ISG Provider Lens™

Cybersecurity – Solutions and Services

Extended Detection and Response (XDR)

Uma análise do mercado de segurança cibernética, comparando a atratividade do portfólio do provedor e os pontos fortes competitivos

Customized report courtesy of:

kaspersky

RELATÓRIO DE QUADRANTE | AGOSTO 2023 | BRASIL

Índice

Autor do Relatório: David de Paulo Pereira

No Brasil, serviços e produtos de segurança cibernética têm se tornado cada vez mais imprescindíveis.

O país é o segundo na América Latina com mais ataques cibernéticos, ficando atrás apenas do México. Ou seja, continua sendo um dos mais atacados no mundo. Aliás, os ataques cibernéticos vêm causando danos financeiros, operacionais e reputacionais às vítimas, além de comprometerem a segurança e a privacidade dos dados. E é difícil identificar um setor que não tenha sido atingido por ataques cibernéticos no Brasil: órgãos do Governo, Hospitais, Grupos de Educação, Manufatura, Redes de Varejo e empresas de tecnologia foram atacadas e viraram notícias em vários jornais.

A cibersegurança é uma questão estratégica para garantir a continuidade dos negócios e a confiança dos clientes. Por isso, é fundamental estar preparado para enfrentar as ameaças e minimizar os impactos dos ataques. Com base nos dados do Cert (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), pode-se observar que os ataques cibernéticos tiveram um pico em 2020 e apresentaram uma queda no ano seguinte, mas voltaram a crescer em 2022.

Como a tecnologia continua avançando em ritmo acelerado, o cenário de ameaças à segurança cibernética no Brasil está em constante crescimento. Em 2022, organizações em todo o país enfrentaram uma série de ameaças à segurança cibernética, desde ataques de ransomware a violações de dados e muito mais. Foram diversos os tipos de ameaças à segurança cibernética das quais as empresas no Brasil tiveram que lidar.

Ataques de ransomware: os ataques de ransomware estão se tornando cada vez mais comuns no Brasil e essa tendência deve continuar. Eles são lucrativos para os criminosos, que costumam pedir o pagamento em criptomoedas para dificultar o rastreamento.

No Brasil, cibersegurança é uma **questão estratégica** para garantir a **continuidade de negócios**.

O ransomware é um tipo de malware que criptografa os dados de uma organização, tornando-os inutilizáveis até que um resgate seja pago. Por isso, esses ataques podem ser devastadores para as empresas, causando perda significativa de dados e tempo de inatividade.

Para se proteger contra-ataques de ransomware, as organizações devem investir em tecnologia, mas também repensar processos e fornecer treinamento de conscientização de segurança aos funcionários para ajudá-los a identificar e evitar golpes de phishing.

Ataques à cadeia de suprimentos: Os ataques à cadeia de suprimentos são outra ameaça crescente no Brasil. Neles, os cibercriminosos visam um fornecedor ou fornecedor terceirizado com o objetivo de obter acesso às redes dos clientes do fornecedor. Isso pode ser particularmente perigoso para organizações que dependem muito de vendedores ou fornecedores terceirizados.

Ataques de engenharia social: ataques de engenharia social, como vshing, phishing e spear-phishing, continuam sendo uma ameaça significativa no Brasil. Eles envolvem cibercriminosos enganando os indivíduos para que divulguem informações confidenciais, como credenciais de login ou informações financeiras. Para se proteger contra-ataques de engenharia social, as organizações devem fornecer treinamento de conscientização de segurança aos funcionários para ajudá-los a identificar e evitar esses tipos de golpes.

Ataques baseados em IoT: Com a crescente adoção de dispositivos da Internet das Coisas (IoT), o risco de ataques baseados em IoT também está aumentando. Os dispositivos IoT geralmente são mal protegidos, tornando-os um alvo atraente para os cibercriminosos. Para se proteger contra-ataques baseados em IoT, as empresas devem garantir que os dispositivos IoT estejam devidamente protegidos, com senhas fortes e firmware atualizado.

Ameaças internas: Ameaças internas, como roubo ou sabotagem de funcionários, continuam representando um risco significativo para as organizações no Brasil. Para mitigar esse risco, as empresas devem implementar controles de acesso rígidos e monitorar a atividade dos funcionários em busca de comportamento suspeito.

Em adição ao conjunto de ameaças descrito anteriormente, outros fatores acabam sendo um desafio para a maioria das organizações:

Cenário de ameaças em rápida evolução: as ameaças cibernéticas estão em constante evolução, com novas possibilidades de perigo e métodos de ataque surgindo o tempo todo.

Falta de experiência em segurança cibernética: muitas empresas não possuem a experiência interna necessária para gerenciar com eficácia seus riscos de segurança cibernética. Isso pode dificultar a identificação e mitigação de ameaças cibernéticas, deixando as empresas vulneráveis a ataques.

Aumento da complexidade dos ambientes de TI: À medida que as empresas adotam novas tecnologias, seus ambientes de TI se tornam mais complexos, com uma variedade maior de dispositivos, aplicativos e sistemas para gerenciar. Essa complexidade pode dificultar a proteção efetiva dos dados e da infraestrutura da organização.

