ISG Provider Lens™

Cyber Security - Solutions & Services

Data Leakage/Loss Prevention (DLP)

Brasil 2020

Quadrant Report

Um relatório de pesquisa comparando pontos fortes, desafios e diferenciadores competitivos dos fornecedores.

Customized report courtesy of:

opentext™

Agosto 2020

Sobre este Relatório

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 presentes neste relatório incluem pesquisa do programa ISG Provider Lens™, programas ISG Research™ em curso, entrevistas com consultores da ISG, reuniões de apresentação dos provedores de serviços e análises de informações de mercado disponíveis publicamente a partir de múltiplas fontes. Os dados coletados para este relatório representam informações que eram atuais maio 2020. A ISG reconhece que muitas fusões e aquisições podem ter ocorrido desde aquele período, mas tais mudanças não estão refletidas neste relatório.

Todas as referências a respeito de receitas estão em dólares americanos ($ US), a menos que expressamente disposto em sentido contrário.

O principal autor deste relatório é Pedro Luís Bicudo Maschio. As editoras são Ipshita Sengupta e Ambrosia Sabrina. A analista de pesquisa é Monica K e o analista de dados é Kankaiah Yasareni.

ISG Provider Lens™

ISG Provider Lens™

A ISG Provider Lens™ fornece estudos, pesquisas e consultoria práticas, de vanguarda, focando em tecnologia e nos pontos fortes e fracos de provedores de serviços, e em como estão posicionados com relação a seus pares no mercado. Esses relatórios fornecem insights influentes acessados por nossa ampla base de consultores, que estão ativamente aconselhando negócios de terceirização, bem como muitos clientes corporativos da ISG, que são potenciais terceirizadores.

Para mais informações sobre os estudos Provider Lens™ da ISG, por favor, mande um e-mail para ISGLens@isg-one.com, ligue para +1.203.454.3900 ou visite ISG Provider Lens™.

ISG Research™

A ISG Research™ fornece pesquisa por assinatura, consultoria recomendatória e serviços de eventos executivos com foco em tendências do mercado e tecnologias disruptivas causando mudanças na computação corporativa. A ISG Research™ entrega diretrizes que ajudam negócios a acelerar o crescimento e criar mais valor comercial.

Para mais informações sobre as assinaturas da ISG Research, envie um e-mail para contact@isg-one.com, ligue para +1.203.454.3900 ou acesse research.isg-one.com.

1 Sumário Executivo

7 Introdução

18 Data Leakage/Loss Prevention (DLP)

30 Metodologia

SUMÁRIO EXECUTIVO

Tendências Gerais

A crescente importância da segurança cibernética está mudando a maneira como as empresas adquirem serviços estratégicos de segurança. Os principais executivos estão cada vez mais ativos na tomada de decisões e estão interessados em entender os riscos cibernéticos. Regulamentos mais rigorosos estão levando à maturidade do mercado de segurança. No Brasil, a aplicação da Lei Geral de Proteção de Dados (LGPD) exige que a maioria das empresas altere seus processos e tecnologias de suporte em torno da proteção de dados e define funções, responsabilidades e penalidades de acordo. Agosto de 2020 era o prazo final para conformidade das organizações sediadas no Brasil. No entanto, com o lockdown parcial da COVID-19, muitas empresas de consultoria estão especulando que o prazo será estendido.

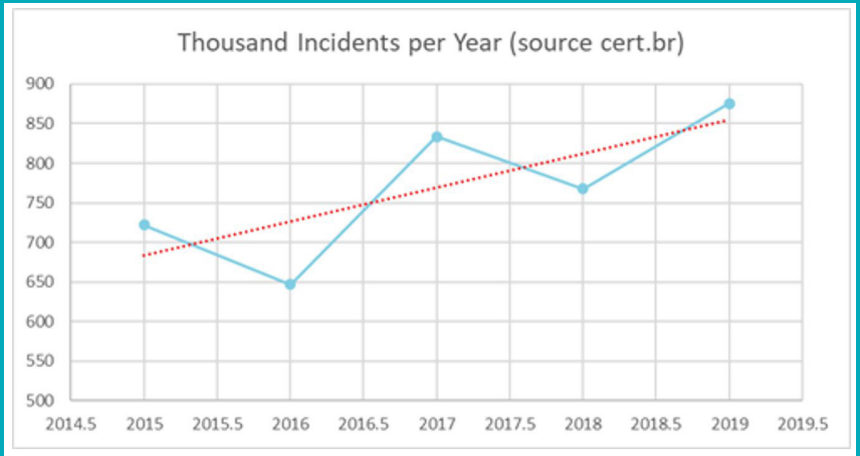
O surto de COVID-19 no Brasil ocorreu em março de 2020, no momento em que os participantes estavam respondendo ao questionário desse estudo. Os dados coletados não foram impactados e os efeitos da COVID-19 não foram considerados na análise. Durante os briefings, alguns fabricantes e fornecedores participantes relataram que os clientes aceleraram suas decisões para atualizar o software de segurança e implementar novas medidas de segurança cibernética que estavam em negociação para melhorar e proteger o trabalho em casa. Da mesma forma, os provedores de serviços relataram sua capacidade de trabalhar em casa, incluindo aqueles que realizam monitoramento e resposta a incidentes.

ISG Provider Lens™

Strategic Services Trends

Há uma percepção de que os ataques cibernéticos aumentaram durante a COVID-19; no entanto, as estatísticas não estão disponíveis para o Brasil. O número de incidentes de segurança relatados aumentou 14% em 2019. Os dados de cinco anos mostram essa tendência de aumento. A maioria dos incidentes no ano em questão, 69%, teve origem no país. O aumento de incidentes também corresponde à atenção dos principais executivos para melhorar as medidas de segurança.

Imagem: Mais de 850.000 incidentes relatados ao CERT brasileiro em 2019



Nos últimos anos, a consultoria em torno da estratégia de TI havia perdido a atenção das empresas de consultoria de negócios. Em vez disso, as discussões de estratégia mudaram para negócios digitais e transformação digital. A crescente importância da segurança cibernética está obrigando as empresas de consultoria tradicionais a se concentrarem nas avaliações e no design da arquitetura de tecnologia cibernética. Essas empresas estão contratando especialistas, anunciando novas ofertas de serviços e estabelecendo laboratórios de segurança cibernética. Algumas estão renovando seus escritórios para incluir tecnologias de segurança cibernética para treinamento, experimentação e sandbox.

Grandes empresas de consultoria vêm reestruturando seu portfólio de consultoria estratégica para incluir segurança cibernética. A governança, o risco e a conformidade (GRC), que antes eram focados em fatores de negócios, agora incluem segurança cibernética devido às implicações de uma violação de dados ou um ataque de ransomware nos custos e na imagem da marca. Regulamentos como a GDPR para empresas europeias presentes no Brasil ou o LGPD brasileira também têm um impacto significativo na adoção de medidas de segurança cibernética devido às altas penalidades monetárias envolvidas. Todos os provedores incluídos neste quadrante possuem avaliações de prontidão para LGPD e serviços de design de conformidade em seu portfólio.

Entre as 55 empresas participantes deste estudo, 16 se qualificaram para esse quadrante. Seis são líderes e uma é uma Rising Star.

Technical Services Trends

Um grande número de soluções de segurança está disponível no mercado, mas, apesar do número de opções, há falhas de cobertura de segurança. Os principais fornecedores de serviços desenvolveram plataformas proprietárias que integram muitas soluções de segurança e preenchem lacunas de segurança com funcionalidades específicas desenvolvidas para esse fim.

