ISG Provider Lens™

Cybersecurity – Solutions and Services 2023

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

BROCHURE | JANEIRO DE 2023 | GLOBAL

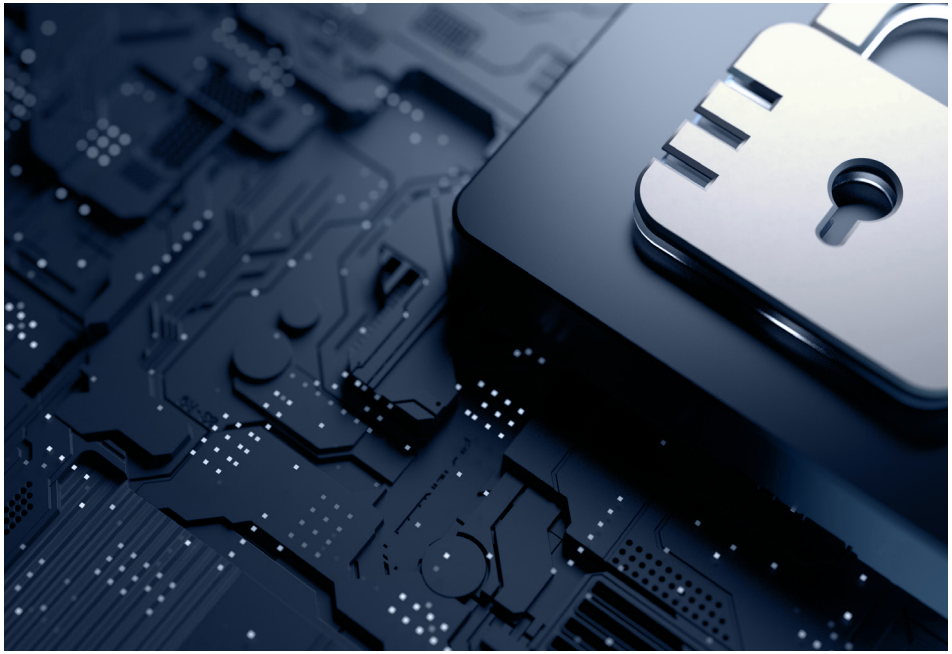
Table of Contents

Introdução

O ano de 2022 pode ser considerado tumultuado do ponto de vista da segurança cibernética; embora tenha havido uma diminuição nos incidentes de violação de dados, o ano viu um aumento significativo na sofisticação e gravidade dos ataques. Em 2022, as empresas aumentaram seus investimentos em segurança cibernética e priorizaram iniciativas relevantes para prevenir ataques e melhorar sua 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.

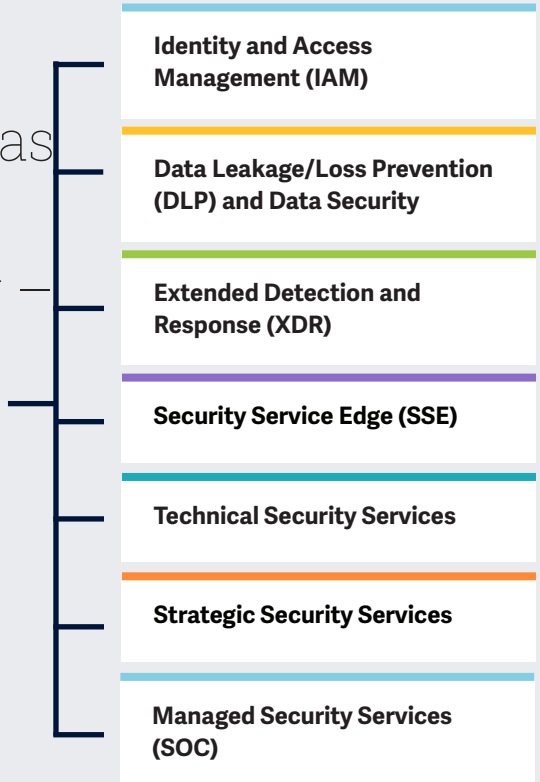
Do ponto de vista empresarial, até mesmo as pequenas empresas entenderam o impacto das ameaças cibernéticas e perceberam que são alvos ativos e altamente vulneráveis a ataques cibernéticos. Isso reforçou a necessidade de serviços de segurança (gerenciados) e serviços de resiliência cibernética que permitiriam que as empresas se recuperassem e retomassem as operações rapidamente após um incidente cibernético. Os provedores 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 e são aprimoradas com inteligência comportamental e contextual e automação para oferecer uma postura de segurança superior.