Erro humano: os funcionários podem ser um elo fraco nas defesas de segurança cibernética de uma organização, pois podem clicar inadvertidamente em e-mails de phishing, usar senhas fracas ou cair em golpes de engenharia social. Para mitigar esse risco, as empresas devem fornecer treinamento de conscientização de segurança aos funcionários e implementar políticas e procedimentos rígidos de segurança.

Restrições orçamentárias: as soluções de segurança cibernética podem ser caras, então muitas empresas lutam para alocar recursos suficientes para que consigam dar conta delas. Isso pode dificultar o investimento em novas tecnologias e a contratação do conhecimento necessário para gerenciar com eficácia os riscos cibernéticos.

Requisitos de conformidade: as empresas devem cumprir os requisitos regulatórios sobre segurança cibernética, mas eles podem ser complexos e difíceis de entender, além de exigir recursos e conhecimentos significativos. Mesmo assim, as empresas devem garantir que estão em conformidade com esses regulamentos, como a LGPD.

O ISG observou claramente essa evolução no mercado de segurança cibernética no Brasil e em outras regiões, pois os fornecedores tiveram que adaptar sua postura de segurança e arquitetura de solução para melhor atender às necessidades dos clientes por segurança de última geração, avaliando alguns temas principais em quadrantes. Descrevemos abaixo algumas tendências apresentadas por empresas brasileiras e globais.

Identity and Access Management (IAM)

O gerenciamento de identidade e acesso (IAM) é um componente crítico da estratégia de segurança cibernética de uma empresa, pois ajuda a controlar o acesso a dados e sistemas confidenciais. No estudo deste ano observamos algumas tendências em IAM:

IAM baseado em nuvem: as soluções IAM baseadas em nuvem estão se tornando cada vez mais populares, à medida que mais empresas movem seus dados e aplicativos para a nuvem.

IAM de confiança zero**:** o IAM de confiança zero é uma abordagem que pressupõe que todos os usuários e dispositivos não são confiáveis até que sejam verificados.

Governança e administração de identidades (IGA): as soluções IGA estão se tornando cada vez mais importantes à medida que as empresas buscam gerenciar um número crescente de identidades e permissões de acesso em suas redes e sistemas.

Consumer IAM: as soluções de Consumer IAM estão se tornando mais importantes à medida que as empresas buscam fornecer uma experiência de usuário perfeita e segura para os clientes que acessam seus aplicativos e serviços.

Machine-to-machine (M2M) IAM: Com a crescente adoção de dispositivos IoT, as soluções M2M IAM estão se tornando mais importantes.

Para gerenciar com eficiência seus riscos de IAM, as empresas devem se manter atualizadas com as últimas tendências e tecnologias e investir nas soluções e conhecimentos necessários para proteger seus sistemas e dados.

Extended Detection and Response (XDR)

A detecção e resposta estendida (XDR) é uma tecnologia emergente de segurança cibernética que visa melhorar a detecção e resposta a ameaças, integrando várias fontes de dados de segurança e aplicando análises avançadas para identificar e responder a ameaças. Aqui estão algumas das principais tendências em XDR:

Integração com segurança na nuvem: as soluções XDR estão sendo cada vez mais integradas às soluções de segurança na nuvem, à medida que mais empresas movem seus dados e aplicativos para a nuvem.

Automação e orquestração: as soluções XDR estão cada vez mais incorporando recursos de automação e orquestração para ajudar a simplificar os processos de detecção e resposta a ameaças.

Integração de inteligência de ameaças: as soluções XDR estão cada vez mais integrando feeds de inteligência de ameaças para fornecer contexto e priorizar possíveis perigos.

Análise comportamental: as soluções XDR estão cada vez mais incorporando recursos de análise comportamental para ajudar a detectar ameaças que podem não ser visíveis por meio de métodos tradicionais de detecção baseados em assinatura.

Serviços XDR gerenciados: à medida que as soluções XDR se tornam mais complexas, algumas empresas estão recorrendo a serviços XDR gerenciados para ajudá-las a implementar e gerenciar esses recursos.

À medida que as empresas buscam melhorar seus métodos de detecção e resposta a ameaças, é provável que as soluções XDR se tornem uma parte cada vez mais importante de sua estratégia de segurança cibernética.

Technical Security Services

Os serviços técnicos de segurança cibernética abrangem uma ampla gama de serviços que ajudam as organizações a gerenciar os riscos de segurança cibernética. Aqui estão algumas das principais tendências em serviços técnicos de segurança cibernética observadas:

Testes de penetração e avaliações de vulnerabilidade: os testes de penetração e as avaliações de vulnerabilidade estão se

tornando mais importantes à medida que as organizações buscam identificar e corrigir vulnerabilidades em suas redes e sistemas.

Serviços de resposta a incidentes: os serviços de resposta a incidentes estão se tornando mais importantes à medida que as organizações buscam se preparar e responder a incidentes de segurança cibernética.