O mercado no Brasil é altamente fragmentado, com centenas de provedores de serviços oferecendo serviços de integração. No entanto, a maioria não possui experiência adequada ou opera apenas em uma região específica. Eles permanecem no mercado para oferecer suporte a clientes de fornecedores globais de software, localmente; o vasto território do Brasil e a baixa densidade de negócios obrigam os fornecedores globais a buscar muitas pequenas empresas parceiras para cobrir todas as regiões. A ISG não inclui esses nichos, pequenos concorrentes, porque eles não podem lidar com implementações em escala empresarial.

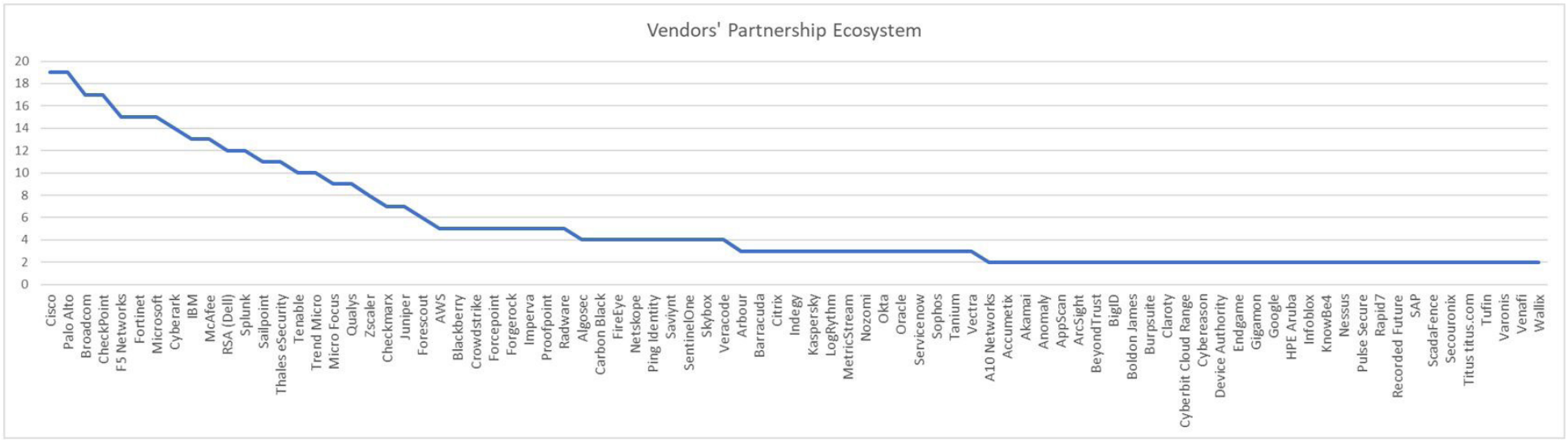
Os parceiros de serviço são os principais canais de vendas para fornecedores de software. Eles apoiam o relacionamento com os clientes e são os consultores confiáveis que estimam a capacidade e escrevem os requisitos do sistema. Os produtos de segurança exigem dispositivos de alto desempenho e configurações complexas de nuvem e rede. Os consultores dos parceiros de serviço projetam a arquitetura de implementação e o plano do projeto e combinam os requisitos com os modelos e o software do dispositivo.

Os clientes que adquirem soluções de segurança devem, a princípio, identificar os parceiros de serviço no mercado local que podem fornecer engenharia, arquitetura e integração. O processo de aquisição deve agrupar os parceiros de software, hardware e serviço, equilibrando a decisão de garantir suporte de serviço a longo prazo. Em particular, para soluções de segurança, os clientes podem precisar de assistência imediata em caso de violação de dados e ataques cibernéticos. Os prestadores de serviços no Brasil normalmente têm parcerias com 24 fornecedores. Essa diversidade permite que os especialistas em segurança técnica dos provedores aconselhem os clientes sobre a melhor configuração da solução.

Este estudo identificou 220 fornecedores de software de segurança. O gráfico a seguir ilustra a dispersão do ecossistema de parceiros, mostrando que os dez primeiros têm um ecossistema mais saudável em comparação com o restante.

Imagem: Número de parceiros para cada fornecedor.

Dos 55 participantes deste estudo, 18 se qualificaram para este quadrante. Seis são líderes e um é uma Rising Star.



Managed Security Services Trends

Os serviços gerenciados de segurança estão evoluindo de SOCs (Centros de Operações de Segurança) para organizações complexas do tipo exército de defesa cibernética com inteligência artificial.

Os serviços de SOC normalmente incluem alertas de monitoramento gerados por soluções de segurança e soluções de monitoramento de eventos, como firewalls, ferramentas de segurança de terminais, roteadores de rede e software antimalware. No entanto, eles incluem segurança básica, o que não é suficiente para impedir ameaças sofisticadas.

O cibercrime está se tornando mais complexo com o uso da IA para automatizar a criação de ameaças, identificar vulnerabilidades e espalhar malware. Para se defender, as empresas precisam se manter atualizadas com o uso de ferramentas sofisticadas. Consequentemente, surgiram os Centros de Defesa Cibernética (CDCs), não para substituir os SOCs, mas para expandir as operações de segurança.

Os CDCs incluem ferramentas avançadas de aprendizado de máquina (ML) que ingerem grandes quantidades de dados e usam análises inteligentes para identificar como as ameaças estão se transformando e se espalhando. Além disso, essas organizações compartilham informações entre si para se manter atualizadas sobre ameaças cibernéticas. Novas ferramentas surgiram, como a microssegmentação, permitindo que especialistas isolem hackers ou bots quando esses invadem uma rede corporativa.

Serviços relacionados à governança de gerenciamento de identidades e proteção de dados que ajudam os clientes a regular o acesso gerenciam a segregação de tarefas e até produzem evidências sobre a existência de medidas de proteção antes de uma violação de dados, reduzindo assim as consequências (e penalidades em caso de requisitos de conformidade). Os serviços gerenciados de segurança cibernética, portanto, tornaram-se uma necessidade para as empresas.

As empresas que utilizam serviços gerenciados de segurança (MSS) devem avaliar as ferramentas que os provedores de serviços possuem. Além disso, eles devem prestar atenção aos acordos de nível de serviço (SLAs). Um SLA típico de serviço de segurança envolve 15 minutos para responder (começar a trabalhar no incidente) e quatro horas de resolução (eliminar o problema). Essas medidas antigas são adequadas para incidentes internos, como aplicação de patch em uma área de trabalho, alteração de uma regra de firewall ou correção de uma configuração incorreta do AWS S3 bucket. No entanto, levar 15 minutos para reagir pode ser fatal, pois é suficiente para um cyber bot de ransomware atingir um ponto irrecuperável. As empresas precisam repensar suas expectativas de serviço e trabalhar em negócios inovadores. Ao mesmo tempo, os provedores de serviços devem trabalhar imediatamente, alocando os recursos necessários, sem temer não serem compensados pelo custo adicional incorrido. SLAs cronometrados não têm sentido em segurança. Novos acordos devem penalizar por não agir para impedir um ataque, falta de habilidades disponíveis, ferramentas com defeito ou comportamento lento. A tomada

rápida de decisões é crucial para interromper um ataque. Portanto, falhas na resolução e erros humanos não devem ser penalizados. À medida que um ataque evolui, mais recursos são necessários e os custos aumentam. Um acordo equilibrado permite um pagamento extra pela alocação de recursos adicionais, além de compartilhar o risco com o provedor, que não deve cobrar horas extras, uso de ferramentas, licenças e custos indiretos.