Principais áreas de foco para Cybersecurity – Solutions and Services 2023



Simplified Illustration Source: ISG 2023

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

- Transparência sobre os pontos fortes e de atenção dos provedores relevantes.
- Um posicionamento diferenciado de provedores por segmentos em suas vantagens competitivas e atratividade de portfólio.
- Foco em diferentes mercados, incluindo EUA, Reino Unido, países nórdicos, Alemanha, Suíça, França, Brasil, Austrália, Cingapura e Malásia e o setor público dos EUA. O tema SSE será analisado para o mercado global.

Nossos estudos servem como uma importante base de tomada de decisão para 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 atuais com fornecedores e possíveis compromissos.

Definição

Os fornecedores e provedores de soluções de IAM avaliados para este quadrante são caracterizados por sua capacidade de oferecer software proprietário e serviços associados para gerenciar identidades e dispositivos de usuários corporativos. Este quadrante também inclui ofertas de SaaS baseadas em software proprietário. **Ele não inclui provedores de serviços puros que não oferecem um produto de IAM (no local e/ou na nuvem) baseado em software proprietário.** Dependendo dos requisitos organizacionais, essas ofertas podem ser implantadas de várias maneiras, como no local ou na nuvem (gerenciada por um cliente) ou como um modelo como serviço ou uma combinação deles.

As soluções de IAM visam gerenciar (coletar, registrar e administrar) identidades de usuários e direitos de acesso relacionados e também incluem acesso especializado a ativos críticos por meio de gerenciamento de acesso privilegiado (PAM), onde o acesso é concedido com base em políticas definidas. Para lidar com os requisitos de aplicações novas e existentes, os conjuntos de soluções de IAM são cada vez mais integrados a mecanismos, estruturas e automação seguros (por exemplo, análise de risco) para fornecer funcionalidades de perfil de ataque e usuário em tempo real. Os provedores de soluções também devem fornecer funcionalidades adicionais relacionadas à mídia social e ao uso móvel para atender às necessidades específicas de segurança além do tradicional gerenciamento de direitos contextuais e da web. O gerenciamento de identidade de máquina também está incluído aqui.

Critérios de Elegibilidade

1. A solução deve ser capaz de ser **implantada** como um modelo **local, na nuvem, de identidade como serviço** (IDaaS) e gerenciado por terceiros.
2. A solução deve ser capaz de oferecer **suporte à autenticação** como uma combinação de **logon único (SSO), autenticação multifator (MFA),** modelos baseados em risco e baseados em contexto.
3. A solução deve ser capaz de **suportar acesso baseado em função** e PAM.
4. O fornecedor de IAM deve ser capaz de fornecer **gerenciamento de acesso** para uma ou mais necessidades corporativas, como **nuvem, endpoint, dispositivos móveis, interfaces de programação de aplicações (APIs) e aplicações da web.**
5. A **solução deve ser capaz de suportar um ou mais padrões de IAM legados e novos,** incluindo, entre outros, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust e SCIM.
6. Para oferecer suporte ao acesso seguro, o portfólio deve incluir um ou mais dos seguintes – **soluções de diretório, painel ou gerenciamento de autoatendimento** e soluções de gerenciamento do ciclo de vida (migração, sincronização e replicação).