Treinamento e conscientização de segurança: os serviços de treinamento e conscientização de segurança estão se tornando mais importantes à medida que as organizações buscam melhorar a conscientização e as habilidades de segurança cibernética de seus funcionários.

Automação e orquestração de segurança cibernética: a automação e a orquestração estão se tornando mais importantes nos serviços técnicos de segurança cibernética, pois as organizações buscam simplificar as operações de segurança e responder às ameaças com mais rapidez.

Os serviços técnicos de segurança cibernética estão evoluindo rapidamente à medida que as organizações buscam gerenciar os riscos de segurança cibernética com mais eficiência.

Strategic Security Services

A consultoria em segurança cibernética e os serviços estratégicos ajudam as organizações a desenvolver e implementar estratégias eficazes de segurança cibernética para gerenciar os riscos de segurança cibernética. Aqui estão algumas das principais tendências em consultoria de segurança cibernética e serviços estratégicos observadas no estudo da ISG:

Gestão de riscos: a gestão de riscos está se tornando cada vez mais importante em consultoria de segurança cibernética e serviços estratégicos, pois ajuda as organizações a identificar, avaliar e priorizar seus riscos de segurança cibernética, assim como desenvolver estratégias de mitigação de riscos alinhadas com os objetivos de negócios.

Requisitos de conformidade e regulamentares: os requisitos de conformidade e regulamentares estão se tornando mais complexos, com novos regulamentos, como a LGPD.

Governança de segurança cibernética: a governança de segurança cibernética está se tornando mais importante à medida que as organizações buscam garantir que suas políticas e procedimentos de segurança cibernética sejam eficazes e estejam alinhadas com seus objetivos de negócios.

Desenvolvimento de programas de segurança cibernética: desenvolvimento e programas eficazes de segurança cibernética incluem planos de resposta a incidentes, treinamento de conscientização de segurança e gerenciamento de vulnerabilidades.

Análise de segurança cibernética: a análise de segurança cibernética está se tornando mais importante em consultoria de segurança cibernética e serviços estratégicos.

Os serviços de consultoria de segurança cibernética e os serviços estratégicos estão evoluindo rapidamente à medida que as organizações buscam gerenciar seus riscos de segurança cibernética com mais eficiência.

Managed Security Services (SOC)

Serviços de segurança gerenciados (MSS) são serviços terceirizados de segurança cibernética que fornecem às organizações soluções de segurança abrangentes. Aqui estão algumas das principais tendências observadas no quadrante Serviços Gerenciados de Segurança:

MSS baseado em nuvem: com a crescente adoção da computação em nuvem, os MSS baseados em nuvem estão se tornando mais populares.

Detecção e resposta avançadas de ameaças: os fornecedores de MSS estão usando cada vez mais análises avançadas, aprendizado de máquina e inteligência artificial (IA) para detectar e responder a ameaças com mais rapidez e eficácia.

Segurança de confiança zero: a segurança de confiança zero está se tornando mais importante no MSS à medida que as organizações buscam melhorar sua postura de segurança.

Detecção e resposta gerenciadas (MDR): MDR é uma tendência emergente em MSS que se concentra na detecção e resposta a ameaças de forma mais rápida e eficaz.

Automação e orquestração de segurança: a automação e a orquestração estão se tornando mais importantes no MSS, pois as organizações buscam simplificar suas operações de segurança e responder às ameaças com mais rapidez.

Para gerenciar com eficiência os riscos de segurança cibernética, as organizações devem se manter atualizadas com as últimas tendências e tecnologias em MSS e investir nas soluções e conhecimentos necessários para proteger seus sistemas e dados.

Atualmente, organizações no Brasil e no mundo enfrentam diversos desafios de segurança cibernética, incluindo ataques de ransomware, ataques à cadeia de suprimentos, técnicas de engenharia social, ataques baseados em IoT e ameaças internas. Não basta mais apenas atualizar o antivírus para garantir a segurança da informação. É necessário adotar uma abordagem mais ampla e estratégica para enfrentar esses desafios.

Posicionamento do Fornecedor

Página 1 of 8

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Accenture	Not In	Not In	Not In	Leader	Leader	Leader
Agility	Not In	Not In	Not In	Leader	Not In	Leader
Atos	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger
BluePex	Not In	Contender	Not In	Not In	Not In	Not In
Broadcom	Leader	Leader	Product Challenger	Not In	Not In	Not In
Capgemini	Not In	Not In	Not In	Leader	Leader	Product Challenger
Cato Networks	Not In	Not In	Leader	Not In	Not In	Not In
Check Point	Contender	Product Challenger	Not In	Not In	Not In	Not In
Cipher	Not In	Product Challenger	Not In	Contender	Market Challenger	Product Challenger
Cirion	Not In	Not In	Not In	Not In	Not In	Leader

