ISG Provider Lens™

Cybersecurity – Services and Solutions

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

CATÁLOGO | JANEIRO DE 2025 | AUSTRÁLIA, BRASIL, FRANÇA, ALEMANHA, SUÍÇA, REINO UNIDO, EUA, SETOR PÚBLICO DOS EUA E GLOBAL

Índice

Segurança cibernética na era da IA e novas tecnologias disruptivas

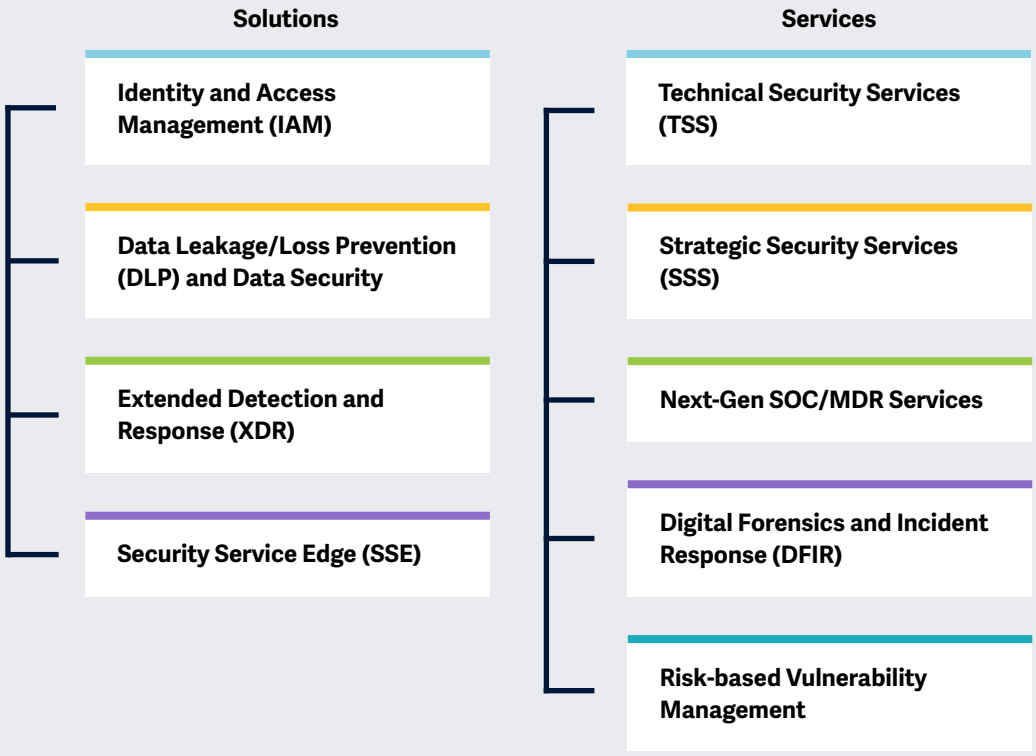
Na era de avanços tecnológicos rápidos e integração de IA em operações diárias, o cenário de segurança cibernética é cada vez mais complexo e multifacetado. Exigências regulatórias como a Diretiva 2 de Segurança de Rede e Informações (NIS) na União Europeia elevam a demanda por medidas fortes de segurança cibernética, levando organizações a reavaliarem seus frameworks de segurança entre novas ameaças. Ao mesmo tempo, a comoditização de ferramentas hackers reduziram significativamente as barreiras de entrada para atores maliciosos, levando a uma onda de atividades criminais cibernéticas e uma proporcional escalada de riscos.

A proliferação de tecnologia ampliou a superfície de ataque, trazendo desafios críticos para organizações conforme navegam entre tecnologia operacional (TO) e TI. A escassez de pessoal qualificado em segurança cibernética ampliou esta complexidade, estimulando demanda acelerada por serviço de serviço gerenciados de segurança conforme empresas buscam especialização externa para fortificar suas defesas.

Desenvolvimento contínuo de IA apresenta riscos e oportunidades no espaço de segurança cibernética. Fornecedores de segurança cibernética ajudam clientes a navegar no cenário de riscos cibernéticos, no qual a vigilância é crucial para identificar e mitigar novas ameaças e entender o impacto de transformação das novas tecnologias como computação quântica. Em resposta a estes desafios, negócios investem cada vez mais em soluções como IAM, DLP, XDR e SSE, combinando ferramentas avançadas e especialização humana com inteligência contextual e comportamental para aumentar sua postura de segurança.