Das 55 empresas avaliadas neste estudo, 21 se qualificaram para esse quadrante. Oito são líderes e uma é uma Rising Star.

IAM Software Market Trends

O gerenciamento de identidade e acesso (IAM) está se tornando cada vez mais importante com a adoção da nuvem. O logon único federado (SSO) permite que um usuário identificado acesse vários sistemas que residem em redes ou nuvens separadas. Portanto, o IAM envolve a autenticação em um sistema, com acesso seguro nos outros.

O IAM está evoluindo de ferramentas internas, como o protocolo de aplicação aberto (LDAP) ou Microsoft AD, para plataformas de diretório baseadas na nuvem, devido ao crescente uso do software como serviço (SaaS) por quase todas as empresas. Outra tendência é o IAM como serviço, uma consequência natural de tudo o que está migrando para a nuvem.

Os participantes do mercado que possuem soluções legadas do IAM adaptaram suas plataformas para instalar e executar na nuvem. Os concorrentes que desenvolveram suas soluções na nuvem e para a nuvem afirmam ter melhores interfaces de programa de aplicações (APIs) para fornecer SSO federado. As duas abordagens para o desenvolvimento e hospedagem do IAM estão competindo ferozmente, mas existem prós e contras para cada solução. Os clientes que possuem aplicações legadas usando ferramentas IAM legadas podem ser melhor atendidos com atualizações, enquanto outro cliente que se transformou na nuvem pode achar vantajoso o IAM nativo da nuvem.

O IAM para consumidor (CIAM) é de crescente interesse, impulsionado por solicitações de conformidade. O CIAM permite que as informações privadas do cliente residam na ferramenta de IAM, seguras e criptografadas, em vez de gerar dados e senhas de privacidade em vários sistemas. A identidade em blockchain está sendo testada por pelo menos dois fornecedores, mas nenhum caso real em produção pôde ser identificado para inclusão neste estudo.

É cedo para dizer se o IAM compartilhado prevalecerá como um Serviço. No entanto, alguns fornecedores acreditam que este é o caminho a seguir. Ao habilitar o IAM como serviço escalonável, hospedado em nuvem e atendendo várias empresas, os fornecedores imaginam a possibilidade de se tornarem fornecedores globais de serviços de identidade em um futuro, onde um indivíduo teria uma única identidade digital em vez de várias cópias em muitas empresas e sistemas.

As empresas que adquirem o software de IAM devem considerar suas necessidades particulares. O suporte ao fornecedor, a rede de parceiros e o roteiro de desenvolvimento de produtos devem ser rigorosamente avaliados, pois a tecnologia está mudando rapidamente diante da evolução das tecnologias de identificação, das novas ofertas de SaaS e dos crescentes requisitos para incluir a funcionalidade do IAM nos DevOps e contêineres, bem como para proteger os dispositivos da Internet das Coisas (IoT).

Dos 55 prestadores de serviços avaliados neste estudo, 17 se qualificaram para esse quadrante. Seis são líderes e um é uma Rising Star.

DLP Software Market Trends

As ferramentas de prevenção contra perda de dados (DLP) estão aumentando em importância para as empresas no Brasil devido à Lei Geral de Proteção de Dados (LGPD), equivalente ao GDPR para o Brasil, que exige privacidade e proteção de dados. A LGPD havia planejado agosto de 2020 como o prazo final para conformidade para as organizações com sede no Brasil. No entanto, com o lockdown parcial da COVID-19, muitas empresas de consultoria estão especulando que o prazo será estendido.

As ferramentas avançadas de DLP podem verificar arquivos e bancos de dados em busca de dados particulares, marcar esses ativos e emitir um alerta em caso de intervenção. Os clientes podem definir regras para processar esses ativos. As opções são: excluir dados de privacidade de arquivos ou bancos de dados, ofuscar os dados privados, substituir dados, criptografar dados ou mover arquivos para armazenamento seguro. Ao usar ferramentas de DLP, os clientes podem corrigir dados ou arquivos antigos para cumprir com os novos regulamentos relacionados a dados.

Os clientes devem estar cientes de que algumas soluções de DLP são altamente eficientes e sofisticadas, por exemplo, aquelas projetadas para dar suporte a transações de alto volume de grandes instituições financeiras. Outras empresas podem segregar logicamente dados de privacidade e dados de transações, exigindo soluções de DLP menos complexas para lidar com privacidade e LGPD. O primeiro fator a considerar ao adquirir soluções de DLP é a frequência com que os dados privados e confidenciais são alterados. Alterar os processos de negócios para segregar dados privados e confidenciais reduz a complexidade (e o custo) das soluções de DLP.

Os clientes que adquirem soluções de DLP devem procurar parceiros locais e verificar seus recursos de implementação, suporte pós-venda e modelos de licenciamento. Se a principal preocupação for a conformidade, os clientes devem se concentrar em ferramentas que buscam e ofuscam dados. Os clientes preocupados com dados que causam malware, ransomware, violações de dados e proteção à propriedade intelectual devem considerar ferramentas que fornecem monitoramento de acesso a dados em tempo real e bloqueio de acesso automatizado. Alguns fornecedores oferecem bloqueio em tempo real e sua eficácia varia de acordo com a configuração e o contexto. Ferramentas de inspeção de tráfego que fornecem microssegmentação podem ser necessárias para bloquear o acesso a dados e impedir ataques de ransomware.

Dos 55 prestadores de serviços avaliados neste estudo, 15 se qualificaram para este quadrante e seis foram nomeados Líderes.

Introdução

Definição

Com a digitalização e a Internet das Coisas Industrial (IIoT), os processos de negócios estão cada vez mais focados na necessidade crescente de proteger os sistemas de TI e comunicação nas empresas, tanto que a segurança de TI passa a representar a segurança dos negócios.

As infraestruturas de dados e TI são constantemente expostas a ameaças cibernéticas. Além da necessidade de proteger dados confidenciais sensíveis nas organizações, a aplicação de regulamentos como o Regulamento Geral de Proteção de Dados (GDPR) na Europa obriga as empresas a implementar salvaguardas mais fortes para combater ataques cibernéticos.

No entanto, os executivos de TI costumam se esforçar para justificar investimentos em segurança para as partes interessadas nos negócios, principalmente os CFOs. Ao contrário de outros investimentos relacionados à TI, nem sempre é possível medir ou demonstrar o retorno do investimento (RoI) em ameaças à segurança. Portanto, as medidas de segurança geralmente não são suficientes para lidar com ameaças sofisticadas. Por outro lado, a falta de tecnologia adequada não é a única razão para vulnerabilidades de segurança; muitos incidentes de segurança como ataques de Trojan e phishing são causados devido ao descuido dos usuários. Portanto, os treinamentos de usuários desempenham um papel fundamental, juntamente com tecnologia e equipamentos de TIC atualizados, para evitar ameaças cibernéticas.

O estudo 2020 ISG Provider Lens™ Cyber Security - Solutions & Services visa apoiar os tomadores de decisão de TIC na otimização de seus orçamentos de segurança.

Definição (cont.)