Posicionamento do Fornecedor

Página 2 of 8

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Cisco	Contender	Contender	Leader	Not In	Not In	Not In
Claranet	Not In	Not In	Not In	Product Challenger	Product Challenger	Rising Star ★
Cloudflare	Not In	Not In	Market Challenger	Not In	Not In	Not In
Compugraf	Not In	Not In	Not In	Contender	Not In	Not In
CrowdStrike	Not In	Leader	Not In	Not In	Not In	Not In
CyberArk	Product Challenger	Not In	Not In	Not In	Not In	Not In
Cybereason	Not In	Product Challenger	Not In	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	Not In	Contender
Edge UOL	Not In	Not In	Not In	Not In	Not In	Leader

Posicionamento do Fornecedor

Página 3 of 8

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Ericom Software	Not In	Not In	Product Challenger	Not In	Not In	Not In
E-TRUST	Leader	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	Not In	Leader	Not In	Not In	Not In
ForgeRock	Product Challenger	Not In	Not In	Not In	Not In	Not In
Fortinet	Contender	Rising Star ★	Product Challenger	Not In	Not In	Not In
GoCache	Not In	Contender	Not In	Not In	Not In	Not In
HackerSec	Not In	Not In	Not In	Not In	Contender	Not In
HPE (Aruba)	Not In	Not In	Rising Star ★	Not In	Not In	Not In

Posicionamento do Fornecedor

Página 4 of 8

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Huge Networks	Not In	Contender	Not In	Not In	Not In	Not In
IBLISS	Not In	Not In	Not In	Not In	Product Challenger	Not In
IBM	Leader	Product Challenger	Not In	Leader	Leader	Leader
iboss	Not In	Not In	Product Challenger	Not In	Not In	Not In
Infinite Networks	Not In	Not In	Contender	Not In	Not In	Not In
ISH	Not In	Not In	Not In	Leader	Leader	Leader
iT.eam	Not In	Not In	Not In	Contender	Not In	Contender
Italtel	Not In	Not In	Not In	Not In	Not In	Contender
Kaspersky	Not In	Leader	Not In	Not In	Not In	Not In
KPMG	Not In	Not In	Not In	Not In	Product Challenger	Not In

Posicionamento do Fornecedor

Página 5 of 8

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Kyndryl	Not In	Not In	Not In	Rising Star ★	Product Challenger	Not In
Logicalis	Not In	Not In	Not In	Leader	Leader	Leader
Lookout	Not In	Not In	Contender	Not In	Not In	Not In
Microsoft	Leader	Leader	Not In	Not In	Not In	Not In
NEC	Not In	Not In	Not In	Not In	Market Challenger	Not In
Netskope	Not In	Not In	Leader	Not In	Not In	Not In
Nextios	Not In	Not In	Not In	Contender	Not In	Not In
NTT Ltd.	Not In	Not In	Not In	Leader	Rising Star ★	Leader
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

Posicionamento do Fornecedor

Página 6 of 8

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Open Systems	Not In	Not In	Contender	Not In	Not In	Not In
OpenText	Rising Star ★	Leader	Not In	Not In	Not In	Not In
Oracle	Contender	Not In	Not In	Not In	Not In	Not In
Palo Alto Networks	Not In	Product Challenger	Leader	Not In	Not In	Not In
Perimeter 81	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
Proofpoint	Not In	Not In	Contender	Not In	Not In	Not In
PwC	Not In	Not In	Not In	Leader	Leader	Not In
Redbelt	Not In	Not In	Not In	Not In	Contender	Not In
RSA	Leader	Not In	Not In	Not In	Not In	Not In

Posicionamento do Fornecedor

Página 7 of 8

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
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
Service IT	Not In	Not In	Not In	Product Challenger	Not In	Not In
Skyhigh Security	Not In	Not In	Product Challenger	Not In	Not In	Not In
SONDA	Not In	Not In	Not In	Market Challenger	Not In	Market Challenger
Sophos	Not In	Product Challenger	Not In	Not In	Not In	Not In
Stefanini	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader
TCS	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In
TDEC	Not In	Not In	Not In	Not In	Not In	Contender
Thales	Product Challenger	Not In	Not In	Not In	Not In	Not In

Posicionamento do Fornecedor

Página 8 of 8

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
TIVIT	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger
Trellix	Not In	Product Challenger	Not In	Not In	Not In	Not In
Trend Micro	Not In	Leader	Not In	Not In	Not In	Not In
T-Systems	Not In	Not In	Not In	Product Challenger	Not In	Leader
Unisys	Market Challenger	Not In	Not In	Not In	Product Challenger	Leader
Versa Networks	Not In	Not In	Leader	Not In	Not In	Not In
VMware	Not In	Leader	Contender	Not In	Not In	Not In
Wipro	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader
Zscaler	Not In	Not In	Leader	Not In	Not In	Not In

Neste estudo foram avaliados os seguintes quadrantes como principais áreas de foco para o IPL **Cybersecurity – Solutions and Services 2023**

