ISG Provider Lens®

Cybersecurity — Services and Solutions

Análise do mercado de segurança cibernética: portfólio de fornecedores e forças competitivas

CATÁLOGO | JANEIRO DE 2026 | AUSTRÁLIA, BRASIL, FRANÇA, ALEMANHA, SUÍÇA, REINO UNIDO, EUA E SETOR PÚBLICO DOS EUA

Índice

Introdução

Para a cibersegurança em 2026, prevê-se ameaças mais sofisticadas, expansão das exigências regulamentares e rápida transição para modelos de defesa orientados por inteligência. Há uma pressão eminente em todos os setores para se proteger arquiteturas e infraestrutura crítica cada vez mais distribuídas, resguardar dados sensíveis em ambientes híbridos e responder com efetivida ao aumento de ataques habilitados por IA. Enquanto isso, conselhos de administração e órgãos reguladores buscam resiliência cibernética e eficácia dos controles, abrindo caminho para programas de segurança como parte das agendas de transformação digital.

Nesse contexto, o mercado se reorganiza em domínios de capacidade bem definidos. Enquanto TSS garantem integridade da configuração, implementações seguras e reforço contínuo da segurança, SSS ganham importância à medida que executivos priorizam cibersegurança com governança, gestão de riscos e alinhamento arquitetônico.

SOCs de última geração e serviços de MDR também ganham força com demanda por monitoramento de ameaças 24/7, análises com suporte de IA e modelos de resposta baseados em resultados. Além disso, gestão de vulnerabilidades baseada em risco reforça segurança preventiva, priorizando exposições com base no contexto de negócios e em informações sobre as táticas de ataques. Por fim, consultoria em criptografia pós-quântica entra no mercado conforme as organizações se preparam e organizam inventários criptográficos e definem estratégias de transição para salvaguardar a confidencialidade dos dados a longo prazo.

Estudo do IPL abrange, entre outros, domínios de capacidade mencionados e oferece visão abrangente de como fornecedores se diferenciam em ambiente caracterizado por velocidade, inteligência e resiliência.

Key focus areas for Cybersecurity – Services and Solutions 2026.

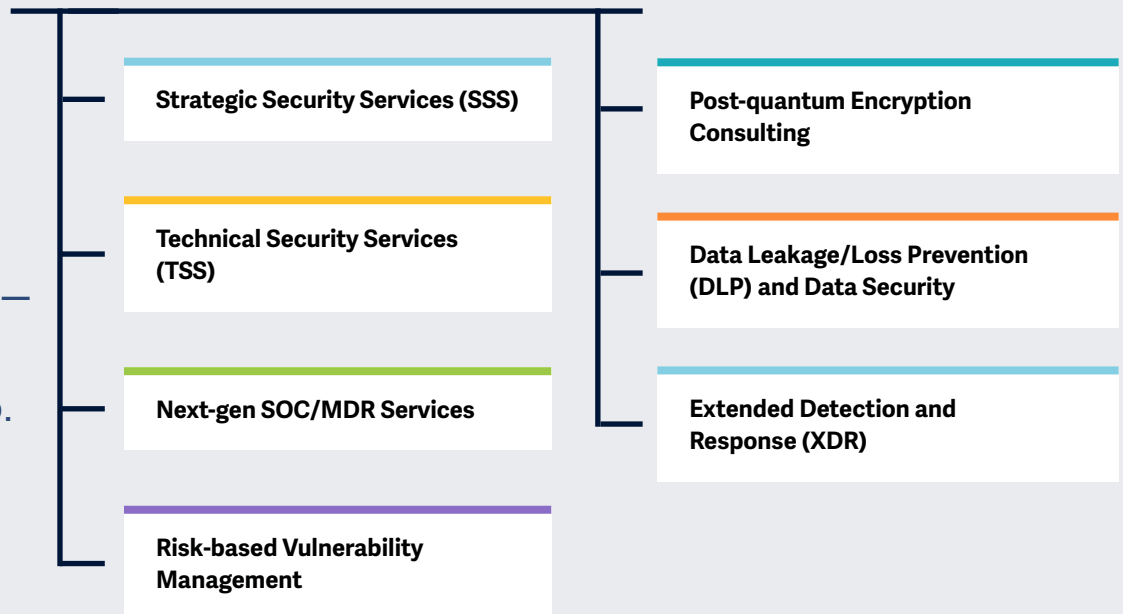


Ilustração simplificada Fonte: ISG 2026

Este estudo ISG Provider Lens® Cybersecurity — Services and Solutions proporciona para tomadores de decisão de negócios e TI:

- Transparência sobre os pontos fortes e fracos dos fornecedores de serviço relevantes.
- Posicionamento diferenciado de fornecedores por segmentos com base em seus pontos fortes competitivos e atratividade de portfólio.
- Foco em diferentes mercados, incluindo Austrália, Brasil, França, Alemanha, Suíça, Reino Unido, EUA e o Setor Público dos EUA.
- Características específicas de cada país: Consultoria em criptografia pós-quântica na Alemanha e nos EUA, análise de XDR e gerenciamento de vulnerabilidades baseado em risco no Brasil, e análise de DLP na Alemanha.