Scope of Report

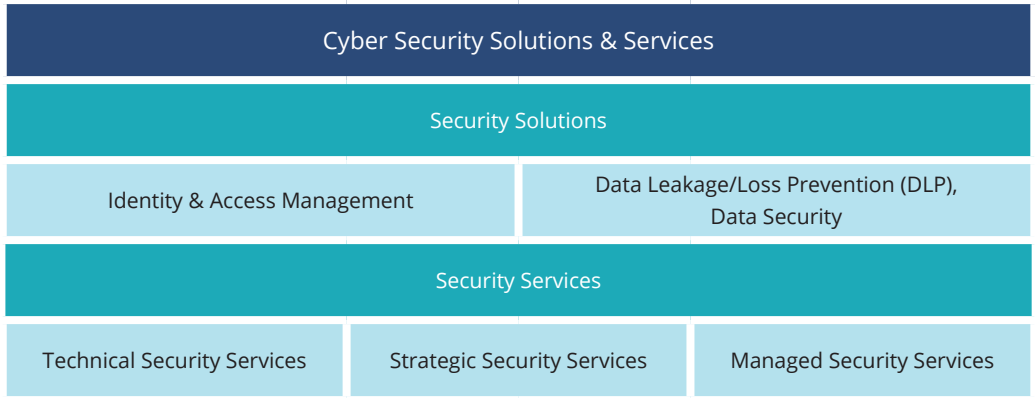
O estuda ISG Provider Lens™ oferece o seguinte aos tomadores de decisão de TI:

- Transparência quanto aos pontos fortes e de atenção dos fornecedores relevantes
- Posicionamento diferenciado de fornecedores por segmentos
- Perspectiva de mercados, incluindo EUA, Alemanha, Suíça, Reino Unido, países nórdicos e Brasil.

Os estudos de pesquisa de mercado da ISG servem como uma importante base de tomada de decisão para posicionar os principais relacionamentos e considerações de entrada no mercado. Os consultores da ISG e os clientes corporativos usam as informações desses relatórios para avaliar seus relacionamentos atuais com fornecedores e possíveis compromissos.

Portanto, os estudos da ISG compreendem vários quadrantes que cobrem o espectro de serviços que um cliente corporativo exige, conforme ilustrado na figura a seguir:

Simplified Illustration



Source: ISG 2020

Definição (cont.)

As descrições dos quadrantes são as seguintes:

Gerenciamento de identidade e acesso (IAM): Ele compara os fornecedores de produtos usados para coletar, registrar e gerenciar identidades de usuários e direitos de acesso relacionados. Esse mercado inclui modelos de licenciamento de software no local, SaaS e opções de serviço somente na nuvem.

Prevenção de vazamento/perda de dados (DLP): Ele compara fornecedores de produtos que identificam e monitoram dados confidenciais, restringem o acesso apenas a usuários autorizados e evitam o vazamento de dados. Esse quadrante inclui dispositivos, licenciamento de software no local, SaaS e opções de serviço somente na nuvem.

Serviços estratégicos de segurança: Esse quadrante inclui consultoria para soluções de segurança, governança, risco e conformidade de TI. Ele examina os provedores de serviços que não têm foco exclusivo em produtos ou soluções proprietárias.

Serviços técnicos de segurança: Essa avaliação de mercado inclui os provedores de serviços de integração, manutenção e suporte para soluções de segurança de TI. Esse quadrante examina os provedores de serviços que não têm foco exclusivo em seus respectivos produtos proprietários e podem implementar e integrar soluções de fornecedores.

Serviços gerenciados de segurança: Esse quadrante inclui operações e gerenciamento de infraestruturas de segurança de TI para um ou vários clientes por um SOC. Os serviços típicos incluem monitoramento de segurança, análise de comportamento, detecção de acesso não autorizado, aconselhamento sobre medidas preventivas, teste de penetração, operações de firewall, operações antivírus, serviços de operação de IAM, operações de DLP e outros serviços operacionais.

Classificações de Fornecedor

Os quadrantes da ISG Provider Lens™ foram criados usando uma matriz de avaliação contendo quatro segmentos, onde os fornecedores estão posicionados em conformidade.

Leader

Os líderes (leaders) entre os distribuidores/fornecedores, têm um produto altamente atraente e oferta de serviços, bem como um mercado muito forte e posição competitiva; eles cumprem todas as exigências para o cultivo bem-sucedido do mercado. Eles podem ser considerados como formadores de opinião, fornecendo impulsos estratégicos ao mercado. Também garantem força inovadora e estabilidade.

Product Challenger

Os desafiadores com produto (product challengers) oferecem um portfólio de produtos e serviços que fornece uma cobertura de exigências corporativas acima da média, mas também não são capazes de fornecer os mesmos recursos e pontos fortes que os líderes em relação às categorias de cultivo de mercado individuais. Com frequência, isso se deve ao tamanho do respectivo distribuidor ou de sua fraca projeção/foco no respectivo segmento alvo (quadrante).

Market Challenger

Desafiadores com mercado (Market challengers) também são muito competitivos, mas ainda há potencial para ampliação de seu portfólio, e eles claramente ficam atrás dos líderes. Com frequência, os desafiadores com mercado são fornecedores estabelecidos, mas de certa forma lentos na abordagem de novas tendências, devido ao tamanho e estrutura da empresa, tendo, portanto, algum potencial para otimizar seus portfólios e aumentar suas atratividades.

Contender

Competidores em geral (Contenders) ainda precisam de produtos e serviços maduros ou profundidade e amplitude suficientes de suas ofertas, enquanto também mostram alguns pontos fortes e potenciais de melhorias em seus esforços de cultivo de mercado. Esses distribuidores são frequentemente generalistas ou focados em um nicho de mercado.

Classificações de Fornecedor (cont.)

Cada quadrante ISG Provider Lens™ pode incluir um ou mais fornecedores de serviços que a ISG acredita ter forte potencial para alcançar o quadrante de leader.

Rising Star

Rising stars são “estrelas em ascenção”, basicamente são fornecedores com alto potencial no futuro. Ao receber o selo rising star, tais empresas têm um portfólio promissor, incluindo o roteiro necessário e um foco adequado nas tendências-chave do mercado e exigências dos clientes. Além disso, o rising star tem excelente gerenciamento e entendimento do mercado local. Este selo somente é dado a distribuidores ou fornecedores de serviços que fizeram grande progresso em seus objetivos nos últimos 12 meses e estão em um bom caminho para alcançar o quadrante de líderes nos próximos 12-24 meses, em função de seu impacto e força inovadora acima da média.

Not In

Esse fornecedor de serviços ou distribuidor não foi incluído neste quadrante porque a ISG não conseguiu obter informações suficientes para posicioná-lo. Essa omissão não implica que o fornecedor de serviços ou distribuidor não fornece tal serviço.

