pesquisa com 7 analistas baseados na região, o Kaspersky Global Research and Analysis Team (GReAT), a empresa contribui significativamente para o desenvolvimento das soluções, garantindo que elas sejam equipadas com as mais recentes tecnologias de detecção e prevenção de ameaças.

Automação e orquestração de resposta a incidentes: a soluções da Kaspersky Lab automatizam processos de resposta a incidentes, desde a detecção até a remediação, reduzindo o tempo de resposta e o impacto potencial de ataques cibernéticos. Ferramentas integradas facilitam a investigação detalhada de incidentes de segurança, permitindo o rastreamento da cadeia de ataque, o entendimento de causa raiz e a implementação de medidas de prevenção de recorrência em todo o ambiente gerenciado.

Parceiros e especialistas no Brasil: a Kaspersky Lab conta com mais de 1600 parceiros no país e uma forte equipe técnica local, que também atua no contexto Américas, para que novas ameaças sejam rapidamente neutralizadas.

Centros de transparência: localizados em São Paulo, Toronto, Kuala Lumpur, Madri, Zurique, e mais 5 localidades, estão abertos a governos, clientes corporativos e parceiros regulatórios e permitem ampla revisão de seus códigos-fonte, assim como a avaliação de suas atualizações e regras de detecção.

Atenção

Reconhecida amplamente pela sua competência técnica e agilidade, a Kaspersky Lab pode considerar expandir sua oferta de soluções XDR no mercado, especialmente para pequenas e médias empresas, aproveitando-se da grande base instalada para ocupar espaços neste mercado dinâmico.

Star of Excellence

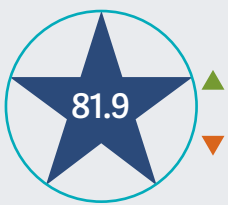
Um programa, desenvolvido pela ISG, para coletar feedback de clientes sobre o sucesso dos fornecedores em demonstrar os mais altos padrões de excelência em atendimento ao cliente e foco no cliente.

Fonte: Programa de pesquisa Star of Excellence™ do ISG, insights até Junho de 2024

Na pesquisa Star of Excellence™ do ISG sobre experiência do cliente (CX), clientes que são empresas forneceram feedback sobre a experiência que tiveram com fornecedores de serviços em seus serviços de **Cybersecurity Solutions and Services**.

Com base no feedback direto de clientes pessoas jurídicas, obtivemos os destaques a seguir:

Pontuação média de CX do setor



▲ CX com pontuação mais alta: 91.0

▼ CX com pontuação mais baixa: 64.8

Pontuação de CX: 100 mais satisfeitos, 0 menos satisfeitos Total de respostas (N) = 419

Papel Comercial do Cliente

▲ **Maior satisfação**
Information Technology

▼ **Menor satisfação**
Human Resources

Região

▲ **Maior satisfação**
Africa

▼ **Menor satisfação**
Eastern Europe

Setor

▲ **Maior satisfação**
Chemicals

▼ **Menor satisfação**
Public sector

Pilar de CX mais importante

Execution and Delivery

Modelos de entrega de serviço	% média do trabalho realizado
No local	53.6%
Nearshore	21.6%
Offshore	24.8%

Apêndice

O estudo de pesquisa "ISG Provider Lens™ Cybersecurity – Solutions and Services 2024 - Brasil" 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.

Patrocinador do estudo:
Heiko Henkes

Autores principais:
Christian Horst Alves Reis, Gowtham Sampath, and Dr. Maxime Martelli

Editores:
TGT and Padma Kalyani Mohapatra

Analista de Pesquisa:
Bruno Nakazone and Monica K

Analistas de Dados:
Rajesh Chillappagari and Laxmi Sahebrao

Gerente de Projetos:
Shreemadhu Rai B

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 Maio de 2024, 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 ndicado de outra forma.