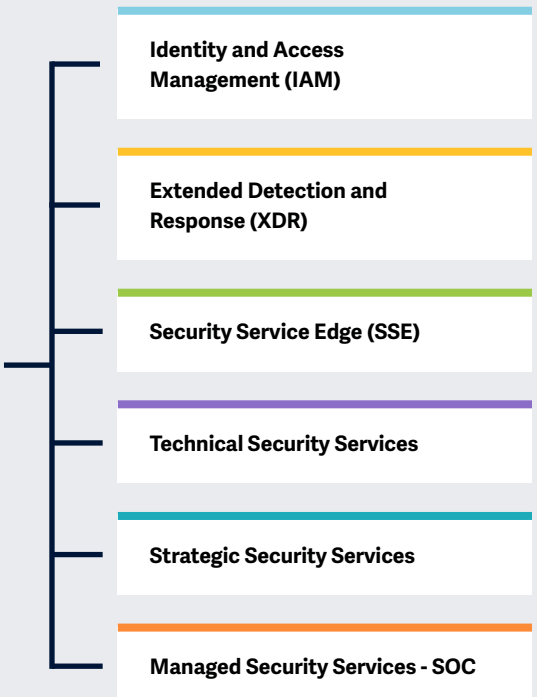


Ilustração simplificada Fonte: ISG 2023

Definição

O ano de 2022 pode ser considerado tumultuado do ponto de vista da segurança cibernética; embora tenha havido diminuição nos incidentes de violação de dados, o ano viu um aumento significativo na sofisticação e gravidade dos ataques.

Em 2022, as empresas aumentaram os investimentos em segurança cibernética e priorizaram iniciativas relevantes para prevenir ataques e melhorar a postura de segurança. Os aprendizados contínuos dos ataques de 2021 levaram executivos e empresas de todos os tamanhos e setores a investir em medidas para responder e sobreviver a ameaças e ataques cibernéticos à segurança cibernética.

Do ponto de vista empresarial, até mesmo as pequenas empresas entenderam o impacto das ameaças cibernéticas e perceberam que são alvos ativos e altamente vulneráveis a ataques cibernéticos. Isso reforçou a necessidade de serviços de segurança especializados e serviços de resiliência cibernética que permitiriam que as empresas se recuperassem e retomassem as operações rapidamente após um incidente cibernético. Os fornecedores de serviços e fornecedores estão, portanto, oferecendo serviços e soluções que auxiliam na recuperação e na continuidade dos negócios.

Do ponto de vista dos cibercriminosos, eles começaram a explorar vulnerabilidades em larga escala, como o Log4shell, e continuaram usando ransomware para interromper as atividades comerciais, visando especificamente a saúde, a cadeia de suprimentos e os serviços do setor público.

Isso levou as empresas a investir em recursos como gerenciamento de identidade e acesso (IAM), prevenção de perda de dados (DLP), detecção e resposta gerenciadas (MDR) e proteção de nuvem e endpoints.

O mercado está mudando para soluções integradas, como borda de serviços de segurança (SSE) e detecção e resposta estendidas (XDR), que utilizam as melhores ferramentas e experiência humana, além de serem aprimoradas com inteligência comportamental e contextual e automação para oferecer uma postura de segurança superior.

Escopo do Relatório

Neste relatório de quadrantes ISG Provider Lens™, o ISG abrange os 6 (seis) seguintes quadrantes para serviços / soluções: Identity and Access Management (IAM), Extended Detection and Response (XDR), Technical Security Services, Strategic Security Services e Managed Security Services - SOC.

Os fornecedores que oferecem soluções de Security Service Edge (SSE) são analisados e posicionados em uma perspectiva global e não em regiões individuais, uma vez que o mercado está em estágios iniciais ainda em maturação.

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

- Transparência sobre os pontos fortes e fracos dos fornecedores de software 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, relacionamentos-chave e considerações de entrada no mercado. Os consultores e clientes corporativos do ISG também usam as informações desses relatórios para avaliar seus relacionamentos existentes com fornecedores 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 gruposalvo 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 o 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:** 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).

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 (XDR)

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.

A agilidade é fundamental na detecção e resposta de ameaças, uma vez que o tempo de acesso do cibercriminoso no ambiente é proporcional aos danos causados. Assim, as empresas buscam plataformas de XDR com ferramentas de inteligência artificial e de automação para diminuir o tempo médio de detecção e resposta a ameaças.

Outra preocupação das organizações são as novas ameaças que surgem constantemente, como novos golpes, novos ataques de engenharia social e novas táticas de ransomware. Os fornecedores estão investindo na integração de suas plataformas XDR com feeds de inteligência, para permitir a atuação da ferramenta contra novas ameaças.

O controle visual da segurança, com painéis e dashboards, é cada vez mais demandado pelas empresas, pois facilita e simplifica a visualização de dados, como comportamentos suspeitos, ativos protegidos e ameaças detectadas.

Diretores 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.

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.

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.