Nosso estudo serve como uma importante base de tomada de decisão para posicionamento, 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 compromissos em potencial.

Definição

Avalia fornecedores de cibersegurança voltados à consultoria, com foco em estratégia, governança, gestão de riscos e transformação organizacional segura para ambientes de TI e OT. Eles avaliam maturidade da segurança, quantificam riscos, definem modelos operacionais alvo e desenvolvem estratégias, políticas e roteiros de cibersegurança alinhados a objetivos de negócios e requisitos regulatórios. Serviços incluem auditorias, avaliações, programas de conscientização sobre segurança, planejamento de continuidade de negócios, exercícios simulados e consultoria na seleção de tecnologia. Eles também empregam consultores experientes que ajudam empresas a planejar programas, melhorar governança e desenvolver capacidades, incluindo modelos de vCISO para liderança estratégica contínua ou sob demanda. Ao contrário dos TSS, que enfatizam a integração prática e a engenharia, fornecedores de SSS focam em resultados de consultoria em vez de monitoramento operacional ou execução de produtos proprietários.

Critérios de Qualificação

1. Prestar **consultoria de segurança independente de fabricante**, com avaliações de maturidade, desenvolvimento de estratégias, elaboração de políticas, modelos de governança e criação de roteiros.
2. Ter competências estratégicas como quantificação de riscos, conformidade regulatória, seleção de fornecedores, planejamento de continuidade de negócios e consultoria ampla em riscos cibernéticos.
3. **Aplicar estruturas reconhecidas** e cumprir normas (como ISO 27000, NIST CSF, CIS Controls) ao orientar programas empresariais.
4. **Prestar pelo menos um dos** serviços de segurança estratégica **acima mencionados** na região alvo, com consultores qualificados e certificados.
5. Ter **evidências documentadas de projetos** que melhoraram postura de segurança, estruturas de governança, prontidão para conformidade ou tomada de decisão baseada em risco do cliente.
6. Fornecer **metodologias de consultoria estruturadas**, modelos ou manuais para avaliações, planejamento estratégico ou transformação organizacional.
7. Operar como **fornecedores de consultoria**, em vez de fornecedores de produtos, permitindo o uso de estruturas ou ferramentas proprietárias que apoiem a prestação de serviços de consultoria.
8. **Não** focar exclusivamente em produtos ou soluções proprietários

Definição

Avalia fornecedores que projetam, integram, implementam e modernizam tecnologia de segurança de TI e OT em ambientes com vários fornecedores. Serviços incluem implementação e configuração de controles de segurança para gestão de identidade e acesso, nuvem e data centers, SASE/SSE, endpoints, redes, tecnologia operacional (OT) e ICS, além de áreas relacionadas. Fornecedores usam arquiteturas de referência, estruturas de automação e aceleradores proprietários para transformações lideradas por engenharia, que simplificam implementação e aumentam controle.

Têm parcerias sólidas com fornecedores de segurança, certificações especializadas e dão suporte a tarefas do ciclo de vida: reforço de segurança, otimização, aplicação de patches e gestão de dispositivos. Ao contrário dos SSS, que se concentram em consultoria e governança, os TSS enfatizam execução técnica prática. Não oferecem monitoramento baseado em SOC ou operações de MDR, mas podem fornecer serviços tradicionais de segurança gerida.

Critérios de Qualificação

1. Ter experiência em **projetar, integrar e implementar** tecnologias de segurança de TI e/ou OT, com certificações de múltiplos fornecedores e parcerias com OEMs.
2. Implementar **aceleradores, ferramentais proprietários ou arquiteturas de referência** que melhorem a implementação, interoperabilidade e tempo de retorno do investimento.
3. Contratar **engenheiros e arquitetos certificados**, com experiência em configurar, personalizar e otimizar soluções de segurança em ambientes de nuvem, redes, endpoints e OT.
4. Ter **abordagem estruturada e metodológica** para avaliar, selecionar e integrar tecnologias de segurança alinhadas com requisitos do cliente, perfis de risco e restrições arquitetônicas.
5. Fornecer **serviços de engenharia de ciclo de vida**, como gestão de configuração, ajuste de políticas, aplicação de patches, reforço de controles e modernização de tecnologia.
6. Apresentar **estudos de caso** documentados com implantações ou transformações bem-sucedidas de tecnologias de segurança na região-alvo.
7. Operar como **integradores orientados a serviços**, em vez de ISVs independentes, permitindo aceleradores proprietários ou ferramentas desenvolvidas internamente que suportem a entrega de serviços.
8. **Não focar** apenas em **produtos** ou soluções **proprietários**