Cyber Security - Solutions & Services - Lista de Participantes 1 de 4

	Identity & Access Management	Data Leakage/Loss Prevention (DLP)	Technical Security Services	Strategic Security Services	Managed Security Services
Absolute Software	Not In	Contender	Not In	Not In	Not In
Accenture	Not In	Not In	Not In	Leader	Product Challenger
Agility Networks Tecnologia	Not In	Not In	Leader	Contender	Leader
Atos	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Broadcom	Leader	Leader	Not In	Not In	Not In
Capgemini	Not In	Not In	Leader	Product Challenger	Product Challenger
CenturyLink	Not In	Not In	Not In	Not In	Leader
Cipher	Not In	Not In	Not In	Contender	Product Challenger
Compasso UOL	Not In	Not In	Not In	Not In	Leader
Compugraf	Not In	Not In	Contender	Not In	Not In
CorpFlex	Not In	Not In	Not In	Not In	Product Challenger
Dell/RSA	Market Challenger	Not In	Not In	Not In	Not In
Deloitte	Not In	Not In	Leader	Leader	Product Challenger
DXC Technology	Not In	Not In	Rising Star	Product Challenger	Contender
E-TRUST	Rising Star	Not In	Not In	Not In	Not In

Cyber Security - Solutions & Services - Lista de Participantes 2 de 4

	Identity & Access Management	Data Leakage/Loss Prevention (DLP)	Technical Security Services	Strategic Security Services	Managed Security Services
EY	Not In	Not In	Not In	Leader	Not In
Forcepoint	Not In	Leader	Not In	Not In	Not In
Forgerock	Product Challenger	Not In	Not In	Not In	Not In
Fortinet	Contender	Not In	Not In	Not In	Not In
GBS	Not In	Contender	Not In	Not In	Not In
Google	Not In	Contender	Not In	Not In	Not In
IBM	Leader	Leader	Market Challenger	Leader	Leader
ISH Tecnologia	Not In	Not In	Leader	Market Challenger	Leader
Logicalis	Not In	Not In	Leader	Leader	Leader
McAfee	Not In	Leader	Not In	Not In	Not In
Micro Focus/Fortify	Contender	Not In	Not In	Not In	Not In
Microsoft	Leader	Market Challenger	Not In	Not In	Not In
NEC (Arcon)	Not In	Not In	Product Challenger	Contender	Contender
Netspoke	Not In	Contender	Not In	Not In	Not In
Nextios	Not In	Not In	Contender	Not In	Not In

Cyber Security - Solutions & Services - Lista de Participantes 3 de 4

	Identity & Access Management	Data Leakage/Loss Prevention (DLP)	Technical Security Services	Strategic Security Services	Managed Security Services
NTT	Not In	Not In	Leader	Not In	Not In
Okta	Leader	Not In	Not In	Not In	Not In
One Identity	Product Challenger	Not In	Not In	Not In	Not In
OneLogin	Product Challenger	Not In	Not In	Not In	Not In
OpenText	Not In	Leader	Not In	Not In	Not In
Oracle	Leader	Not In	Not In	Not In	Not In
Ping Identity	Product Challenger	Not In	Not In	Not In	Not In
PwC	Not In	Not In	Not In	Leader	Not In
SailPoint	Contender	Not In	Not In	Not In	Not In
SAP	Market Challenger	Not In	Not In	Not In	Not In
senhasegura	Leader	Not In	Not In	Not In	Not In
Sonda	Not In	Not In	Contender	Not In	Market Challenger
Stefanini Rafael	Not In	Not In	Contender	Rising Star	Leader
TDec Network	Not In	Not In	Contender	Not In	Not In
Tempest Security Intelligence	Not In	Not In	Product Challenger	Contender	Contender

Cyber Security - Solutions & Services - Lista de Participantes 4 de 4

	Identity & Access Management	Data Leakage/Loss Prevention (DLP)	Technical Security Services	Strategic Security Services	Managed Security Services
Thales eSecurity	Market Challenger	Not In	Not In	Not In	Not In
Titus	Not In	Contender	Not In	Not In	Not In
TIVIT	Not In	Not In	Not In	Not In	Contender
Trend Micro	Not In	Leader	Not In	Not In	Not In
T-Systems	Not In	Not In	Contender	Not In	Product Challenger
Unisys	Not In	Not In	Not In	Market Challenger	Leader
Varonis	Not In	Leader	Not In	Not In	Not In
WatchGuard Technologies	Not In	Product Challenger	Not In	Not In	Not In
Wipro	Not In	Not In	Product Challenger	Product Challenger	Rising Star
Zscaler	Not In	Contender	Not In	Not In	Not In

Cyber Security - Solutions & Services Quadrantes

CONTEXTO DO EMPREENDIMENTO

Data Leakage/Loss Prevention (DLP)

Este relatório é relevante para empresas de todos os setores do Brasil na avaliação de fabricantes de produtos de prevenção de vazamento/perda de dados (DLP), incluindo serviços de nuvem, que identificam e monitoram dados confidenciais, fornecem acesso apenas a usuários autorizados e evitam o vazamento de dados.

Neste relatório de quadrantes, a ISG destaca o atual posicionamento do mercado de fabricantes de soluções DLP e de segurança de dados no Brasil e a maneira como eles lidam com os principais desafios enfrentados pelas empresas no país. A ISG observa que as empresas estão enfrentando o desafio de controlar movimentos/transferências de dados à medida que a conectividade se torna onipresente.

O mercado de cibersegurança no Brasil é maduro e competitivo, com a presença de fornecedores globais e concorrentes locais. O uso de soluções de DLP está crescendo à medida que a segurança dos dados continua sendo importante, e devido à necessidade de cumprir a Lei Geral de Proteção de Dados Pessoais (LGPD), onde as ferramentas de DLP ajudam na conformidade.

Os líderes de TI e tecnologia devem ler este relatório para entender o posicionamento e os recursos relativos das soluções de DLP. O relatório também compara as capacidades técnicas dos vários fabricantes presentes no mercado.

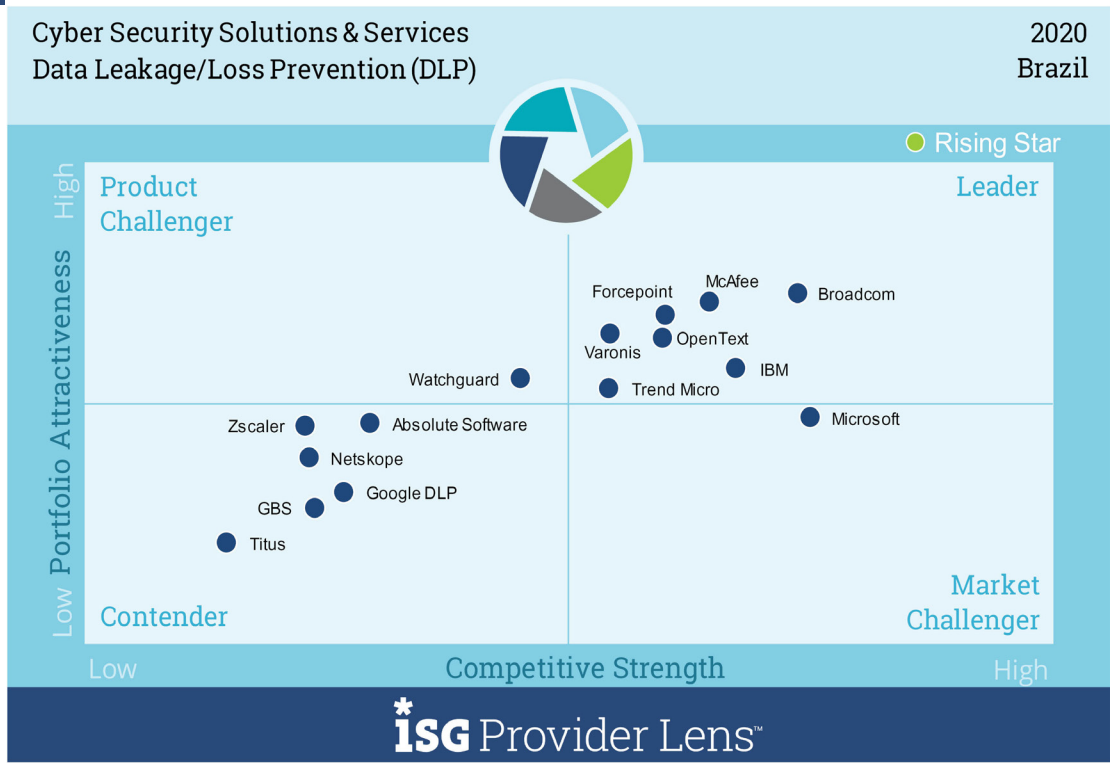
Os profissionais de segurança e dados devem ler este relatório para entender como os fabricantes, suas ferramentas e soluções de segurança de DLP ajudam a cumprir a LGPD no Brasil e como eles podem ser comparados entre si.