O estudo foi dividido nas seguintes etapas:

1. Definição do mercado de 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. Aproveite os 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

Christian Horst Alves Reis

Analista principal

Christian Reis é analista líder da ISG Brasil e tem uma vasta experiência tanto no lado executivo em cargos seniores quanto em posições de consultoria, com constante exposição global. Suas principais áreas de especialização incluem transformação de negócios, inovação, modernização e racionalização de TI, segurança cibernética e conformidade.

Ele está focado em serviços de consultoria para empresas na América Latina e é muito ativo em fóruns de inovação na região.

Autor

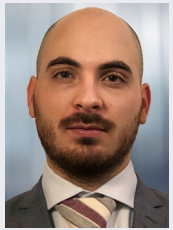
Gowtham Sampath

Diretor Sénior, ISG Provider Lens™

Gowtham Sampath é gerente sênior da ISG Research, responsável pela criação de relatórios do quadrante ISG Provider Lens™ para o mercado de tecnologia/plataformas bancárias, serviços bancários digitais, segurança cibernética e soluções e serviços de análise. Com 15 anos de experiência em pesquisa de mercado, Gowtham trabalha na análise e na ponte entre fornecedores de análise de dados e empresas, abordando oportunidades de mercado e melhores práticas. Na sua função, também trabalha com consultores para dar resposta aos pedidos de investigação ad-hoc dos clientes empresariais no sector dos serviços de TI, em todos os sectores.

É também autor de estudos de liderança, documentos técnicos e artigos sobre tecnologias emergentes no sector bancário nas áreas da automatização, DX e experiência UX, bem como sobre o impacto da análise de dados em diferentes sectores verticais da indústria.

Autor



Dr. Maxime Martelli

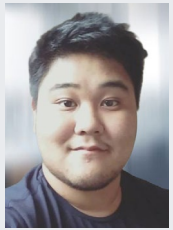
Gerente de Consultoria e Analista de Segurança

Maxime participa da solução de "Segurança cibernética" do ISG para empresas multinacionais e serviços do setor público, além de aplicar sua especialização em projetos de Segurança da Informação e Segurança na Nuvem.

Autor, professor e palestrante na área de TI, Maxime é apaixonado por tecnologia e aplica seu conhecimento de processos, estratégia digital e organização de TI para satisfazer as necessidades de seus clientes.

Como consultor de segurança, conduz projetos de transformação e estratégia para todos os tipos de produtos e soluções de segurança, e lidera o tópico SASE/SSE do lado cibernético no ISG EMEA.

Enterprise Context and Global Visão Geral



Bruno Nakazone

Analista de Pesquisa

Bruno Nakazone é analista de pesquisano ISG e é responsável por apoiar e sercoautor de estudos do Provider Lens™sobre ecossistema Oracle, ecossistemaMicrosoft, Digital business innovation,ESG e Digital Banking Industry Services.Ele apoia os principais analistas no processode pesquisa e é coautor do relatórioresumido global com tendências e insightsde mercado. Bruno também desenvolveconteúdo sob uma perspectiva empresarial.Bruno está alocado nesta função desde 2023.

Antes dessa função, trabalhou comoconsultor de processos de negócios, ondeadquiriu experiência e capacidade técnicana análise em processos de negócios. Suaárea de especialização inclui tecnologia,logística e pesquisa de mercado.

Contexto corporativo e visão geral global

Monica K

Assistente de gerenciamento, especialista sênior em pesquisa

Monica K. é gerente assistente e especialista líder em pesquisa e especialista digital da ISG. Ela criou conteúdo para os estudos do Provider Lens™, bem como conteúdo da perspectiva corporativa e é a autora do relatório global relatório de resumo global para o mercado de segurança cibernética, ESG e sustentabilidade mercado de sustentabilidade. Monica K. tem mais de uma década de de experiência e conhecimento nas áreas de tecnologia, negócios e mercado pesquisa de mercado para clientes do ISG. Anteriormente, ela trabalhou em uma empresa de pesquisa empresa de pesquisa, onde se especializou em em tecnologias emergentes, como IoT e desenvolvimento de produtos, perfis de fornecedores e inteligência de talentos. Suas Suas responsabilidades incluíam o gerenciamento de projetos de pesquisa abrangentes e a colaboração com as partes interessadas internas em várias iniciativas de consultoria.