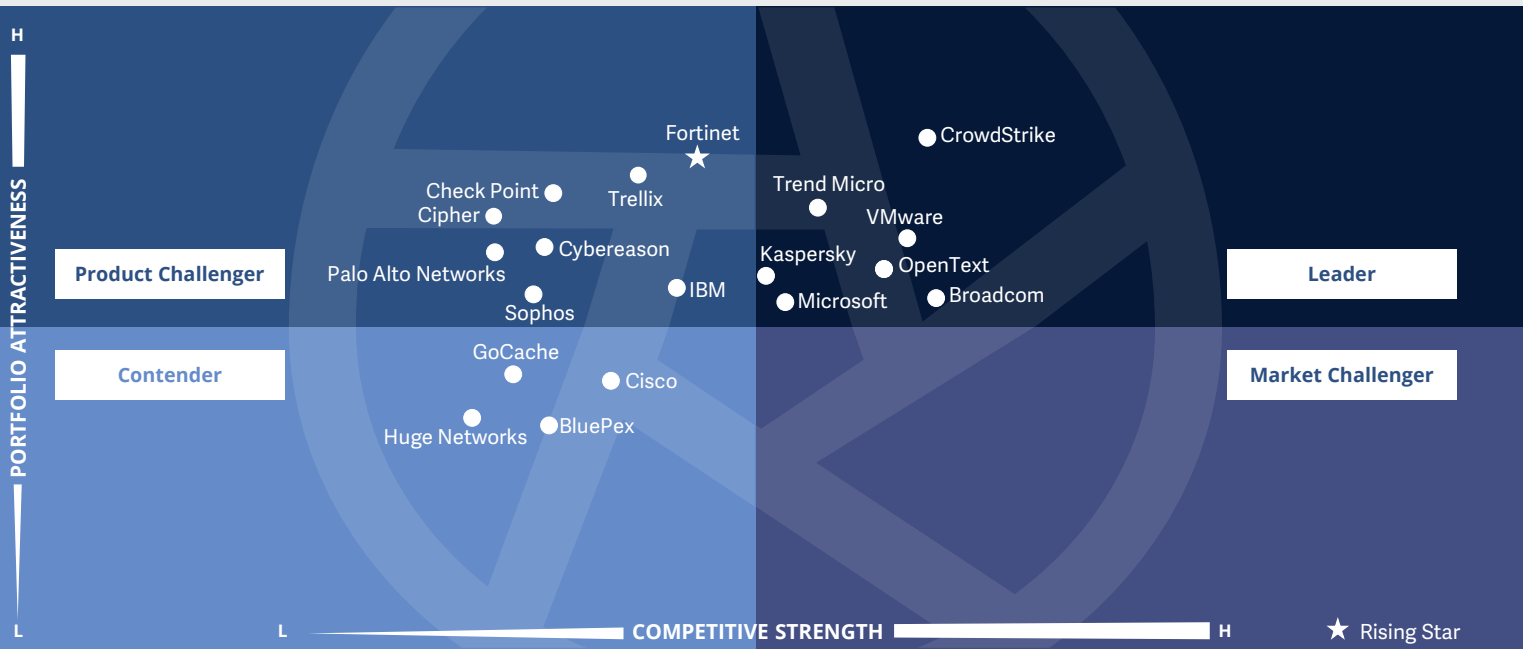
Profissionais de produtos digitais devem ler este relatório para entender como os fornecedores de XDR podem ajudar na estabilização de produtos para aumentar a segurança de seus clientes.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity – Solutions and Services
Extended Detection and Response (XDR)

Brasil 2023



Este quadrante avalia fornecedores de **soluções XDR**, que fornecem software e serviços para monitorar continuamente todos os pontos de extremidade e fornecer visibilidade total. Eles podem **analisar, prevenir e responder a ameaças avançadas**.

David de Paulo Pereira

Definição

Os fornecedores de soluções de XDR avaliados para este quadrante são caracterizados por sua capacidade de oferecer uma plataforma que integra, correlaciona e contextualiza dados e alertas de vários componentes de prevenção, detecção e resposta a ameaças.

A XDR é uma tecnologia fornecida em nuvem, compreendendo soluções de multiponto. Ela usa analytics avançado para correlacionar alertas de várias fontes, inclusive de sinais individuais fracos para permitir detecções precisas. As soluções de XDR consolidam e integram vários produtos e são projetadas para fornecer segurança abrangente do espaço de trabalho, da rede ou da carga de trabalho. Normalmente, as soluções de XDR visam melhorar muito a visibilidade e o contexto da ameaça identificada em toda a empresa. Portanto, essas soluções incluem características específicas, incluindo telemetria e análise de dados contextuais, detecção e resposta.

As soluções de XDR compreendem ainda vários produtos e soluções integrados em um único painel para visualizar, detectar e responder com recursos sofisticados. A alta maturidade de automação e a análise contextual oferecem recursos de resposta exclusivos e personalizados para o sistema afetado e priorizam alertas com base na gravidade em relação a estruturas de referência conhecidas.

Os fornecedores de serviços puros que não oferecem uma solução de XDR baseada em software proprietário não estão incluídos aqui. As soluções de XDR visam reduzir a dispersão de produtos, fadiga de alertas, desafios de integração e despesas operacionais e são particularmente adequadas para equipes de operações de segurança que têm dificuldade em gerenciar um portfólio de soluções de ponta ou obter valor de informações de segurança e gerenciamento de eventos (SIEM) ou solução de segurança, orquestração, automação e resposta (SOAR).