Os líderes de conformidade e governança devem ler este relatório para entender o panorama da DLP, pois ele afeta diretamente a conformidade com a LGPD.

DATA LEAKAGE/LOSS PREVENTION (DLP)

Definição

Os produtos de DLP podem identificar e monitorar dados confidenciais, restringir o acesso apenas a usuários autorizados e impedir o vazamento de dados. Os produtos de DLP estão ganhando considerável importância, pois tornou-se difícil para as empresas controlar movimentos e transferências de dados com o aumento do número de dispositivos, inclusive móveis, usados para armazenar dados. Geralmente, eles são equipados com conexão à Internet e podem enviar e receber dados sem passar por um gateway central da Internet. Os dispositivos incluem uma infinidade de interfaces, como portas USB, Bluetooth, rede local sem fio (WLAN) e comunicação de campo próximo (NFC), permitindo o compartilhamento contínuo de dados. Esse quadrante inclui dispositivos, licenciamento de software local, SaaS e opções de serviço apenas na nuvem.



Source: ISG Research 2020

DATA LEAKAGE/LOSS PREVENTION (DLP)

Critérios de Elegibilidade

- Relevância (receita, número de clientes) como fornecedor de produtos de DLP no Brasil
- Oferta de DLP baseada em software proprietário e não em software de terceiros

Observações

As ferramentas de DLP estão se tornando cada vez mais importantes para as empresas no Brasil. A LGPD, equivalente ao GDPR da Europa, para privacidade e proteção de dados, determinou agosto de 2020 como o prazo final para a conformidade de empresas com sede no Brasil. No entanto, é duvidoso que as empresas no Brasil possam fazer todas as alterações necessárias para se tornarem compatíveis até agosto de 2020 devido à situação da COVID-19; alguns analistas especulam que o Congresso possa mudar esse prazo. No entanto, para fornecedores de DLP, a alteração da data pode não afetar as expectativas de vendas e crescimento, porque muitos clientes já iniciaram programas de conformidade.

As ferramentas avançadas de DLP podem verificar arquivos e bancos de dados em busca de dados privados, marcar esses ativos e alertar em caso de qualquer intervenção. Os clientes podem definir regras para processar esses ativos. As opções são: excluir dados de privacidade de arquivos ou bancos de dados, ofuscar os dados privados, substituir dados, criptografar dados ou mover arquivos para armazenamento seguro. Ao usar as ferramentas de DLP, os clientes podem verificar, pesquisar e encontrar não-conformidades para permitir correções antes de auditorias ou violações de dados.

DATA LEAKAGE/LOSS PREVENTION (DLP)

Observações (cont.)

Os clientes devem estar cientes de que algumas soluções são altamente eficientes e sofisticadas, por exemplo, aquelas projetadas para dar suporte a transações de alto volume em grandes instituições financeiras. Os varejistas e o comércio eletrônico que possuem altos volumes de transações podem segregar logicamente dados particulares e dados de transação; a última exigindo soluções de DLP menos complexas para lidar com privacidade e conformidade com a LGPD. O primeiro fator a considerar ao adquirir a DLP está relacionado à frequência com que os dados privados e confidenciais são alterados. Alterar os processos de negócios para segregar dados privados e confidenciais reduz a complexidade (e o custo) das soluções de DLP.

Os tomadores de decisão das soluções de DLP são o CIO, CTO, CISO e o diretor de conformidade, quando a função existe na organização. Os clientes que adquirem soluções de DLP devem procurar parceiros locais e seus recursos de implementação, suporte pós-venda e modelo de licenciamento. Se a principal preocupação for a conformidade, os clientes devem se concentrar em ferramentas que buscam e ofuscam dados. Os clientes preocupados com dados danosos de malware, ransomware, violações de dados e proteção à propriedade intelectual devem considerar ferramentas que fornecem monitoramento de acesso a dados em tempo real e bloqueio automático de acesso. Alguns fornecedores oferecem bloqueio em tempo real, onde a eficácia varia de acordo com a configuração e o contexto. Ferramentas de inspeção de tráfego que fornecem microssegmentação podem ser necessárias para impedir o acesso a dados e ransomware.

Algumas soluções de DLP permitem que os usuários ou aplicativos marquem informações particulares e confidenciais antes de salvar o arquivo. Essas soluções de DLP mais diretas inspecionam o arquivo, formulário, e-mail ou mensagem antes de enviá-los ou salvá-los, identificando e evitando a não conformidade. Essas ferramentas não se referem a bancos de dados e documentos existentes. O segundo tipo de soluções de DLP inspeciona arquivos, bancos de dados e documentos existentes para identificar e corrigir a não conformidade. No entanto, eles não impedem que o próximo documento seja salvo, encontrando uma não conformidade somente depois que isso acontecer, no próximo ciclo de digitalização. O terceiro tipo é mais complexo e caro. Ele inspeciona os dados em movimento na rede, verificando quem está acessando e o contexto (por exemplo, a origem, destino, credencial, localização e sensibilidade dos dados) para bloquear ou permitir o acesso e a alteração. Estão disponíveis várias combinações desses três tipos, oferecendo aos usuários e clientes um vasto número de alternativas.

DATA LEAKAGE/LOSS PREVENTION (DLP)

Observações (cont).

Dos 55 prestadores de serviços avaliados neste estudo, 15 se qualificaram para este quadrante e seis foram nomeados Líderes.

- A **Broadcom** Inc. é uma empresa de hardware e software. Nos últimos anos, fez várias aquisições notáveis. A Symantec é uma dessas aquisições. Atualmente, a Symantec é a principal marca de software de segurança da Broadcom. O conjunto de ferramentas do Symantec Data Loss Prevention fornece DLP. A Broadcom vende seu amplo portfólio de segurança diretamente aos clientes existentes e por meio de um extenso programa de parceiros. Ela possui mais de 80 parceiros no Brasil.
- A **Forcepoint** é uma fornecedora global de soluções de segurança que presta suporte a 14.000 clientes em todo o mundo. As soluções baseadas em comportamento da Forcepoint se adaptam aos riscos em tempo real e são entregues por meio de uma plataforma de segurança convergente. A empresa possui escritórios em São Paulo e seis parceiros no Brasil.
- A **IBM** é um conglomerado global focado em pesquisa de segurança e desenvolvimento de produtos e já entregou mais de 3.000 patentes de segurança. O IBM Security Guardium é um produto projetado para proteger dados críticos; ele oferece proteção de dados, monitoramento de atividades e relatórios de conformidade. A IBM tem anos de experiência no Brasil. Sua organização de serviços profissionais pode oferecer suporte a clientes que usam produtos IBM no Brasil.
- A **McAfee** é dedicada ao software de segurança, possui 1.550 patentes e presta suporte a 69.000 clientes corporativos. É uma das maiores empresas de segurança do mundo. Para DLP, seus produtos incluem McAfee DLP Discover, McAfee DLP Prevent, McAfee DLP Monitor e McAfee DLP Endpoint. No Brasil, ela possui um escritório em São Paulo e 15 parceiros.
- A **OpenText** é uma empresa do Canadá que adquiriu 44 empresas, incluindo a XMedius (2020), Carbonite (2019) e Guidance Software (2017). A empresa fornece gerenciamento de ciclo de vida de documentos, incluindo segurança de conteúdo. Ela possui dois escritórios em São Paulo, 15 parceiros no Brasil e 40 parceiros globais.