Definição

Este quadrante avalia os fornecedores de serviços que oferecem monitoramento contínuo e serviços de MDR por meio de SOCs. Suas ofertas abrangem todo o ciclo de vida do incidente, incluindo detecção, triagem, investigação, contenção e remediação coordenada. Os fornecedores integram e operam tecnologias de segurança modernas, aplicam inteligência de ameaças e análises avançadas e oferecem busca de ameaças automatizada e conduzida por humanos para fortalecer a resiliência empresarial. Os serviços SOC/MDR de última geração combinam operações de segurança gerenciadas com análises inovadoras orientadas por IA, triagem autônoma e orquestração de segurança, automação e resposta (SOAR) para reduzir os tempos de resposta e melhorar a visibilidade das ameaças em ambientes de TI e OT.
Eles apoiam modelos de gestão compartilhada e não se concentram em consultoria estratégica ou implementação de tecnologia, que se enquadram no escopo do SSS e do TSS, respectivamente.

Critérios de Qualificação

1. Prestar serviços **de monitoramento, detecção e resposta** 24 / 7, por **SOCs próprios**, em ambientes de TI e/ou OT.
2. Ter **capacitações específicas para MDR**, com análise comportamental, integração de inteligência de ameaças com reconhecimento de LLM, busca de ameaças automatizada e conduzida por humanos e engenharia de detecção avançada.
3. **Operar e gerenciar** sistemas de Gestão de Informações e Eventos de Segurança (SIEM), SOAR, EDR, NDR e outras tecnologias de segurança relevantes, com suporte de certificações OEM.
4. Ter **abordagem estruturada de resposta a incidentes**, com triagem, investigação, contenção, coordenação de remediação e melhoria pós-incidente.
5. Usar análises **baseadas em IA**, agentes de triagem autônomos e fluxos de trabalho SOAR para acelerar detecção e reduzir tempo médio de resposta (MTTR).
6. Ter **modelos de serviço cogeridos** com equipes de empresas para visibilidade compartilhada, colaboração entre analistas e processos de resposta conjunta.
7. Apresentar **casos de referência** com melhorias mensuráveis em cobertura de detecção, eficiência de resposta ou resiliência operacional na região alvo.
8. **Não** focar apenas em produtos proprietários, mas gerenciar e operar melhores ferramentas de segurança do mercado.

Definição

Este quadrante avalia fornecedores de serviços contínuos de gestão de vulnerabilidades baseados em risco em ambientes de TI, nuvem, aplicativos e infraestrutura digital. Eles identificam, avaliam e priorizam vulnerabilidades com base no potencial de exploração exposição e impacto nos negócios, e não apenas em pontuações de gravidade. Seus serviços combinam descoberta automatizada, testes de penetração, testes de segurança de aplicativos e análise contextual de riscos para lidar com técnicas de ataque em rápida evolução, incluindo aquelas aceleradas pela GenAI, e com o aumento da atividade de ransomware. A gestão de vulnerabilidades baseada em risco facilita a visibilidade contínua dos ativos internos e externos à internet, permite a priorização da correção alinhada às táticas de ataque reais e à criticidade dos negócios, e ajuda as empresas a reduzir a exposição em cenários tecnológicos em rápida evolução por meio de observabilidade, avaliação, reteste e recalibração de riscos contínuos.

Critérios de Qualificação

1. Fornecer **serviços contínuos de avaliação de vulnerabilidades** que priorizem descobertas com base na explorabilidade, exposição e impacto nos negócios, e não apenas em métricas estáticas de gravidade.
2. Fornecer **serviços de teste** em aplicações web e mobile, APIs, redes internas, ambientes de nuvem (containers, Kubernetes/ K8S e Docker), ATMs, URAs, IoT e outros ativos expostos.
3. Aplicar **métodos de teste reconhecidos**, como testes de penetração, DAST, SAST, IAST e técnicas relacionadas, combinando ferramentas automatizadas e validação manual por especialistas.
4. Alinhar **descobertas e relatórios de vulnerabilidades** com padrões e estruturas relevantes, como ISO 27001, NIST SP 800-53, PCI DSS, SOC 2 e requisitos regulamentares ou específicos do setor aplicáveis.
5. Oferecer **retestes, acompanhamento de remediação e reavaliação contínua de riscos** para refletir mudanças na exposição, inteligência de ameaças e progresso na mitigação.
6. Contratar **profissionais de segurança**, como hackers éticos (CEHs), profissionais certificados em segurança ofensiva (OSCPs) e profissionais de segurança de sistemas de informação (CISSPs), além de especialistas com certificações CompTIA PenTest+ ou GIAC, para garantir a consistência na qualidade dos serviços.