Critério de Elegibilidade

1. A oferta de **XDR** deve ser baseada em **software proprietário** e não em software de terceiros
2. Uma solução de XDR precisa ter dois componentes principais: **XDR de front-end e XDR de back-end**
3. **O front-end deve ter 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**, gerenciamento de identidade, segurança de e-mail, detecção de ameaça móvel, proteção de carga de trabalho em nuvem e identificação de fraude
4. A solução deve fornecer **cobertura e visibilidade abrangentes** e totais de todos os endpoints em uma rede
5. A solução deve demonstrar **eficácia no bloqueio** de ameaças sofisticadas, como as persistentes avançadas, além de **ransomware e malware**
6. A solução deve utilizar a **inteligência de ameaças**, assim como analisar e oferecer **informações em tempo real sobre os perigos que emanam** dos endpoints
7. A solução deve incluir **recursos de resposta automatizada**

Observações

As soluções XDR empregam análises avançadas para investigar alertas de várias fontes, desde sinais individuais fracos até a detecção precisa de ameaças. Essas soluções são projetadas para fornecer segurança abrangente para espaços, redes e cargas de trabalho, integrando vários produtos em uma única plataforma. O principal objetivo das soluções XDR é aumentar a visibilidade das ameaças em uma empresa e fornecer contexto às ameaças identificadas.

Essas soluções incorporam recursos específicos, como telemetria e análise de dados contextuais, assim como detecção e resposta para melhorar os recursos personalizados do sistema afetado. A análise contextual é altamente automatizada e pode priorizar alertas com base na gravidade em relação a estruturas de referência conhecidas.

A maioria das empresas oferece integrações com outras ferramentas de segurança e construiu portfólios em torno dos recursos de detecção e resposta de endpoint. As ofertas de produtos bem-sucedidas geralmente adotam uma abordagem baseada em plataforma, com o objetivo de ser o principal fornecedor de soluções no mercado.

Há uma demanda crescente por soluções XDR que podem fornecer visibilidade em todos os ativos e detectar e responder prontamente às ameaças. Métricas como o tempo médio para responder ou detectar agora são amplamente utilizadas em esforços de marketing para que os principais players se diferenciem dos concorrentes.

De 261 empresas pesquisadas para este estudo, 19 se qualificaram para este quadrante sendo 7 Líderes e uma Rising Star.

Broadcom

A **Broadcom** apresenta uma solução que usa Machine Learning e Inteligência Artificial para oferecer uma ampla cobertura de funcionalidades, incluindo Proteção Adaptativa, Threat Defense, firewall e sistema de prevenção contra invasões, além do Symantec CloudSOC CASB.

CrowdStrike

A solução **CrowdStrike** Falcon oferece vasta experiência em detecção e resposta de endpoint, arquitetura nativa da nuvem para escalabilidade e flexibilidade, visibilidade em tempo real e flexibilidade de aquisição por meio de diferentes bundles, desde a opção básica até a mais avançada.

kaspersky

Com recursos de gerenciamento centralizado, a **Kaspersky** Endpoint Security Suite oferece proteção avançada contra ameaças cibernéticas, incluindo análise de comportamento em tempo real, aprendizado de máquina e verificação baseada em assinatura.

Microsoft

A **Microsoft** oferece uma plataforma integrada para detecção e resposta a ameaças, que inclui o Microsoft Sentinel e o Microsoft Defender, bem como o Microsoft Defender for Cloud. A inovação constante da Microsoft é um destaque em todas as soluções de segurança apresentadas.

Open Text (Microfocus)

A Micro Focus adquiriu a **OpenText**, trazendo tecnologias importantes, como categorias de IA, desenvolvimento de aplicativos e gerenciamento de operações digitais. A solução XDR da ArcSight Intelligence oferece recursos de detecção, integração e personalização de painéis.

Trend Micro

A plataforma **Trend Micro** Vision One oferece uma abordagem de segurança convergente, integrando várias soluções de segurança em uma única plataforma, além de gerenciamento de políticas unificado.

VMware

A solução Carbon Black da **VMware**, inclui o uso de Machine Learning e IA para detecção e resposta a ameaças em tempo real, bem como uma arquitetura nativa multicloud que permite implantar e gerenciar ambientes em várias nuvens.

Fortinet

A plataforma **FortiXDR** oferece uma abordagem de segurança integrada e extensível, com detecção de ameaças orientada por inteligência artificial e aprendizado de máquina. Utiliza um conceito de Security Fabric que integra serviços de segurança FortiGuard de forma nativa para fornecer detecção e aplicação coordenadas em toda a superfície de ataque.

Leader

"A Kaspersky tem uma solução XDR sofisticada para proteção de TI /TO e um portfólio de serviços que abrange da educação em segurança, inteligência de ameaças até soluções que respeitam requisitos de soberania de dados em ambientes on-premises ou nuvem."