Definição

Os fornecedores de DLP e provedores de soluções avaliados para este quadrante são caracterizados por sua capacidade de oferecer software proprietário e serviços associados. Este quadrante também inclui soluções de SaaS baseadas em software proprietário. **Ele não inclui provedores de serviços puros que não oferecem um produto de DLP (local ou baseado em nuvem) baseado em software proprietário.** As soluções de DLP podem identificar e monitorar dados confidenciais, fornecer acesso apenas para usuários autorizados e evitar perda/vazamento de dados. As soluções de fornecedores neste espaço incluem uma combinação de produtos capazes de fornecer visibilidade e controle sobre dados confidenciais que residem em aplicações na nuvem, endpoints, redes e vários dispositivos.

Essas soluções estão ganhando importância considerável, pois se tornou cada vez mais difícil para as empresas controlar as movimentações e transferências de dados (mais de um terço das violações de dados são de origem interna). O número de dispositivos, incluindo dispositivos móveis, usados para armazenar dados está aumentando nas empresas. Equipados com uma conexão com a Internet, esses dispositivos podem enviar e receber dados sem passá-los por um gateway central da Internet. As soluções de segurança de dados protegem os dados contra acesso não autorizado, divulgação ou roubo, priorizando, classificando e monitorando os dados (em repouso e em trânsito), permitindo que as organizações relatem e melhorem a segurança de seus dados em risco.

Critérios de Elegibilidade

1. A oferta de DLP deve ser baseada em **software proprietário** e não em software de terceiros.
2. A solução deve ser capaz de suportar DLP **em qualquer arquitetura, como nuvem, rede, armazenamento ou endpoint**.
3. A solução deve ser capaz de **lidar com a proteção de dados confidenciais em dados estruturados** ou não estruturados, texto ou dados binários.
4. A solução deve ser oferecida com **suporte básico de gerenciamento,** incluindo, entre outros, geração de **relatórios, controles de políticas,** instalação e manutenção e funcionalidades avançadas de detecção de ameaças.
5. A solução deve ser capaz de **identificar dados confidenciais, impor políticas**, monitorar tráfego e melhorar a conformidade de dados.

Definição

Os provedores 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, segurança da rede ou segurança da carga de trabalho. Normalmente, as soluções de XDR visam melhorar muito a visibilidade e melhorar 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 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 personalizados para o sistema afetado e priorizam alertas com base na gravidade em relação a estruturas de referência conhecidas. **Os provedores 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).

Critérios 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 **ameaças persistentes avançadas, ransomware** e malware.
6. A solução deve utilizar a **inteligência de ameaças** e analisar e oferecer **informações em tempo real sobre as ameaças** que emanam dos endpoints.
7. A solução deve incluir **recursos de resposta automatizada**.

Definição

Os provedores de soluções de SSE avaliados neste quadrante oferecem soluções centradas na nuvem que combinam software proprietário e/ou hardware e serviços associados, permitindo acesso seguro a serviços em nuvem, aplicações de SaaS, serviços da web e aplicações privadas. Os fornecedores oferecem soluções de SSE como um serviço de segurança integrado por meio de pontos de presença (PoP) posicionados globalmente com suporte para armazenamento de dados local que combina soluções individuais, como acesso à rede de confiança zero (ZTNA), corretor de segurança de acesso à nuvem (CASB), gateways da web seguros (SWG) e firewall como serviço (FWaaS). O SSE também pode incluir outras soluções de segurança, como prevenção contra perda/vazamento de dados (DLP), isolamento de navegador e firewall de última geração (NGFW) para oferecer acesso seguro a aplicações na nuvem e no local.

Os fornecedores demonstram experiência em atender às leis locais, regionais e domésticas (como a soberania de dados) para clientes globais.

Os componentes de rede de borda segura de acesso seguro (SASE), como SD-WAN ou microssegmentação, não estão incluídos neste quadrante, mas são abordados no estudo Network - Software Defined Solutions and Services.