Key focus areas for Cybersecurity – Services and Solutions 2025.

Ilustração simplificada Fonte: ISG 2025



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

- Transparência sobre os pontos fortes e as oportunidades de melhorias relevantes dos fornecedores de serviço.
- Um posicionamento diferenciado de fornecedores por segmento, 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.
- Os tópicos sobre IAM, SSE e XDR serão analisados quanto ao mercado global.
- Para considerar características específicas do país neste estudo global, a análise de XRD seria estendida ao Brasil, a de DLP seria analisada exclusivamente para Alemanha, um foco em DFIR seria realizado para França e a Gestão de Vulnerabilidade com Base em Riscos será avaliada para França e Brasil.

Pesquisa de Quadrantes

Our study serves as an important decision-making basis for positioning, key relationships and go-to-market considerations. ISG advisors and enterprise clients also use information from these reports to evaluate their current vendor relationships and potential engagements.

Definição

Fornecedores IAM avaliados neste quadrante são identificados pelo software, incluindo SaaS e serviços para gestão de identidades de usuário de empresa. Exclui fornecedores puros que não oferecem produto IAM, on premises ou em nuvem, desenvolvido com software proprietário. Dependendo das necessidades organizacionais, as soluções podem ser implementadas tanto localmente, em nuvens geridas pelo consumidor, como modelos como serviço ou um mix destas opções.

Soluções IAM focam na gestão de identidades de usuário e direitos de acesso, com acesso especializado por gestão de acesso privilegiado regido por políticas definidas. Pacotes IAM integram mecanismos, frameworks e automação seguros para usuário em tempo real e perfil de ataque para necessidades de aplicativo em evolução. Espera-se que fornecedores incluam funcionalidades de redes sociais e acesso móvel, atendendo a requisitos de segurança além da gestão tradicional de direitos de web. Este quadrante engloba gestão de identidade por máquina.

Critérios de Qualificação

1. Oferecer soluções que possam ser **implementadas localmente**, em **nuvem**, como **IDaaS** ou por modelo de terceiro gerenciado
2. Entregar soluções **compatíveis com autenticação**, como uma combinação de **logon único (SSO), autenticação multifatores** (MFA) e modelos baseados em risco e em contexto
3. Oferecer soluções **compatíveis com acesso baseado em funções** e PAM
4. Fornecer **gerenciamento de acesso** para atender múltiplas necessidades empresariais, como **nuvem, endpoint, dispositivos móveis, APIs** e **aplicativos web**
5. Propor soluções que podem **apoiar legados e novos padrões IAM** incluindo, entre outros, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust e SCIMOffer e portfólio com uma ou mais das seguintes soluções – **gestão de diretório, painel ou autoatendimento** e gestão de ciclo de vida (migração, sincronização e replicação) – para apoiar acesso seguro

Data Leakage/Loss Prevention (DLP) and Data Security

Definição

Fornecedores de soluções avaliados neste quadrante são identificados pelo software proprietário, incluindo SaaS e serviços associados. Exclui fornecedores puros que não oferecem produto DLP implementados localmente ou em nuvem, desenvolvido com software proprietário. Soluções DLP podem identificar e monitorar dados sensíveis e fornecer acesso a usuários autorizados. Incluem uma combinação de produtos que oferecem visibilidade e controle sobre dados confidenciais em aplicativos em nuvem, endpoints, redes e vários dispositivos.

Soluções DLP ajudam empresas a enfrentar desafios em controlar movimentos de dados, considerando-se que mais de um terço de violações de dados tem origem interna. A proliferação de dispositivos móveis e outros para armazenamento de dados aumentam tais questões, já que podem trocar dados sem gateways centrais. Soluções de segurança de dados protegem contra acesso não autorizado e roubo ao priorizar, classificar e monitorar dados em repouso e em trânsito, permitindo a melhoria da proteção sobre os dados.