Post-quantum Encryption Consulting

Definição

Quadrante avalia fornecedores de consultoria que auxiliam empresas na preparação e execução da transição criptográfica necessária para mitigar riscos associados à computação quântica. Eles avaliam dependências criptográficas em ambientes de TI, OT, IoT e cadeia de suprimentos digital, incluindo gestão de estoque, identificação de algoritmos vulneráveis a ataques quânticos e exposição a ameaças de *coleta imediata e descriptografia posterior*. Desenvolvem estratégias de criptografia pós-quântica (PQC) baseadas em risco, projetam roteiros de migração e criptografia híbrida e oferecem consultoria de adoção de padrões pós-quânticos emergentes alinhados com NIST, Escritório Federal de Segurança da Informação (BSI) e outros órgãos reguladores. Consultoria da PQC aborda impactos na gestão de chaves, sistemas de identidade, comunicações, aplicações e arquiteturas de infraestrutura, permitindo que organizações planejem transformações criptográficas compatíveis, escaláveis e resilientes ao futuro.

Critérios de Qualificação

1. Realizar **avaliações de risco criptográfico e quântico**, incluindo o inventário de ativos criptográficos, algoritmos e uso de chaves em ambientes de TI, OT, IoT, nuvem, rede e aplicativos.
2. Demonstrar **capacidade de consultoria no desenvolvimento de estratégias de PQC**, incluindo roteiros de migração faseada, planejamento de criptografia híbrida e análise de dependências.
3. Prestar serviços de consultoria alinhados com as **normas e diretrizes emergentes**, como NIST PQC, BSI TR-02102, ETSI e as normas ISO/IEC relevantes.
4. Avaliar os **impactos na gestão de chaves**, infraestrutura de chaves públicas (PKI), sistemas de identidade e acesso, comunicações seguras e arquiteturas de aplicativos.
5. Apresentar evidências de **compromisso com clientes relacionados à PQC**, projetos-piloto, simulações ou provas de conceito abordando a redução de riscos orientada pela computação quântica.
6. Oferecer serviços de consultoria imparciais em relação a fornecedores, demonstrando conhecimento dos ecossistemas tecnológicos relevantes e das implementações criptográficas.
7. **Apoiar conformidade** com exigências governamentais e atingir os objetivos das iniciativas de transição criptográfica específicas do setor ou nacionais.

Definição

Avalia fornecedores ISVs com soluções proprietárias de DLP e segurança de dados, disponibilizadas como software local, plataformas em nuvem ou SaaS. Tais produtos permitem descoberta, classificação e monitoramento de dados sensíveis em endpoints, redes, serviços em nuvem e sistemas de armazenamento, além de aplicar controles baseados em políticas para impedir acesso não autorizado ou exfiltração de dados. Tecnologias DLP modernas integram reforço da segurança dos dispositivos, controle de aplicativos e análise comportamental para evitar uso indevido de dados nos endpoints e aplicar políticas até em ambientes offline ou não geridos.

Fornecem governança centralizada, relatórios e suporte à conformidade para proteger dados estruturados e não estruturados ao longo o ciclo de vida. Em cenário de TI distribuído com riscos elevados de violações internas e de fluxo de dados, são a principal proteção para ativos de informação críticos e garantir práticas consistentes de tratamento de dados.

Critérios de Qualificação

1. Fornecer um **produto proprietário de DLP ou segurança de dados** (sem mecanismos de DLP de terceiros incorporados)
2. **Suporte a arquiteturas essenciais**, como ambientes de endpoint, rede, nuvem e armazenamento.
3. **Detectar, classificar e proteger** dados estruturados e não estruturados em repouso e em trânsito.
4. Oferecer **funções de gestão centralizadas**, incluindo controles de políticas, relatórios e configuração.
5. **Permitir** a descoberta de dados, o monitoramento em tempo real e a aplicação de políticas.
6. **Demonstrar** implantações em escala empresarial e adoção documentada pelo cliente.

Definição

Este quadrante avalia os ISVs que desenvolvem plataformas XDR proprietárias, integrando capacitações de telemetria, análise e resposta em endpoints, redes, identidades, cargas de trabalho em nuvem e aplicativos. Essas soluções correlacionam e contextualizam dados de múltiplos controles de segurança para aprimorar a precisão da detecção, reduzir a fadiga de alertas e fortalecer a eficiência operacional. As plataformas XDR modernas unificam a visibilidade das ameaças em uma única interface, aplicam análises comportamentais e de ML e automatizam ações de resposta com base na gravidade e no contexto de negócios. Elas operam como arquiteturas baseadas em nuvem ou híbridas, com uma camada de sensores front-end definida e um mecanismo de análise e orquestração back-end. À medida que as empresas buscam consolidar ferramentas e aprimorar a maturidade de detecção, o XDR serve como uma base estratégica para uma defesa coordenada e orientada por inteligência.