As soluções de SSE concentram-se fortemente no foco do usuário, fornecendo segurança aos usuários finais na borda ou dispositivos por meio da nuvem – em vez de permitir que os usuários acessem aplicações e bancos de dados corporativos de forma centralizada – em redes dedicadas. O ZTNA cria conectividade exclusiva entre um usuário e uma aplicação, usando analytics comportamental baseado em contexto para controlar o acesso. O CASB oferece visibilidade, impõe políticas de segurança e conformidade e permite o controle do uso da nuvem de TI oculta, enquanto o FWaaS e o SWG evitam ameaças maliciosas e o acesso a sites e aplicações infectadas. Normalmente, uma solução de SSE tem um console unificado para visibilidade e governança e avalia a experiência do usuário com automação avançada.

Critérios de Elegibilidade

1. O SSE deve ser oferecido como uma **solução integrada** e deve ter os seguintes componentes essenciais: **rede de confiança zero (ZTNA), agente de segurança de acesso à nuvem (CASB), gateways de web seguros (SWG) e firewall como serviço (FWaaS).**
2. Os componentes acima devem ser **predominantemente baseados em software proprietário,** eles podem **depender parcialmente de soluções de parceiros,** mas **não podem depender totalmente de software de terceiros.**
3. Os fornecedores devem ter **PoPs localizados globalmente** para fornecer essas soluções.
4. A solução deve ser capaz de **fornecer SSE para ambientes de nuvem e locais** (incluindo ambientes híbridos).
5. A solução deve exibir **avaliações e análises contextuais e comportamentais (entidade do usuário e analytics de comportamento/UEBA)** para detectar e prevenir intenções maliciosas ou suspeitas.
6. A solução deve ser oferecida com **suporte básico de gerenciamento,** incluindo, entre outros, **geração de relatórios, controles de políticas,** instalação e manutenção e funcionalidades avançadas de detecção de ameaças.
7. A solução deve estar **totalmente e globalmente disponível.**

Definição

Os provedores de serviços técnicos de segurança (TSS) avaliados neste quadrante abrangem integração, manutenção e suporte para produtos ou soluções de segurança de TI e tecnologia operacional (OT). Eles também oferecem serviços de DevSecOps. O TSS aborda todos os produtos de segurança, incluindo antivírus, segurança em nuvem e data center, IAM, DLP, segurança de rede, segurança de endpoint, gerenciamento unificado de ameaças (UTM), segurança de OT, SASE e outros.

Os provedores de TSS oferecem manuais e roteiros padronizados que ajudam a transformar um ambiente de segurança existente com as melhores ferramentas e tecnologias, melhorando a postura de segurança e reduzindo o impacto das ameaças. Seus portfólios são projetados para permitir a transformação completa ou individual de uma arquitetura de segurança existente com produtos relevantes em domínios como redes, nuvem, local de trabalho, OT, IAM, privacidade e proteção de dados, gerenciamento de risco e conformidade e SASE, entre outros. As ofertas também incluem identificação, avaliação, design e desenvolvimento de produtos ou soluções, implementação, validação, testes de penetração, integração e implantação. Os provedores também utilizam soluções sofisticadas que permitem varredura abrangente de vulnerabilidades em aplicações, redes, endpoints e usuários individuais para descobrir pontos fracos e mitigar ameaças externas e internas.

Os provedores de TSS investem no estabelecimento de parcerias em domínios de tecnologia de segurança, nuvem, dados e rede para obter credenciamentos especializados e expandir o escopo de seus trabalhos e portfólios. Este quadrante também engloba serviços de segurança gerenciados clássicos, ou seja, aqueles fornecidos sem um centro de operações de segurança (SOC).