Critérios de Qualificação

1. Oferecer soluções DLP baseadas em **softwares exclusivos**, e não em softwares de terceiros
2. Demonstrar capacidade de suporte a DLP **em qualquer arquitetura, como nuvem, rede, armazenamento ou endpoint**
3. Exibir capacidade de **proteger dados sensíveis, estruturados ou não**, em texto ou formatos binários
4. Fornecer solução com **suporte básico de gerenciamento**, incluindo, sem limitação, **geração de relatórios, controles de políticas**, instalação e manutenção e funcionalidades avançadas de detecção de ameaças
5. Oferecer solução capaz de **identificar dados confidenciais, aplicar políticas**, monitorar tráfego e melhorar a conformidade dos dados

Definição

Fornecedores de XDR avaliados no quadrante são identificados pelas plataformas que integram, correlacionam e contextualizam dados e alertas de múltiplos componentes de prevenção, detecção e resposta a ameaças. XDR é uma tecnologia com base em nuvem que integra várias soluções de segurança e usa análise para melhorar a precisão de detecção. Consolida produtos de segurança para melhorar a visibilidade e o contexto de ameaça em espaços de trabalho, redes e cargas de trabalho da empresa.

XDR usa telemetria e dados contextuais para detecção e resposta, integrando múltiplos produtos em uma interface unificada. Têm alta automação e priorizam alertas com base na gravidade para determinar a necessidade de respostas personalizadas. Quadrante exclui fornecedores puros que não oferecem solução XDR **baseada em** softwares exclusivos. XDR reduz dispersão de produtos, fadiga de alertas e lida com desafios de integração. Ajudam equipes de segurança a gerenciar ou obter valor de soluções de SIEM ou de SOAR.

Critérios de Qualificação

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 e IDPS), detecção e resposta de rede, gestão de identidade, segurança de e-mail, detecção de ameaças de dispositivos móveis, proteção de carga de trabalho na nuvem e identificação de fraude
4. Fornecer solução com **cobertura e visibilidade abrangentes de todos os endpoints** em uma rede
5. Oferecer soluções capazes 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. Entregar soluções com **características de resposta automatizadas**

Definição

Fornecedores de soluções de SSE avaliados neste quadrante oferecem soluções centradas na nuvem que combinam software ou hardware exclusivo e serviços associados, permitindo acesso seguro à aplicativos em nuvem, SaaS, serviços da Web e aplicativos privados. Fornecedores oferecem soluções de SSE como um serviço de segurança integrado por meio de pontos de presença posicionados globalmente, com suporte para armazenamento local de dados que combina soluções individuais, como acesso à rede usando confiança zero (ZTNA), agente de segurança de acesso à nuvem (CASB), gateways seguros da internet (SWG) e firewall como serviço (FWaaS). O SSE também pode incluir outras soluções de segurança, tais como DLP, isolamento de navegador e NGFW – firewalls de última geração para garantir acesso seguro a aplicativos na nuvem e local.

Fornecedores demonstram especialização no cumprimento de leis locais, regionais e nacionais, como soberania de dados, para clientes globais. Este quadrante exclui os componentes de rede de SASE, como SD-WAN, que serão abordados no estudo ISG Provider Lens™ Network – Software Defined Services and Solutions 2025.

Critérios de Qualificação

1. Fornecer SSE como **solução integrada** com componentes **ZTNA, CASB, SWG e FWaaS**
2. Oferecer soluções **predominantemente baseadas em softwares exclusivos**, podendo **contar parcialmente com soluções de parceiros**, evitando a **total dependência em softwares de terceiros**
3. Manter **pontos de presença localizados globalmente** para entregar soluções
4. Entregar **funcionalidades SSE para nuvem e ambientes locais** (incluindo ambientes híbridos)
5. Realizar **avaliações e análises contextuais e comportamentais (análise de comportamento e entidade do usuário [UEBA]**) para detectar e prevenir intenções maliciosas ou suspeitas
6. Oferecer **suporte básico de gerenciamento**, incluindo, mas não se limitando a **geração de relatórios** e manutenção e funcionalidades avançadas de detecção de ameaças
7. Garantir **disponibilidade das soluções globalmente**

Technical Security Services (TSS)

Definição

Fornecedores de TSS avaliados neste quadrante oferecem integração, manutenção e suporte para produtos ou soluções de segurança de TI e OT. TSS engloba ampla gama de produtos de segurança, incluindo segurança de nuvem e data center, IAM, DLP, segurança de rede, segurança de endpoint, segurança de TO, SASE e outros.

Fornecedores oferecem manuais e mapas para melhorar a segurança com as melhores opções de ferramentas, aprimorando a postura e reduzindo ameaças. Portfólios apoiam transformações de arquitetura de segurança completas ou individuais, com identificação, avaliação, design e implementação de produto ou solução. Investem em parcerias com soluções de segurança e fabricantes de tecnologia para credenciamentos e para expandir portfólio.