Critérios de Qualificação

1. Fornecer uma **plataforma XDR proprietária** (sem depender de mecanismos XDR de terceiros)
2. Incluir uma **interface XDR definida** (integração multissensor) e uma interface XDR de back-end (análise, correlação e orquestração).
3. **Integrar pelo menos três** sensores nativos ou fortemente acoplados, por exemplo, plataforma de proteção de endpoints/EDR (EPP), NDR, identidade, e-mail, dispositivos móveis ou proteção de cargas de trabalho em nuvem.
4. Oferecer **visibilidade unificada** em endpoints, redes e ambientes de nuvem
5. Demonstrar **capacidade de detectar e bloquear ameaças sofisticadas**, como ameaças persistentes avançadas (APTs), ransomware e malware avançado.
6. **Utilizar inteligência de ameaças**, análises comportamentais e correlações de telemetria em tempo real.
7. Fornecer ações de resposta **automatizadas ou semiautomatizadas** com impacto mensurável

Quadrantes Por Região

Como parte deste estudo de quadrante do ISG Provider Lens®, estamos apresentando sete quadrantes a seguir, sobre Cybersecurity — Services and Solutions 2026

Quadrant	Austrália	Brasil	França	Alemanha	Suíça	Reino Unido	EUA	Setor Público dos EUA
Strategic Security Services (SSS)	✓	✓	✓	✓	✓	Grandes e Médias	Grandes e Médias	✓
Technical Security Services (TSS)	✓	✓	✓	✓	✓	Grandes e Médias	Grandes e Médias	✓
Next-gen SOC/MDR Services	✓	Grandes e Médias	✓	Geral e Médias	Geral, Grandes e Médias	Grandes e Médias	Grandes e Médias	✓
Risk-based Vulnerability Management		✓						
Post-quantum Encryption Consulting				✓			✓	
Data Leakage/Loss Prevention (DLP) and Data Security				✓				
Extended Detection and Response (XDR)		✓						

Fase de pesquisa entre janeiro e junho de 2026 com levantamento, avaliação, análise e validação. Resultados serão apresentados à imprensa em julho de 2026.

Milestones	Início	Fim
Lançamento da Pesquisa	7 de janeiro de 2026	
Fase de Pesquisa	7 de janeiro de 2026	13 de fevereiro de 2026
Chamada de webinar	12 de janeiro de 2026	
Prévia dos Resultados	Maio de 2026	Junho de 2026
Comunicado à Imprensa e Publicação	Julho de 2026	

Consulte a agenda de **investigação do ISG Provider Lens® 2026** para ver e transferir a lista de outros estudos realizados pelo ISG Provider Lens®

Acesso ao Portal On-linel

Você pode visualizar/baixar o questionário aqui usando as credenciais que você já criou ou consultar as instruções no e-mail de convite para gerar uma nova senha. Aguardamos a sua participação!

Guia dos Compradores

A ISG Software Research, anteriormente denominada "Ventana Research", oferece insights do mercado ao avaliar fornecedores de tecnologia e produtos por meio de seus Guias dos Compradores As descobertas são extraídas da análise com base em pesquisa das categorias de produto e experiência do cliente, ranqueamento e classificação de fornecedores de software e produtos para ajudar a tornar os processos de tomada de decisão e seleção para tecnologia mais fáceis.

Durante o lançamento do Cybersecurity — Services and Solutions IPL, gostaríamos de aproveitar a oportunidade para chamar sua atenção para pesquisas e insights relacionados que a ISG Research publicará em 2025. Para mais informações, consulte o cronograma de pesquisa do Guia dos Compradores.

Isenção de Responsabilidade de Produção de Pesquisa

O ISG coleta dados para fins de condução de pesquisas e criação de perfis de fornecedores/fabricantes de serviços. Os perfis e dados de suporte são usados pelos consultores do ISG para fazer recomendações e informar os seus clientes sobre a experiência e as qualificações de fornecedores/fabricantes aplicáveis para a terceirização do trabalho identificado pelos clientes. Esses dados são coletados como parte do processo ISG FutureSource™ e do processo de Qualificação de fornecedores candidatos (CPQ). O ISG pode optar por utilizar apenas esses dados coletados referentes a determinados países ou regiões para a educação e propósitos de seus consultores e não produzir relatórios do ISG Provider Lens™. Essas decisões serão tomadas com base no nível e integridade das informações recebidas diretamente dos fornecedores/fabricantes e na disponibilidade de analistas experientes para esses países ou regiões. As informações enviadas também podem ser usadas para projetos de pesquisa individuais ou para apresentação de notas que serão escritas pelos analistas líderes.

ISG Star of Excellence™ – Chamada para indicações

O Star of Excellence é um reconhecimento independente da excelente prestação de serviços com base no conceito de opinião do consumidor. O ISG desenvolveu o programa Star of Excellence para coletar feedback do cliente sobre o sucesso dos fornecedores de serviços em demonstrar os mais altos padrões de excelência no atendimento ao cliente e centrado no consumidor.