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

Critérios de Elegibilidade

1. Demonstrar experiência na **implementação de soluções de segurança** cibernética para empresas no respectivo país.
2. **Estar autorizado por fornecedores de tecnologia de segurança** (hardware e software) para distribuir e dar suporte a soluções de segurança.
3. Os provedores devem **empregar especialistas certificados** (as certificações podem ser credenciais patrocinadas por fornecedores, lideradas por associações e organizações ou de agências governamentais) capazes de oferecer suporte a tecnologias de segurança.

Definição

Os provedores de Serviços de Segurança Estratégica (SSS) avaliados neste quadrante oferecem consultoria para segurança de TI e OT. Os serviços abrangidos neste quadrante incluem auditorias de segurança, serviços de consultoria de conformidade e risco, avaliações de segurança, consultoria de arquitetura de solução de segurança e conscientização e treinamento. Esses serviços são usados para avaliar a maturidade de segurança e postura de risco e definir estratégias de segurança cibernética para empresas (adequadas para requisitos específicos).

Os provedores de SSS devem contratar consultores de segurança com ampla experiência em planejamento, desenvolvimento e gerenciamento de programas de segurança de ponta a ponta para empresas. Com a crescente necessidade desses serviços entre as PMEs e a falta de disponibilidade de talentos, os provedores de SSS também devem disponibilizar esses especialistas sob demanda por meio dos serviços do vCSIO (diretor de informações de segurança virtual). Dado o maior foco na resiliência cibernética, os provedores que oferecem SSS devem ser capazes de formular roteiros de continuidade de negócios e priorizar aplicações críticas de negócios para recuperação. Eles também devem realizar exercícios de simulação periódicos e exercícios cibernéticos para membros do conselho, principais executivos de negócios e funcionários para ajudá-los a desenvolver a alfabetização cibernética e estabelecer as melhores práticas para responder melhor às ameaças e ataques cibernéticos reais. Eles também devem estar familiarizados com as tecnologias e produtos de segurança disponíveis no mercado e oferecer conselhos sobre como escolher o melhor produto e fornecedor adequado aos requisitos específicos de uma empresa.

Este quadrante examina provedores de serviços que não estão focados exclusivamente em produtos ou soluções proprietárias. Os serviços aqui analisados cobrem todas as tecnologias de segurança, especialmente segurança de OT e SASE.

Critérios de Elegibilidade

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

Definição

Os provedores avaliados no quadrante Serviços Gerenciados de Segurança (SOC) (MSS (SOC)) oferecem serviços relacionados à operação e gerenciamento de infraestruturas de segurança de TI e OT para um ou vários clientes por um centro de operações de segurança (SOC). **Este quadrante examina provedores de serviços que não estão focados exclusivamente em produtos proprietários, mas podem gerenciar e operar as melhores ferramentas de segurança.** Esses provedores de serviços podem lidar com todo o ciclo de vida do incidente de segurança, desde a identificação até a resolução.

Há uma demanda crescente de fornecedores para ajudar as empresas a aprimorar sua postura geral de segurança de TI e maximizar a eficácia de seus programas de segurança a longo prazo com melhoria contínua.

Para conseguir isso, os provedores de MSS (SOC) devem combinar serviços gerenciados de segurança tradicionais com inovação para fortalecer seus clientes com um mecanismo integrado de defesa cibernética. Eles devem ser capazes de fornecer serviços gerenciados de detecção e resposta (MDR) e estar equipados com as mais recentes tecnologias, infraestrutura e especialistas qualificados em busca de ameaças e gerenciamento de incidentes, permitindo que as empresas detectem e respondam ativamente por meio da mitigação e contenção de ameaças. Devido às crescentes expectativas dos clientes em relação à busca proativa de ameaças, os provedores estão aprimorando seus ambientes de SOC com inteligência de segurança, com investimentos significativos em tecnologias como automação, big data, analytics, IA e aprendizado de máquina. Esses SOCs sofisticados devem oferecer suporte à resposta de inteligência de segurança orientada por especialistas, oferecendo aos clientes uma abordagem holística e unificada para segurança de nível avançado.