Este quadrante inclui serviços clássicos de segurança gerenciados fornecidos sem centro de operações de segurança. Analisa fornecedores que não estão focados apenas em seus produtos exclusivos, mas que podem implementar e integrar soluções de outros fabricantes e fornecedores.

Critérios de Qualificação

1. Demonstrar experiência na criação e **implementação de soluções de segurança cibernética** para empresas no respectivo país
2. Obter **autorização de fabricantes de tecnologia de segurança** (hardware e software) para distribuir e oferecer suporte a soluções de segurança
3. **Empregar especialistas certificados** (as certificações podem ser credenciais patrocinadas por fabricantes, lideradas por associações e organizações ou por órgãos governamentais) capazes de oferecer suporte a tecnologias de segurança
4. **Não focar exclusivamente** em **produtos** ou soluções **proprietários**
5. Apresentar **estudos de caso** que demonstram design, implantação e gestão bem-sucedida de soluções de segurança cibernética para empresas no país alvo

Definição

Fornecedores de SSS do quadrante oferecem consultoria de segurança de TI e OT. Serviços incluem auditorias de segurança, avaliações e conscientização e treinamento. Eles ajudam a avaliar a maturidade da segurança e definir estratégias de segurança cibernética para requisitos da empresa.

Contratam consultores de segurança experientes para planejar e gerir programas de segurança de ponta a ponta. Com a demanda de SMBs – pequenos e médios negócios e a falta de talentos, estes oferecem especialista sob demanda por serviços como CISO virtuais. Criam mapas de continuidade de negócios, priorizam aplicativos críticos para recuperação, e conduzem exercícios práticos e simulações para melhorar conhecimento cibernético e resposta dos membros do board e as lideranças das áreas operacionais. Orientam a seleção de tecnologias e fornecedores de segurança, revisando estruturas organizacionais para segurança cibernética, avaliando processos e práticas de segurança, e melhorando estes de acordo com os riscos. São examinados não apenas os fornecedores focados em produtos ou soluções exclusivas.

Critérios de Qualificação

1. Demonstrar habilidades em áreas de SSS, como **avaliações, seleção de fabricantes, consultoria de soluções e consultoria de risco**
2. Exibir competência na aplicação de boas práticas e frameworks de segurança de mercado tais como ISO 27000, NIST e CIS
3. **Oferecer pelo menos um** dos serviços estratégicos de segurança acima nos respectivos países para este estudo
4. Fornecer **serviços de consultoria de segurança usando frameworks tais como NIST e ISO**
5. **Não focar exclusivamente** em **produtos ou soluções proprietários**

Definição

Fornecedores avaliados neste quadrante oferecem serviços relacionados ao monitoramento contínuo de infraestruturas de TI e TO por um SOC. Este quadrante analisa fornecedores de serviços que não estão apenas focados em produtos exclusivos, mas podem gerenciar e operar as melhores ferramentas de segurança. Esses fornecedores de serviços abordam todo o ciclo de vida do incidente de segurança, desde a identificação até a resposta e correção.

Fornecedores SOC de próxima geração estão em demanda para fortalecer a postura de segurança da empresa e melhorar a eficácia dos programas de segurança. Incorporam serviços tradicionais gerenciados de segurança com inovação para entregar serviços de defesa cibernética integrada e MDR. Eles também investem na detecção e caça de ameaças, inteligência de ameaças, modelagem e forense, gestão de incidentes e tecnologias avançadas, como automação, big data, IA e ML, para oferecer uma abordagem holística a mitigação proativa de ameaças e segurança avançada.

Critérios de Qualificação

1. Oferecer serviços habituais que incluem **monitoramento de segurança, análise de comportamento, detecção de acesso não autorizado, consultoria sobre medidas de prevenção, testes de penetração** e todos os demais serviços operacionais para proporcionar proteção contínua e em tempo real sem comprometer o desempenho dos negócios
2. Fornecer serviços de segurança, como prevenção e **detecção, serviços de gerenciamento de informações e eventos de segurança (SIEM)**, consultores de segurança e suporte a auditorias, seja remotamente ou no local do cliente
3. Capacitações específicas de MDR, incluindo **inteligência de ameaça avançada e caça à ameaça liderada por humanos e baseada em comportamento**, entregando capacitações de segurança **ofensivas e defensivas** com uma **visão unificada** para geração de relatório e métricas
4. Possuir **credenciamentos** de fabricantes de ferramentas de segurança
5. **Gerenciar os próprios SOCs**
6. Manter **equipe** com certificações, como Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) e Global Information Assurance Certification (GIAC)
7. Oferecer variedade de modelos de precificação em níveis