A pesquisa global é sobre serviços associados a estudos IPL. Em consequência, todos os Analistas do ISG recebem continuamente informações sobre a experiência do cliente de todos os fornecedores de serviços pertinentes. Essas informações são adicionadas ao feedback do consultor existente em primeira mão, as quais o IPL aproveita em sua abordagem de consultoria conduzida por profissionais.

Os fornecedores são convidados a indicar seus clientes para participar. Assim que a indicação for enviada, o ISG enviará uma confirmação por correio para ambas as partes. É evidente que o ISG mantém o anonimato de todos os dados dos consumidores e não os compartilha com terceiros.

Nossa visão para a Star of Excellence é sermos reconhecidos como o reconhecimento do setor líder pela excelência no atendimento ao cliente, e servirá como referência para medir os sentimentos dos clientes. Para garantir que seus clientes selecionados concluam o feedback para sua participação, use a seção de "Indicados (para Fornecedores)" no site web do Star of Excellence™.

Criamos um e-mail onde você pode direcionar qualquer dúvida ou fazer comentários. Este e-mail será verificado diariamente. Aguarde até 24 horas para uma resposta.

Eis o endereço de e-mail:
star@cx.isg-one.com

ISG Star of Excellence

O estudo de pesquisa "ISG Provider Lens® Cybersecurity — Services and Solutions 2026 - 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

Analista Líder:
Frank Heuer, Bhuvaneshwari Mohan, Yash Jethani, Benoit Scheuber, Andrew Milroy e João Mauro

Analista de Pesquisa:
Monica K e Rafael Rigotti

Analista de dados:
Rajesh Chillappagari e Laxmi Sahebrao Kadve

Gerente de Projetos:
Shreemadhu Rai B

A Information Services Group, Inc. é exclusivamente responsável pelo conteúdo deste 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 estudo incluirão dados de pesquisas do programa ISG Provider Lens®, programas contínuos do ISG Research, entrevistas com consultores do ISG, apresentações com fornecedores de serviços e análise de informações de mercado disponíveis ao público de várias fontes. O ISG reconhece a passagem de tempo e os possíveis desenvolvimentos de mercado entre a investigação e a publicação, em termos de fusões e aquisições e reconhece que essas mudanças não serão refletidas nos relatórios deste estudo.

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

Contatos Para Este Estudo

Patrocinador do estudo

Heiko Henkes

Diretor e Analista Principal

Frank Heuer

Analista Líder – Alemanha, Suíça

Bhuvaneshwari Mohan

Analista Líder – Reino Unido, Setor Público dos EUA

Yash Jethani

Analista Líder – EUA

Benoit Scheuber

Analista Líder – França

Andrew Milroy

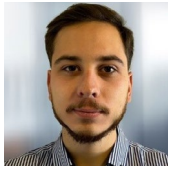
Analista Líder – Austrália

João Mauro

Analista Líder – Brasil

Monica K

Analista de Pesquisa



Rafael Rigotti

Analista de Pesquisa

Rajesh Chillappagari

Analista de dados

Laxmi Sahebrao Kadve

Analista de dados

Shreemadhu Rai B

Gerente de Projetos

Programa de Envolvimento de Consultores do ISG Provider Lens®

O ISG Provider Lens® oferece avaliações de mercado incorporando insights de profissionais, refletindo foco regional e pesquisa independente. O ISG garante o envolvimento do consultor em cada estudo para cobrir os detalhes de mercado relevantes alinhados às respectivas linhas de serviço/tendências de tecnologia, presença do fornecedor de serviços e contexto empresarial.

Em cada região, o ISG tem líderes de pensamento especialistas e consultores respeitados que conhecem os portfólios e ofertas dos fornecedores, bem como os requisitos da empresa e as tendências do mercado. Em média, três consultores participam como parte do processo de revisão de qualidade e consistência de cada estudo.

O consultor garante que cada estudo reflita a experiência dos consultores ISG no campo, o que complementa a pesquisa primária e secundária conduzida pelos analistas.

Os consultores do ISG participam de cada estudo como parte do grupo de consultores e contribuem em diferentes níveis, dependendo de sua disponibilidade e especialização.

Os consultores:

- Ajudam a definir e validar quadrantes e questionários,
- Aconselham sobre a inclusão de fornecedores de serviços, participam de chamadas de apresentação,
- Fornecem as suas perspectivas sobre as classificações dos fornecedores de serviços e revisam os rascunhos dos relatórios.