DATA LEAKAGE/LOSS PREVENTION (DLP)

Observações (cont).

- A **Trend Micro** possui mais de duas décadas de experiência em terminais em escala global, mensagens e segurança da web. Em 2019, a Trend Micro adquiriu a Cloud Conformity. No mesmo ano, conquistou 3.600 novos clientes no mercado de nuvem híbrida. No Brasil, ela possui quatro escritórios e 140 parceiros.
- A **Varonis** é uma empresa de software que opera em 150 países. Ela se concentra na proteção de dados confidenciais em arquivos e e-mails, como dados confidenciais de clientes, pacientes e funcionários, registros financeiros, e propriedade intelectual. A Varonis possui mais de 7.000 clientes em vários setores. A empresa possui 17 parceiros de tecnologia e 13 parceiros provedores de serviços. A maioria de seus parceiros opera no Brasil, onde possui escritório comercial em São Paulo.

BROADCOM

Visão Geral

A Broadcom Inc. é uma empresa de hardware e software com mais de 18.000 funcionários, com receita de US$ 22,6 bilhões em 2019. Nos últimos anos, adquiriu a Symantec, Brocade e a CA Technologies. A Symantec é sua marca líder em software de segurança. O conjunto de ferramentas do Symantec Data Loss Prevention fornece DLP. A Broadcom vende seu amplo portfólio de segurança diretamente aos clientes existentes e por meio de sua extensa rede de parceiros, sendo 80 no Brasil.

Pontos Fortes

Portfólio robusto: A Broadcom fornece várias ferramentas para cobrir diferentes aspectos da DLP. Os clientes se beneficiam de mais de 70 modelos de políticas pré-criadas e um construtor de políticas conveniente para acelerar a adoção de DLP. Seu DLP inclui dados na nuvem, transferências de arquivos, e-mails, terminais e armazenamento.

Verificando todas as fontes de dados: Os agentes lightweight da Broadcom examinam os discos rígidos em busca de arquivos confidenciais, incluindo servidores, notebooks e desktops. Ele reconhece mais de 330 tipos de arquivos com base na assinatura binária de cada um. As ferramentas de tráfego de rede detectam conteúdo e metadados confidenciais em todos os protocolos com zero perda de pacotes. A monitoração de e-mails e arquivos usa pop-ups ou alertas por e-mail para notificar violações de confidencialidade ou privacidade. Usuários podem justificar as exceções no sistema.

Medidas de proteção flexíveis: Os clientes podem administrar as regras a serem aplicadas. Por exemplo, as opções de e-mails incluem modificar, redirecionar ou bloquear mensagens. Os arquivos com informações confidenciais podem ser movidos para quarentena remota, criptografados ou marcados para administrar direitos digitais. Igualmente, uploads, downloads ou transferências de arquivos para armazenamento portátil, como USB, podem ser criptografados automaticamente com base na identidade. Os controles incluem a interrupção do compartilhamento de arquivos confidenciais, quarentena ou bloqueio de arquivos em mais de 100 aplicativos de nuvem, incluindo Office 365, G-Suite, Box, Dropbox e Salesforce.

Pontos de Atenção

A solução de DLP da Broadcom requer várias ferramentas que trabalham em conjunto. Embora as ferramentas forneçam uma integração robusta, a solução é complexa. Os clientes precisam usar outros produtos Broadcom que vão além da funcionalidade de DLP. Os clientes devem equilibrar sua decisão de compra considerando o design da arquitetura de segurança e a eventual padronização em torno do portfólio da Broadcom.

2020 ISG Provider Lens™ Leader

A Broadcom fornece um portfólio de DLP robusto, cobrindo a maioria dos aspectos de identificação de dados, classificação e proteção de acesso e em conformidade com as melhores práticas e com a LGPD.

FORCEPOINT

Visão Geral

A Forcepoint é uma fornecedora global de soluções de segurança com 2.700 funcionários em 150 países. Sediada em Austin, Texas, EUA, a empresa presta suporte a 14.000 clientes em todo o mundo. As soluções baseadas em comportamento da Forcepoint se adaptam aos riscos em tempo real e são entregues por meio de uma plataforma de segurança convergente. A empresa possui escritórios em São Paulo e seis parceiros no Brasil.

Pontos Fortes

Proteção dinâmica de dados (DDP): A DDP da Forcepoint usa análises centradas no comportamento para detectar anomalias na fonte que acessa dados. Alterações nos níveis de risco, medidos em tempo real, permitem alterações automáticas nas políticas, restringindo o acesso aos dados correspondente. Alertas de comportamento suspeito permitem uma investigação proativa. Sua solução inovadora permite o controle interno, protegendo os dados de insiders (com más intenções) que possuem credenciais válidas, mas mostram uma mudança de comportamento.

Gerenciamento robusto de políticas: A Forcepoint fornece um painel ordenado para gerenciar políticas de acesso a dados em repouso, dados em movimento ou dados em uso em aplicações em nuvem, e-mails, web, terminais ou data centers. Para um início rápido, ela fornece uma ampla biblioteca de políticas predefinidas. Os clientes se beneficiam das melhores práticas que aceleram a conformidade legal. Suas bibliotecas fornecem conformidade para mais de 80 países, incluindo o IBAN brasileiro e as informações privadas brasileiras (PII). A pesquisa e classificação de dados abrange informações financeiras da empresa, segredos comerciais, dados de cartão de crédito, informações de saúde e outros, mesmo em imagens ou formatos como PDF.

Pioneirismo na nuvem: A DLP da Forcepoint é um dos primeiros produtos de DLP a integrar-se ao AWS Security Hub. Ele se integra ao Forcepoint Cloud Access Security Broker (CASB) e ao NGFW (firewall) da Forcepoint, fornecendo visibilidade no local e na nuvem. Para e-mails, ele pode detectar roubo de dados ocultos em imagens ou como arquivos criptografados personalizados, mesmo quando é transmitido gradualmente em pequenas quantidades para evitar a detecção.

Pontos de Atenção

A Forcepoint poderia melhorar sua posição ampliando seu programa de parceiros, que atualmente inclui seis parceiros no Brasil.

A biblioteca de políticas da Forcepoint não inclui disposições relacionadas à LGPD. Os clientes podem usar o GDPR como um guia, mas a conformidade total exigiria consultas e avaliações adicionais.

2020 ISG Provider Lens™ Leader

A Forcepoint tem uma solução pragmática. Sua implementação guiada, aproveitando sua robusta biblioteca de políticas, pode acelerar os programas de conformidade.