Eligibility Criteria

1. Os serviços típicos incluem **monitoramento de segurança, análise de comportamento, detecção de acesso não autorizado, consultoria sobre medidas de prevenção, teste de penetração, operações de firewall, operações de antivírus, serviços de operação de gerenciamento de identidade e acesso (IAM), operações de prevenção de vazamento/perda de dados (DLP)** e todos os outros serviços operacionais para fornecer proteção contínua em tempo real, sem comprometer o desempenho dos negócios. Em particular, a borda de serviço de acesso seguro (SASE) está incluída.
2. Capacidade de fornecer serviços de segurança, como **detecção e prevenção; informações de segurança e gerenciamento de eventos (SIEM)** e consultor de segurança e suporte de auditoria, remotamente ou no local do cliente.
3. Possuir **acreditações** de fornecedores de ferramentas de segurança.
4. **SOCs idealmente de propriedade e gerenciados pelo provedor** e não predominantemente por parceiros.
5. Manter **equipe certificada,** por exemplo, com certificações como Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) e Global Information Assurance Certification (GIAC).

Quadrantes Por Região

Como parte deste estudo de quadrantes do ISG Provider Lens™, estamos apresentando os sete quadrantes a seguir em Cybersecurity - Solutions and Services 2023:

Quadrants	EUA	Reino Unido	Nórdicos	Alemanha	Suíça	França	Brasil	Austrália	Singapura e Malásia	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	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Strategic Security Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Managed Security Services (SOC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

A fase de pesquisa ocorre no período entre janeiro e fevereiro de 2023, durante o qual ocorrerá o levantamento, avaliação, análise e validação. Os resultados serão apresentados à mídia em julho de 2023.

Etapas	Início	Encerramento
Lançamento da Pesquisa	12 de janeiro de 2023	
Fase de Pesquisa	12 de janeiro de 2023	13 de fevereiro de 2023
Prévia	maio de 2023	
Comunicado de Imprensa & Publicação	julho de 2023	

Consulte o link para visualizar/baixar a agenda de pesquisa ISG Provider Lens™ 2023

Acesso ao Portal On-line

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

Isenção de responsabilidade da produção de pesquisa:

O ISG coleta dados com o propósito de escrever pesquisas e criar perfis de provedor/fornecedor. Os perfis e dados de suporte são usados por consultores do ISG para fazer recomendações e informar seus clientes sobre a experiência e as qualificações de qualquer provedor/fornecedor aplicável para o trabalho de terceirização identificado pelos clientes. Esses dados são coletados como parte do processo ISG FutureSource e do processo Candidate Provider Qualification (CPQ). O ISG pode escolher utilizar esses dados coletados pertencentes a determinados países ou regiões para a educação e os propósitos de seus conselheiros e não para produzir relatórios ISG Provider Lens™. Essas decisões serão tomadas com base no nível e integridade das informações recebidas diretamente de provedores/fornecedores 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 notas informativas que serão escritas pelos analistas líderes.

ISG Star of Excellence™ – Chamada para indicações

O ISG Star of Excellence™ é um reconhecimento independente da prestação de serviços de excelência com base no conceito de "Voice of the Customer". O Star of Excellence é um programa desenvolvido pelo ISG para coletar feedback dos clientes sobre o sucesso dos provedores de serviços em demonstrar os mais altos padrões de excelência no atendimento ao cliente e foco no cliente.

A pesquisa global é sobre serviços associados a estudos de IPL. Consequentemente, todos os Analistas do ISG receberão continuamente informações sobre a experiência do cliente de todos os provedores de serviços relevantes. Esta informação junta-se ao feedback existente do consultor em primeira mão que o IPL utiliza no contexto de sua abordagem de consultoria liderada por profissionais.

Os provedores são convidados a nominate seus clientes para participar. Depois que a indicação é enviada, o ISG envia uma confirmação por e-mail para ambos os lados. É evidente que o ISG anonimiza todos os dados do cliente e não os compartilha com terceiros.