Definição

Fornecedores avaliados no quadrante DFIR oferecem serviços relacionados a atividades de resposta a ameaças, preservando evidências contra invasores. Quadrante analisa fornecedores que contam com técnicas e metodologias comprovadas de DFIR e podem trabalhar com as melhores ferramentas para responder a incidentes de segurança cibernética.

DFIR envolve a identificação, investigação, contenção e remediação de incidentes de segurança cibernética. Escalonamento da frequência e gravidade dos incidentes de segurança cibernética levou à adoção de serviços de DFIR. DFIR é essencial para identificar a perda de dados após uma violação de segurança e estabelecer respostas eficazes à ameaças por manuais. Fornecedores demonstram especialização em análise forense digital, como triagem, linha do tempo, e análise de registro, exame de malware e análise de artefato. Também têm experiência em suporte de litígio em reivindicações e auditorias e proficiência em ferramentas tais como SIEM, SOAR, EDR e XDR.

Critérios de Qualificação

1. Ter uma **equipe dedicada de resposta a incidentes** (CERT ou CSIRT), com especialistas certificados como GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE) e CISSP, demonstrando sua experiência e compromisso em manter os padrões e boas práticas do setor
2. Possuir experiência e conhecimento no **manuseio de diversas** soluções SIEM, SOAR, EDR e XDR
3. Oferecer serviços DFIR que **identificam a causa raiz** de uma **violação** e avaliam seu impacto a curto e longo prazo
4. **Possuir recursos** de análise de malware, descriptografia de ransomware e recuperação de dados
5. Demonstrar **parceria** com fabricantes de produtos e fornecedores de serviços de segurança gerenciados para melhorar a inteligência sobre ameaças, monitoramento da dark web e recursos SOC, e mitigar ameaças avançadas persistentes e sofisticadas

Definição

Fornecedores de gestão de vulnerabilidade com base em riscos vistos no quadrante são identificados pelo avanço técnico para atualizações contínuas em vulnerabilidades conhecidas e métodos sofisticados ultrapassando defesas consolidadas por práticas como teste de penetração. Ferramentas de GenAI empoderaram criminosos cibernéticos a identificarem e explorarem vulnerabilidades em ativos de tecnologia, especialmente os expostos na internet. Tal tendência e o aumento em incidentes de ransonware, destaca necessidade de gestão de vulnerabilidade contínua ao invés de avaliações esporádicas.

Com a frequência de atualizações dos serviços expostos à internet, implementar detecção de vulnerabilidade contínua é essencial para uma estratégia eficaz de segurança cibernética com base em riscos. Fornecedores devem oferecer soluções que transcendam práticas tradicionais, reconhecendo que um framework com base em riscos é vital para gerir vulnerabilidades e minimizar o impacto de ameaças em evolução.

Critérios de Qualificação

1. Englobar equipes internas especializadas capazes de **avaliar rigorosamente vulnerabilidades e indicar soluções** para remover falhas e gradualmente reduzir sua gravidade com base em evidências concretas de vetores de ataques
2. Oferecer serviços que incluem **abordagens black box, grey box e white box** capazes de avaliar aplicativos web, dispositivos móveis, redes internas, nuvem, APIs, IoT e outros ativos expostos
3. Usar métodos como **DAST, SAST e teste de penetração** de objetivos específicos utilizando ferramentas automatizadas e/ou manuais para entrega de serviço
4. Usar e evidenciar **normas e padrões reconhecidos da indústria**, como SOC 2, ISO27001, NIST 800-53, PCI-DSS e HIPPA ao apontar falhas de segurança
5. Oferecer **retestes, suporte especializado e mecanismos** de monitoramento de ações corretivas, atualização da matriz de riscos e gravidade (exposição a vetores remanescentes) como exigido
6. Ter uma **equipe de especialistas técnicos** (Hackeamento Ético) com certificações como Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), Certified Information Systems Security Professional (CISSP), CompTIA Penetration Testing (CompTIA PenTest+) e GIAC Penetration Tester (GPEN)