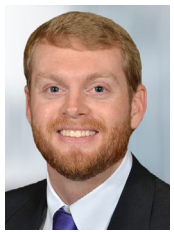
Consultores do ISG para este estudo

Doug
Saylors

Sócio e Líder da Segurança Cibernética do ISG

David
Gordon

Consultor Principal de Segurança Cibernética



Jason
Stading

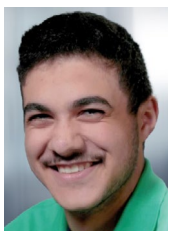
Consultor Principal de Segurança Cibernética

Brendan
Prater

Gerente de Consultoria de Segurança Cibernética

Christophe
deBoisset

Gerente de Consultoria



Marco
Ezzy

Consultor de Segurança Cibernética

Empresas convidadas

Se sua empresa estiver listada nesta página ou você achar que sua empresa deveria estar listada, entre em contato com o ISG para garantir que temos a(s) pessoa(s) de contato correta(s) para participar ativamente desta pesquisa.

* Classificado na iteração anterior

8com
Absolute Software*
AC3*
Accenture*
Acronis*
Actar (Peers Group)
ActioNet*
Addvalue
Advens*
Agility Networks*
Airbus Protect*
Aizoon*
Akamai Technologies
All for One Group*
AlmavivA*
Almond*
Alten*
Amazon Web Services
Appdome
Apura Cyber Intelligence S/A
Arcon
Arctic Wolf Networks, Inc.
Asper*
Atos*
Aveniq*
Avertium*
Avivatec
Axians*
Axur
Azion
BDO
Bechtle/Apixit*
Berghem
BeyondTrust
BIP
Bitdefender
Blaze Information Security
Bluepex*
BlueVoyant*
Brainloop*
Bravo GRC
Brennan IT*
Bricon
Bridewell*
Broadcom*
BT*
CANCOM*
Capgemini*
Capita*
CDW*
Century Data
CGI*
Check Point Software*
CI&T*
Cipher*
Cirion Technologies*
Cisco*
Citrix
Claranet*
Claro empresas

Empresas convidadas

Se sua empresa estiver listada nesta página ou você achar que sua empresa deveria estar listada, entre em contato com o ISG para garantir que temos a(s) pessoa(s) de contato correta(s) para participar ativamente desta pesquisa.

* Classificado na iteração anterior

Clavis*
ClearSale
Cloud Target*
CloudFlare
Cognizant*
Combate a Fraude (Caf)
Compugraf
Computacenter*
Consort Group*
Controlware*
CoSoSys (Netwrix)*
C-Risk
Critical Start*
Crowdstrike*
CTM*
CyberArk
CyberProof*
CyberSecOp*
Cyderes*
Cyera
Cynet Security Ltd.
Darktrace
Data#3*
Datacom*
DATAGROUP*
dataRain
Data-Sec
deepwatch, Inc.
Defcon1
Delfia
Delinea
Deloitte*
Deutsche Telekom*
Devoteam*
Dfense
DIGITALL*
DriveLock*
DXC Technology*
EcoTrust*
Edge UOL*
e-Safer
ESET
E-TRUST
Expel, Inc
EY*
FastHelp
Fidelis Cybersecurity*
FireEye
Forcepoint*
ForgeRock (Ping Identity)
Formind*
Fortinet*
Fortra*
Fujitsu*
Future Segurança da Informação
GBS*

Empresas convidadas

Se sua empresa estiver listada nesta página ou você achar que sua empresa deveria estar listada, entre em contato com o ISG para garantir que temos a(s) pessoa(s) de contato correta(s) para participar ativamente desta pesquisa.

* Classificado na iteração anterior

GC Security
Genetec
Genpact
Getronics*
Gigamon
Globant*
glueckkanja*
GoCache*
Google*
GTT*
HackerOne
HackerSec
Hakai Offensive Security
Happiest Minds*
HCLTech*
Headmind Partners*
Hillstone Networks
HiSolutions*
Holiseum*
HPE Aruba Networking
HSC Brasil
HubOne (SysDream)*
Huge Networks*
IBLISS Digital Security*
IBM*
iC Consult*
ID Quantique
Imperva
inCloud Tecnologia
indevis*
Inetum*
InfoGuard*
Infosys*
Innova Solutions*
Insight*
Inspira*
Integrity360*
Interactive*
Interop
Intrinsec*
IonQ Quantum, Inc.
IPTRUST*
ISH Tecnologia*
iSPIN*
iT.eam*
It4us
Italtel*
ITC Secure*
I-tracing
ITS Group*
itWatch*
Kaspersky*
KnowBe4
KPMG*
Kroll*
KRYPTUS*

Empresas convidadas

Se sua empresa estiver listada nesta página ou você achar que sua empresa deveria estar listada, entre em contato com o ISG para garantir que temos a(s) pessoa(s) de contato correta(s) para participar ativamente desta pesquisa.