É nossa visão que o Star of Excellence seja reconhecido como o principal reconhecimento da indústria pela excelência no atendimento ao cliente e sirva como referência para medir os sentimentos do cliente. Para garantir que seus clientes selecionados concluam o feedback para seu compromisso indicado, use a seção de indicação de clientes no website do Star of Excellence.

Criamos um e-mail para o qual você pode encaminhar qualquer dúvida ou fazer comentários. Este e-mail será verificado diariamente. Aguarde até 24 horas para uma resposta. Aqui está o endereço de e-mail: star@isg-one.com

Contatos para este Estudo

Frank Heuer

Lead Analyst - Germany, Switzerland

Benoit Scheuber

Lead Analyst - France

David Pereira

Lead Analyst - Brazil

Deepika B

Research Analyst

Gowtham Kumar

Lead Analyst - U.S.

Dr. Maxime Martelli

Lead Analyst - France

Phil Hassey

Lead Analyst - U.S. Public Sector

Gabriel Sobanski

Research Analyst

Arun Kumar Singh

Lead Analyst - U.K., Nordics

Andrew Milroy

Lead Analyst - Australia

Bhuvaneshwari Mohan

Research Analyst

Ridam Bhattacharjee

Project Manager

Programa de Envolvimento de Consultores ISG Provider Lens™

O ISG Provider LensTM oferece avaliações de mercado que incorporam insights de profissionais, refletindo o foco regional e pesquisas independentes. O ISG garante o envolvimento do consultor em cada estudo para cobrir os detalhes apropriados do mercado alinhados às respectivas linhas de serviço/tendências tecnológicas, presença do provedor de serviços e contexto empresarial.

Em cada região, o ISG tem líderes de pensamento especializados e consultores respeitados que conhecem os portfólios e ofertas dos provedores, bem como os requisitos corporativos e as tendências do mercado. Em média, três consultores participam como parte da equipe de revisão de qualidade e consistência (QCRT) de cada estudo.

A QCRT garante que cada estudo reflita a experiência dos consultores do ISG no campo, o que complementa a pesquisa primária e secundária conduzida pelos analistas. Os conselheiros do ISG participam de cada estudo como parte do grupo QCRT e contribuem em diferentes níveis, dependendo de sua disponibilidade e experiência.

Os consultores da QCRT:

- Ajudam a definir e validar quadrantes e questionários,
- Aconselham sobre a inclusão do provedor de serviços, participam de chamadas de briefing,
- Apresentam suas perspectivas sobre as classificações do provedor de serviços e revisam os rascunhos dos relatórios.

Consultores do ISG para este Estudo

Doug Saylors

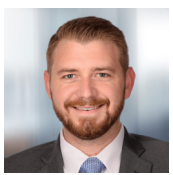
Co-lead, ISG Cybersecurity

Anand Balasubramanium

Senior Consultant

Roger Albrecht

Co-lead, ISG Cybersecurity



Alex Perry

Director

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 tenhamos a(s) pessoa(s) de contato correta(s) para participar ativamente desta pesquisa.

* Classificada na iteração anterior

Solution Providers

Absolute Software*
Acronis*
Akamai*
Aruba
Attivo Networks*
Avatier*
Axis Security
Barracuda Networks
BAYOONET*
Beta Systems*
Bitdefender*
Blackberry (Cylance)*
Brainloop*
Broadcom*
Cato Networks
Check Point*
Cisco*
Cloudflare*
CoSoSys*
CrowdStrike*
CyberArk*
Cybereason*
DriveLock*
Elastic
Ergon*
Ericom Software
ESET*
Fidelis Cybersecurity*
FireEye*
Forcepoint*
ForgeRock
Fortinet
GBS
Google
HelpSystems
IBM
iboss
Ilantus Products*
Infinite Networks
itWatch*
Kaspersky*
Lookout*
Matrix42*
Menlo Security
Micro Focus*
Microsoft*
Netskope*
Nevis*
Nexus
NordLayer
OGiTiX*
Okta*
Omada*
One Identity (OneLogin) *
Open Systems*
OpenText*
Oracle*
Palo Alto Networks*
Perimeter 81

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 tenhamos a(s) pessoa(s) de contato correta(s) para participar ativamente desta pesquisa.