Patrocinador do estudo

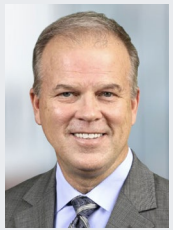
Heiko Henkes

Diretor e Analista Principal

Heiko Henkes atua como diretor e analista principal da ISG, supervisionando o programa Global ISG Provider Lens™ (IPL) para todos os estudos de terceirização de TI (ITO), juntamente com seu papel fundamental na divisão global de IPL como gerente de programa estratégico e líder de pensamento para analistas líderes de IPL.

Henkes dirige a Star of Excellence, a iniciativa global de experiência do cliente do ISG, orientando o design do programa e sua integração com o IPL e a prática de sourcing do ISG. A sua experiência consiste em orientar as empresas através de transformações de modelos de negócios baseados em TI, aproveitando a sua profunda compreensão da transformação contínua, competências de TI, estratégias de negócios sustentáveis e gestão de mudanças num cenário de negócios orientado para a IA na nuvem. Henkes é conhecido pelas suas contribuições como orador principal sobre inovação digital, partilhando ideias sobre a utilização da tecnologia para o crescimento e a transformação das empresas.

Proprietário do produto IPL



Jan Erik Aase

Sócio e Diretor Global – ISG Provider Lens™

O Sr. Aase possui uma vasta experiência na implementação e investigação da integração e gestão de serviços de TI e de processos empresariais. Com mais de 35 anos de experiência, é altamente qualificado na análise de tendências e metodologias de gestão de fornecedores, identificando ineficiências nos processos actuais e aconselhando a indústria. Jan Erik tem experiência em todos os quatro lados do ciclo de vida do sourcing e da gestão de fornecedores - como cliente, analista do sector, fornecedor de serviços e consultor.

Agora, como parceiro e diretor global do ISG Provider Lens™, está muito bem posicionado para avaliar e apresentar relatórios sobre o estado do sector e fazer recomendações tanto para empresas como para clientes fornecedores de serviços.

ISG Provider Lens™

O quadrante ISG Provider Lens™ série de pesquisa é o único serviço avaliação do provedor de seu tipo para combinar empírica, baseada em dados pesquisa e análise de mercado com a experiência do mundo real e observações da assessoria global do ISG equipe. As empresas encontrarão uma riqueza de dados detalhados e análise de mercado para ajudar a orientar sua seleção de parceiros de fornecimento apropriados, enquanto Os conselheiros do ISG usam os relatórios para validar seu próprio conhecimento de mercado e fazer recomendações para a empresa ISG clientes. A pesquisa atualmente abrange provedores que oferecem seus serviços em múltiplas geografias globalmente.

Para mais informações sobre Pesquisa ISG Provider Lens, visite esta página da web.

ISG Research™

ISG Research™ fornece pesquisa por assinatura, consultoria consultoria e evento executive serviços focados nas tendências do mercado e tecnologias disruptivas impulsionando mudança na computação empresarial. A ISG Research oferece orientação que ajuda as empresas a acelerar crescimento e criar mais valor.

O ISG oferece pesquisas especificamente sobre provedores para estado e local governos (incluindo condados, cidades), bem como o ensino superior instituições. Visite: Setor Público.

Para mais informações sobre o ISG Assinaturas de pesquisa, por favor e-mail 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 consultoria tecnológica. Um parceiro commercial confiável para mais de 900 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 IA e 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 1.600 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 isg-one.com.

ISG Provider Lens™

JUNHO DE 2024

RELATÓRIO: CYBERSECURITY – SOLUTIONS AND SERVICES