Quadrantes Por Região

Como parte deste estudo de quadrantes do ISG Provider Lens™, estamos apresentando os nove quadrantes a seguir sobre Cybersecurity – Services and Solutions 2025:

Quadrante	EUA	Reino Unido	Alemanha	Suíça	França	Brasil	Austrália	Setor Público dos EUA	Global
Identity and Access Management (IAM)									✓
Data Leakage/Loss Prevention (DLP) and Data Security			✓						
Extended Detection and Response (XDR)						✓			✓
Security Service Edge (SSE)									✓
Technical Security Services (TSS)	✓	✓	✓	✓	✓	✓	✓	✓	
Strategic Security Services (SSS)	✓	✓	✓	✓	✓	✓	✓	✓	
Next-Gen SOC/MDR Services	✓	✓	✓	✓	✓	✓	✓	✓	
Digital Forensics and Incident Response (DFIR)					✓				
Risk-based Vulnerability Management					✓	✓			

Principais características de framework proprietário:

- Encapsula o que as empresas estão fazendo no mercado da Segurança Cibernética e ajuda a conectá-las às soluções digitais
- Representa toda a cadeia de valor da oferta e demanda no mercado
- Os blocos internos representam temas dos objetivos da empresa
- Os blocos externos representam iniciativas
- Por trás de cada bloco externo há um conjunto específico de capacitações, com fornecedores e soluções exclusivos e líderes de mercado

The research phase falls in the period between January and February 2025, during which survey, evaluation, analysis and validation will take place. The results will be presented to the media in July 2025.

Milestones	Início	Fim
Lançamento da Pesquisa	7 de janeiro de 2025	
Fase da Pesquisa	7 de janeiro de 2025	7 de fevereiro de 2025
Prévia dos Resultados	Maio de 2025	Junho de 2025
Comunicado à Imprensa e Publicação	Julho de 2025	

A coleta de depoimentos de clientes por meio do Programa Star of Excellence requer referências antecipadas de clientes (sem necessidade de referência oficial) porque as pontuações CX têm uma influência direta na posição do fornecedor no quadrante IPL e nos prêmios.

Consulte o link para visualizar/baixar o calendário de pesquisa de 2025 do ISG Provider Lens™.

Acesso ao Portal On-line

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

IA Software Research do ISG, 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.

Ao longo do lançamento do IPL Cybersecurity – Services and Solutions, queremos aproveitar a oportunidade para chamar sua atenção para pesquisas e insights relacionados que 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 2025 Cybersecurity – Services and Solutions 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

Autor Principal:
Frank Heuer, Gowtham Kumar, Bhuvaneshwari Mohan, Benoit Scheuber, Dr. Maxime Martelli, Andrew Milroy and João Mauro

Analista de Pesquisa:
Monica K, Sandya Kattimani and Rafael Rigotti

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 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 ndicado de outra forma.

Contatos Para Este Estudo

Patrocinador do estudo

Heiko Henkes

Director and Principal Analyst

Frank Heuer

Analista Líder - Alemanha, Suíça

Gowtham Kumar

Analista Líder - EUA, Setor Público dos EUA, Global

Bhuvaneshwari Mohan

Analista Líder - Reino Unido, Setor Público dos EUA, Global

Benoit Scheuber

Analista Líder - França

Dr. Maxime Martelli

Analista Líder - Global

Andrew Milroy

Analista Líder - Austrália

João Mauro

Analista Líder - Brasil

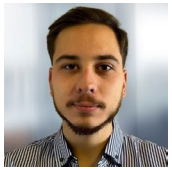
Monica K

Analista de Pesquisa

Contatos Para Este Estudo

Sandya Kattimani

Analista de Pesquisa



Rafael Rigotti

Analista de Pesquisa

Rajesh Chillappagari

Analistas de Dados

Laxmi Sahebrao

Analistas 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 dos fornecedores de serviços e contexto empresarial.