* Classificada na iteração anterior

Ping Identity*
Proofpoint*
Rapid7*
RSA*
SailPoint*
SAP*
Saviynt*
Senhasegura*
SentinelOne*
SolarWinds*
Sophos*
Tehtris
Thales*
Trellix*
Trend Micro*
United Security Providers*
Varonis*
Versa Networks
VMware Carbon Black*
WithSecure
Zscaler

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 tenhamos a(s) pessoa(s) de contato correta(s) para participar ativamente desta pesquisa.

* Classificada na iteração anterior

Service Providers

Accenture*
Adarma
Alice&Bob.Company*
All for One Group*
AT&T Cybersecurity*
Atea
Atos*
Avanade Inc.
Aveniq*
Axians*
Bechtle*
Booz Allen Hamilton
Bridewell Consulting
BT Security
CANCOM*
Capgemini*
CGI*
Cognizant*
Computacenter*
Controlware*
Datacom*
Deloitte*
Deutsche Telekom*
DIGITALL*
DXC Technology*
Edge UOL*
EY*
Fujitsu*
Getronics*
glueckkanja-gab*
Happiest Minds*
HCLTech*
IBM*
iC Consult*
Indevis*
InfoGuard*
Infosys*
Insight UK
ISH Tecnologia
ISPIN*
KHIPU Networks
KPMG*
Kudelski Security*
Logicalis*
LTIMindtree
Lumen*
Mphasis*
MW Group
NCC Group*
Netic
Nixu*
NTT*
Orange Cyberdefense*
Performanta
Persistent Systems*
Proact IT Group
PwC*
Sapphire
Satisnet

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 tenhamos a(s) pessoa(s) de contato correta(s) para participar ativamente desta pesquisa.

* Classificada na iteração anterior

Secureworks*
SecurityHQ
Siemens
Six Degrees
Softcat
Sopra Steria*
Stefanini
Sunny Valley
suresecure*
Swisscom*
Syntax*
Talion
Talion
Tata Communications*
Tata Consultancy Services (TCS) *
Tech Mahindra*
Telia Cygate
Tempest*
terreActive*
Tesserent*
Thales*
Tietoevry*
Trustwave*
T-Systems*
UMB*
Unisys*
United Security Providers*
UST Global
Venzo Group
Verizon*
Wipro*
Zensar*

ISG Provider Lens™

The ISG Provider Lens™ Quadrant research series is the only service provider evaluation of its kind to combine empirical, data-driven research and market analysis with the real-world experience and observations of ISG's global advisory team. Enterprises will find a wealth of detailed data and market analysis to help guide their selection of appropriate sourcing partners, while ISG advisors use the reports to validate their own market knowledge and make recommendations to ISG's enterprise clients. The research currently covers providers offering their services across multiple geographies globally.

For more information about ISG Provider Lens research, please visit this webpage.

ISG Research™

ISG Research™ provides subscription research, advisory consulting and executive event services focused on market trends and disruptive technologies driving change in business computing. ISG Research delivers guidance that helps businesses accelerate growth and create more value.

ISG offers research specifically about providers to state and local governments (including counties, cities) as well as higher education institutions. Visit: Public Sector.

For more information about ISG Research subscriptions, please email contact@isg-one.com, call +1.203.454.3900, or visit research.isg-one.com.

ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 800 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis.

Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, visit www.isg-one.com.

ISG Provider Lens™

JANEIRO DE , 2023

BROCHURE: CYBERSECURITY - SOLUTIONS AND SERVICES