* Classificado na iteração anterior

Kudelski Security*
Kyndryl*
L8 Group
Leidos*
LevelBlue (Trustwave)*
Littlefish
Logical IT
Logicalis*
LRQA Nettitude*
LTIMindtree*
Lumen Technologies*
Macquarie Telecom Group*
ManageEngine*
Materna*
Matrix42*
McAfee
Mckinsey
Metsys*
Micro Focus
Microland*
Microsoft*
Mimecast*
MindPoint Group LLC
Minsait (Indra)
Modulo Security Solutions*
Mphasis*
MTF*
NAVA*
NCC Group*
NEC
NetBr
Netconn
Netfive
NetSecurity
Netskope*
NetSurion
Network Secure
Network Security Professionals, Inc.
Neverhack*
Nextios
Niji*
Nomios*
Nova8
Novacoast
Novared
Noventiq
Npo Sistemas
NRI*
NTSEC
NTT DATA*
Nv7
NXO*
Okta
One Identity
Ontinue (Open Systems)*
OpenText*
Oplium
Optiv*
Optus*
Opus Tech

Empresas convidadas

Se sua empresa estiver listada nesta página ou você achar que sua empresa deveria estar listada, entre em contato com o ISG para garantir que temos a(s) pessoa(s) de contato correta(s) para participar ativamente desta pesquisa.

* Classificado na iteração anterior

Oracle
Orange Cyberdefense*
ORBIT*
Ornisec*
OST Tecnologia
Palo Alto Networks*
pco*
Peers
Performanta*
Persistent Systems*
Post-Quantum
PQShield
Presidio*
PRIDE Security*
Proficio*
Proofpoint*
Protega Managed Cybersecurity
Protiviti/ICTS
PsiQuantum Corp.
PurpleSec*
PwC*
qbeyond
Qrypt
Quantinuum LLC
Quantum Xchange
QuEra Computing, Inc.
QuintessenceLabs
Quorum Cyber*
QuSecure
Rackspace Technology*
Radware
Rapid7
RCZ
Redbelt
ReliaQuest
Reply
Riedel Networks
Rpost
RSA Security
Safe Inc
Safeweb
SailPoint
Samsung
Scaltel
SCC*
Scunna*
SEC4U
Secureway
Secureworks*
Securiti
Security First
SecurityHQ*
SecurityScorecard
SEK (Security Ecossystem Knowledge)*
Sempre IT
Senhasegura
Sequretek*
Service IT*
Servix
Seti

Empresas convidadas

Se sua empresa estiver listada nesta página ou você achar que sua empresa deveria estar listada, entre em contato com o ISG para garantir que temos a(s) pessoa(s) de contato correta(s) para participar ativamente desta pesquisa.

* Classificado na iteração anterior

SFR*
Sigma Telecom
Skaylink
Skyhigh Security*
SLK Software*
Smarttech247*
SNS Security*
Softcat PLC*
Solo Iron*
Solo Networking
Solor
Sonda*
Sophos*
Sopra Steria*
Splunk
Squad*
Stefanini*
Strati
suresecure*
SVA*
Swisscom*
Symantec
Synetis*
Syntax*
Talion*
Tanium
Tata Communications*
TCS*
TDec Network Group*
Tech Mahindra*
Telefonica*
Telstra*
Teltec Solutions*
Tempest Security Intelligence
Tenable
Tenchi Security
terreActive*
Thales*
Think IT*
Tidalcyber
TIVIT*
Trellix*
Trend Micro*
Trigent
T-Systems*
UMB*
Under Protection*
Unisys*
United Security Providers*
Varonis*
Vectra*
Venturus
Verizon Business*
Vigilant
VIVO
VMware Carbon Black
Vodafone
Vortex Security*
Vortex TI
Vultus*

Empresas convidadas

Se sua empresa estiver listada nesta página ou você achar que sua empresa deveria estar listada, entre em contato com o ISG para garantir que temos a(s) pessoa(s) de contato correta(s) para participar ativamente desta pesquisa.

* Classificado na iteração anterior

WatchGuard

Wavestone*

Wipro*

Wizard Group

WWT*

Xantaro*

XYPRO Technology Corp.

You IT

Zensar Technologies*

Zscaler*

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 (Nasdaq: III) é uma empresa global de pesquisa e consultoria tecnológica centrada em IA. Um parceiro confiável para mais de 900 clientes, incluindo 75 das 100 maiores empresas do mundo, o ISG é líder de longa data em sourcing de tecnologia e serviços empresariais que agora está na vanguarda da alavancagem da IA para ajudar organizações a alcançar excelência operacional e crescimento mais rápido.

A empresa, fundada em 2006, é conhecida por seus dados de mercado proprietários, conhecimento profundo dos ecossistemas de fornecedores e pela especialização de seus 1.600 profissionais em todo o mundo trabalhando juntos para ajudar os clientes a maximizarem o valor de seus investimentos em tecnologia.

Para mais informações visite isg-one.com.

ISG Provider Lens®

JANEIRO DE, 2026

CATÁLOGO: CYBERSECURITY — SERVICES AND SOLUTIONS