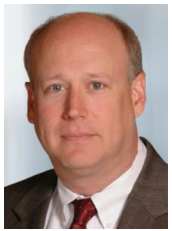
Em cada região, o ISG tem líderes de pensamento especialistas e consultores respeitados que conhecem os portfólios e ofertas dos fornecedores, bem como os requisitos da empresa e as tendências do mercado. Em média, três consultores participam como parte do processo de revisão de qualidade e consistência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

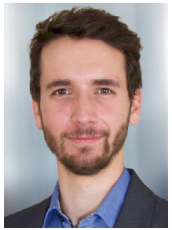


Doug Saylors

Parceiro, Colíder de Segurança Cibernética ISG

David Gordon

Consultor Principal de Segurança Cibernética



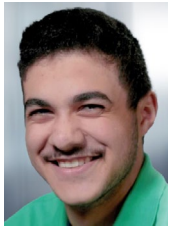
Anas Barmo

Consultor Sênior de Segurança Cibernética

Brendan Prater

Gerente de Consultoria de Segurança Cibernética

Consultores do ISG para este estudo



Marco
Ezzy

Consultor de Segurança Cibernética

Tim
Merscheid

Gerente de Consultoria de Segurança Cibernética

Christophe
de Boisset

Gerente de Consultoria de Segurança Cibernética

Empresas convidadas

Se sua empresa estiver relacionada nesta página ou você achar que sua empresa deveria estar relacionada, entre em contato com o ISG para garantir que temos os contatos corretos para participar ativamente desta pesquisa.

* Classificado na iteração anterior

Absolute Software*
AC3*
Accenture*
ACESI Group
Acronis*
Actar (Peers Group)
ActioNet*
Adarma*
ADIT Group
Advens*
Agility Networks*
Airbus Protect*
AISI
Akamai*
Algosecure
Alice&Bob.Company*
All for One Group*
AlmavivA*
Almond*
Alten*
Amazon Web Services
AntemetA
Apixit
Appdome
Apura Cyber Intelligence S/A
Arcon
Asper*
AT&T Cybersecurity*
Atos*
Avatier*
Aveniq*
Avertium*
Axians*
Axur
Azion
BAYOOSOFT*
BDO
Bechtle*
Berghem*
Beta Systems*
BeyondTrust*
BIP
Bitdefender*
BlackBerry*
Blaze Information Security*
BluePex*
BlueVoyant*
Brainloop*
Bravo GRC
Bridewell
Broadcom
BT*
CANCOM*
Capgemini*
Cato Networks*
CDW*
Century Data
CGI*
ChapsVision CyberGov
Check Point Software*

Empresas convidadas

Se sua empresa estiver relacionada nesta página ou você achar que sua empresa deveria estar relacionada, entre em contato com o ISG para garantir que temos os contatos corretos para participar ativamente desta pesquisa.

* Classificado na iteração anterior

Cipher*
Cirion*
Cisco*
Citrix
Claranet*
Clavis*
ClearSale
Cloud Target
Cloudflare*
Cognizant*
Combate a Fraude (Caf)
Compugraf
Computacenter*
Consort Group*
Consulteer InCyber
Controlware*
CoSoSys (Netwrix)*
Critical Start*
Cross Identity*
CrowdStrike*
CTM*
CyberArk*
CyberCX*
Cybereason*
CyberProof*
Cyberprotect
CyberSecOp*
Cybersolutions
Cyderes*
Darktrace
Data#3*
Datacom*
DATAGROUP*
dataRain
Delfia
Delinea
Deloitte*
Deutsche Telekom
Devensys
Devoteam*
DIGITALL*
DriveLock*
DXC Technology*
EcoTrust
Edge UOL*
Embratel
EmpowerID*
Ensono
Entrust*
Ergon Informatik*
Ericom Software*
e-Safer
ESET*
E-TRUST*
Eviden*
EY*
FastHelp*
Fidelis Cybersecurity*
FireEye
Fischer Identity*

Empresas convidadas

Se sua empresa estiver relacionada nesta página ou você achar que sua empresa deveria estar relacionada, entre em contato com o ISG para garantir que temos os contatos corretos para participar ativamente desta pesquisa.

* Classificado na iteração anterior

Forcepoint*
ForgeRock (Ping Identity)
Formind*
Fortinet*
Fortra*
Framatome Cybersecurity
Fujitsu*
FusionAuth*
Future Segurança da Informação
GBS*
GC Security*
Genetec
Getronics*
Gigamon
Globant*
glueckkanja*
GoCache*
Google*
GTT*
HackerOne
HackerSec*
Hakai Offensive Security*
Happiest Minds*
HCLTech*
Headmind Partners*
HiSolutions*
HPE Aruba Networking
HSC Brasil
HubOne (SysDream)*
Huge Networks*
IBLISS Digital Security*
IBM*
iboss*
iC Consult*
Ilex IAM Platform*
Imperva
Imprivata*
IMS Networks
IN Groupe*
indevis*
InfoGuard*
Infosys*
Integrity360*
Interop
Intrinsec*
ISH Tecnologia*
ISPIN*
IT.eam*
It4us
Italtel*
ITC Secure*
I-Tracing
Itrust (Free Pro)*
ITS Group*
itWatch*
Kaspersky*
KnowBe4
KPMG*
Kroll*
Kryptus*