David de Paulo Pereira

Kaspersky

Visão Geral

A Kaspersky é uma empresa privada internacional sediada em Moscou, Rússia com sua holding registrada no Reino Unido e sua infraestrutura de processamento de dados localizada na Suíça. A empresa tem subsidiárias em 31 países e possui cerca de 4.000 especialistas altamente qualificados. Suas soluções protegem cerca de 240.000 clientes corporativos com atuação em proteção avançada de Endpoints EDR, XDR, MDR e Cloud nativo e Threat Intelligence. A Kaspersky América Latina, com sede no Brasil é uma entidade empresarial registrada no país desde 2013 e subsidiária da holding Kaspersky Limited, que tem sede no Reino Unido.

Fortalezas

Proteção avançada contra ameaças: O Kaspersky XDR coleta dados de várias fontes fornecendo uma visão completa com integração às ferramentas de segurança existentes proporcionando uma visibilidade unificada e correlação de dados de segurança através de análises avançadas e aprendizado de máquina identificando padrões e anomalias para melhorar a detecção de ameaças e resposta a incidentes.

Gestão Centralizada e políticas personalizáveis: A suíte oferece recursos de gerenciamento centralizado, permitindo monitorar e gerenciar a segurança de endpoints e dispositivos com visibilidade do status de segurança e correção automatizada de problemas. Também permite a criação de políticas personalizáveis adaptadas.

Foco na Região: Com mais de 1.600 parceiros no Brasil e 6.000 na América Latina, uma equipe regional de mais de 130 colaboradores, sendo 64 destes no Brasil A Kaspersky oferece serviços de Resposta a Incidentes, Gerenciamento de SOC e Centro de Pesquisa de Ameaças , com atendimento em português e espanhol, abrangendo de educação de usuários a programas automatizados de conscientização.

Kaspersky Transparency Centers: Os centros em Zurique, Madri, Kuala Lumpur, Roma, Singapura, Tóquio, Utrecht, Woburn (Região de Boston) e São Paulo compartilham informações sobre produtos, código fonte e desempenho com parceiros e governos.

Atenção

A Kaspersky utiliza parceiros para atender o mercado nacional e tem um programa de Loyalty com ofertas de desconto baseadas em certificações resultado de vendas. Mas alguns parceiros oferecem soluções de outros fabricantes, podendo resultar em uma condução por critérios diversos conduzidos pelo parceiro.

Apêndice

O estudo de pesquisa "ISG Provider Lens™ Cybersecurity – Solutions and Services 2023" 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™.

Autor principal:
David Pereira

Analista de Pesquisa:
Gabriel Sobanski

Analistas de Dados:
Rajesh Chillappagari and Shilpashree N

Gerente de Projetos:
Donston Sharwin

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 abril de 2023, 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

Analista Lider

David de Paulo Pereira
Analista Lider

David de Paulo Pereira é o autor principal de vários relatórios de IPL para o mercado brasileiro. É um profissional com experiência executiva comprovada em transformação digital, gestão de equipes, projetos e serviços. Atuou em ambientes complexos, como pós fusão de empresas, estabelecimento de modelos de governança, padronização de métodos e processos de trabalho. Possui grande experiência em ambientes multiculturais adquirida em empresas privadas, públicas, multinacionais e familiares, no Brasil e no exterior.

Suas principais habilidades incluem profundo conhecimento da Indústria 4.0: IOT, Nuvem, Big Data, Analytics, RPA, planejamento estratégico, inovação tecnológica, gestão de portfólio e gestão de mudanças. Antes de ingressar na TGT/ISG, ele trabalhou como CIO e CTO para uma empresa de software do Reino Unido, foi Diretor Executivo responsável pela Prática de Transformação de TI na EY, além de atuar como CIO e CTO para empresas globais como Solvay, Jakko Poyry.

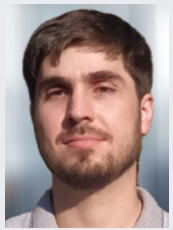
Autor

Gowtham Kumar Sampath
Diretor Adjunto e Analista Principal

Gowtham Sampath é gerente sênior do ISG Research, responsável pela elaboração de relatórios de quadrantes do ISG Provider LensTM 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 analisa e reduz a lacuna entre fornecedores de análise de dados e empresas, abordando oportunidades de mercado e melhores práticas.

Em seu papel, ele também trabalha com consultores para atender às solicitações de clientes corporativos para requisitos de pesquisa ad hoc para serviços de TI, em todos os setores. Ele também é responsável por pesquisas de liderança de pensamento, whitepapers, artigos sobre tecnologias emergentes do setor bancário nas áreas de automação, experiência em DX e UX, bem como o impacto da análise de dados em diferentes segmentos de mercado.

Analista de Pesquisa

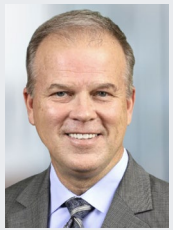


Gabriel Sobanski
Analista de Pesquisa

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 Proprietário do produto



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 parceiro, analista principal e chefe global do 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™

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 comercial 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 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™

AGOSTO, 2023

RELATÓRIO: CYBERSECURITY – SOLUTIONS AND SERVICES