Empresas convidadas

Se sua empresa estiver relacionada nesta página ou você achar que sua empresa deveria estar relacionada, entre em contato com o ISG para garantir que temos os contatos corretos para participar ativamente desta pesquisa.

* Classificado na iteração anterior

Kudelski Security*
Kyndryl*
Lastpass*
Leidos*
Lexfo*
Logical IT
Logicalis*
Lookout*
LRQA Nettitude*
LTIMindtree*
Lumen Technologies*
Macquarie Telecom Group*
ManageEngine*
Mandiant
Materna Radar*
Matrix42*
McAfee
Metsys*
Micro Focus
Microland*
Microsoft*
Modulo Security Solutions
Mphasis*
MTF*
NAVA*
NBS System
NCC Group*
NEC*
Neosoft
NetSecurity
Netskope*
Network Secure
Neverhack*
Nevis*
Nextios
Nok Nok Labs*
Nomios*
Novared
Noventiq
Npo Sistemas
NRI ANZ*
NTSEC
NTT DATA*
NTT Ltd.
NXO*
NYBBLE
OEDIV
Okta*
Omada*
One Identity (OneLogin)*
Open Systems*
OpenText*
Optiv*
Oracle*
Orange Cyberdefense*
OST Tecnologia
P1 SECURITY
Palo Alto Networks*
pco*
Peers

Empresas convidadas

Se sua empresa estiver relacionada nesta página ou você achar que sua empresa deveria estar relacionada, entre em contato com o ISG para garantir que temos os contatos corretos para participar ativamente desta pesquisa.

* Classificado na iteração anterior

Performanta*
Perimeter 81*
Persistent Systems*
Ping Identity*
Presidio*
Pride Security*
Proficio*
Proofpoint*
Protega Managed Cybersecurity
Protiviti/ICTS
PurpleSec*
PwC*
Quorum Cyber*
Rackspace Technology*
Radware
Rapid7*
RCZ
Red river
Redbelt
Redscan*
Reply
RSA Security*
Safeway
Safeweb
SailPoint*
SAP*
Saviynt*
SCC*
Scunna*
SCUTUM
SEC4U
SecureAuth*
Secureway
Secureworks*
Securiti
SecurityHQ*
SecurityScorecard
SEK (Security Ecossystem Knowledge)*
Sekuro*
senhasegura*
SenseOn*
SentinelOne*
Seqrite
Sequretek
Service IT*
Servix
Seti
SFR*
Shearwater Group*
Sigma
Sigma Telecom
Skyhigh Security*
SLK Software*
SNS Security
Softcat*
SolarWinds*
Solor
SONDA*
Sophos*
Sopra Steria*

Empresas convidadas

Se sua empresa estiver relacionada nesta página ou você achar que sua empresa deveria estar relacionada, entre em contato com o ISG para garantir que temos os contatos corretos para participar ativamente desta pesquisa.

* Classificado na iteração anterior

Spie ICS*
Splunk
Squad*
Stefanini*
suresecure*
Swisscom*
Symantec
Synetis*
Syntax*
Sysinterga
Systancia*
Talion*
Tanium
Tata Communications*
TCS*
TDec Network Group*
Tech Mahindra*
TEHTRIS*
Telefonica Tech*
Telstra*
Teltec Solutions*
Tempest Security Intelligence
Tenable
Tenchi Security
terreActive*
Thales*
Think IT*
TIVIT*
Trellix*
Trend Micro*
Trustwave*
T-Systems*
UMB*
Under Protection
Unisys*
United Security Providers*
ValueLabs*
Varonis*
Vectra*
Venturus
Verizon Business*
Versa Networks*
Vigilant
VMware Carbon Black
Vortex Security*
Vortex TI
WALLIX*
WatchGuard
Wavestone*
Wipro*
Xmco
YSSY*
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 (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™

JANEIRO DE 2025

CATÁLOGO: CYBERSECURITY – SERVICES AND SOLUTIONS