IBM

Visão Geral

A IBM é uma empresa global de US$ 77 bilhões. Ela monitora 15 bilhões de eventos de segurança por dia, em mais de 130 países. O foco da empresa em pesquisa de segurança e desenvolvimento de produtos já entregou mais de 3.000 patentes de segurança. O IBM Security Guardium é um produto projetado para proteger dados críticos. Ele oferece proteção de dados, monitoramento de atividades e relatórios de conformidade. A IBM tem muitos anos de experiência no Brasil. Seu braço de serviços profissionais pode fornecer suporte no uso de produtos IBM a seus clientes em todo o Brasil.

Pontos Fortes

Proteção de dados em tempo real: O IBM Guardium monitora os acessos a dados em tempo real para detectar ações não autorizadas em bancos de dados, arquivos, storage, documentos e recursos da nuvem. Sua análise em tempo real captura informações contextuais sobre o usuário, a operação, o ativo e o método usado para acesso. As transações de monitoramento em tempo real, incluindo consultas, fornecem uma trilha de log inviolável. Em resumo, o IBM Guardium Data Protection evita atividades não autorizadas ou suspeitas por parte de privilegiados ou possíveis hackers.

Poderosa descoberta e classificação: O IBM Guardium fornece descoberta de dados, classificação e descoberta de acesso privilegiado em todas as fontes de dados, incluindo a nuvem. Ele emite alertas sobre o acesso com excesso de privilégios para correção. Além disso, monitora o conteúdo dos dados que saem do armazenamento e intercepta e ofusca campos não autorizados automaticamente e de acordo com políticas e privilégios do usuário.

Relatórios analíticos poderosos: A IBM utiliza sua experiência em IA e analytics para fornecer painéis avançados sobre avaliação e conformidade de riscos, com base na ingestão de grandes volumes de dados. As informações do IBM Guardium ajudam a melhorar as políticas de segurança e dados.

Aparelhos de alta capacidade e suporte robusto: A IBM fornece hardware e software de alto desempenho para atender às necessidades de grandes empresas. Sua experiência global permite configurar soluções de DLP para cumprir com a maioria dos regulamentos, incluindo GDPR e LGPD.

Pontos de Atenção

O portfólio da IBM cobre muitos dispositivos e ferramentas e exige que os clientes detalhem o planejamento e a arquitetura para integrar uma solução abrangente. O IBM Guardium foi projetado para alto volume de transações e pode oferecer mais capacidade do que a maioria das organizações precisa. Os clientes devem avaliar cuidadosamente suas reais necessidades antes de adotar a solução.

2020 ISG Provider Lens™ Leader

A IBM oferece uma solução de DLP robusta e altamente escalável, adequada para grandes empresas que operam ambientes de nuvem híbrida e onde os dados são distribuídos em vários locais.

MCAFEE

Visão Geral

A McAfee é dedicada ao software de segurança. Ela possui 1.550 patentes e presta suporte a 69.000 clientes corporativos. Com 7.000 funcionários e 151 parceiros de inovação em segurança em 189 países, é uma das maiores empresas de segurança do mundo. Para DLP, seus produtos incluem McAfee DLP Discover, McAfee DLP Prevent, McAfee DLP Monitor e McAfee DLP Endpoint. No Brasil, a empresa possui um escritório em São Paulo e 15 parceiros.

Pontos Fortes

Conjunto abrangente de ferramentas de DLP: O conjunto de ferramentas de DLP da McAfee abrange todos os aspectos de descoberta e classificação de dados, ofuscação de dados e monitoramento dinâmico de acesso ao comportamento do usuário. A descoberta inclui todos os locais de armazenamento, incluindo a nuvem e oferece correspondência exata de dados com recursos de impressão digital para dados estruturados em bancos de dados e planilhas do Microsoft Excel. A digitalização detecta violações da política; indexa o conteúdo e ajuda a entender como os dados são usados, quem os possui, onde são armazenados e onde proliferaram.

Recursos avançados: O McAfee DLP Prevent for Mobile Email fornece proteção sensível a conteúdo para e-mails móveis, interceptando e-mails para coleta de evidências de conformidade e prevenção de vazamento de dados em dispositivos móveis gerenciados e não gerenciados. O reconhecimento óptico de caracteres (OCR) oferece proteção aprimorada para dados confidenciais ocultos no texto de imagens digitalizadas, formulários e capturas de tela. Modelos de formato de dados privados (dicionários) e consulta de sintaxe regex facilitam a criação de regras de proteção na web e e-mail.

Painel de controle central: O McAfee ePolicy Orchestrator (McAfee ePO™) compartilha políticas de DLP na nuvem, plataformas de colaboração, data centers e terminais. Ele apresenta todas as políticas em um painel central. A solução McAfee DLP fornece uma visibilidade de painel único para aumentar a eficiência dos negócios e reduzir as despesas administrativas.

Pontos de Atenção

A McAfee não fornece quarentena ou criptografia dinâmica de arquivos em caso de acesso a dados.

As ferramentas de DLP da McAfee não oferecem proteção para carregar/baixar e transferir para armazenamento externo, como USB em notebooks ou desktops.

2020 ISG Provider Lens™ Leader

A McAfee fornece a funcionalidade de DLP esperada para resolver as necessidades da maioria das empresas em relação à privacidade, confidencialidade e conformidade regulatória.

OPENTEXT

Visão Geral

A OpenText é uma empresa do Canadá com mais de 12.000 funcionários. Ela começou como um projeto da Universidade de Waterloo para digitalizar o Oxford Dictionary e torná-lo pesquisável (o significado por trás do OpenText). Em 1991, sua tecnologia alimentava o mecanismo de busca Yahoo!. A OpenText adquiriu 44 empresas, incluindo XMedius (2020), oferecendo troca segura de arquivos; Carbonite (2019), oferecendo segurança de terminal e proteção de dados na nuvem; e Guidance Software (2017), oferecendo segurança forense, segurança corporativa e eDiscovery. A OpenText fornece gestão de ciclo de vida de documentos, incluindo segurança de conteúdo. Ela possui dois escritórios em São Paulo, 15 parceiros no Brasil e 40 parceiros globais.

Pontos Fortes

Sem viés de rotulagem: A OpenText usa um sofisticado mecanismo de pesquisa para encontrar e classificar documentos de acordo com os padrões de dados. Usa algoritmos de expressão regular para usos comuns, como o CPF, identidade, carteira de motorista, cartões de crédito e muitos outros da sua biblioteca de referência. Os clientes podem escrever facilmente uma expressão regular para pesquisar em repositórios data lake. O OpenText EnCase Endpoint Investigator fornece investigação em nível forense para determinar fontes de acesso a dados, causas de vazamento e roubo de dados. Ele gera evidências aceitáveis para resolver disputas legais.

Referências robustas de clientes: A OpenText possui uma lista robusta de clientes no Brasil que usam sua solução, incluindo clientes de setores verticais como Óleo e Gás, Mineração e Bancos. Auditores e especialistas forenses usam a OpenText para apoiar suas investigações. Algumas das maiores empresas e órgãos governamentais do mundo dependem da tecnologia da OpenText.

Ativação de conformidade com GDPR e LGPD: A OpenText permite que os clientes eliminem informações obsoletas, conforme exigido pela lei. O OpenText EnCase Risk Manager corrige dados em locais não autorizados por meio de remoção digital, realocação e outras ações de controle, mitigando o risco de perda ou roubo de informações confidenciais.

Pontos de Atenção

A OpenText fornece prevenção de acesso a dados em tempo real através de seus produtos Enterprise Security, mas não com o EnCase Risk Manager. Os clientes devem escolher soluções de IAM para complementar o OpenText DLP se forem necessários controles proativos de acesso a dados confidenciais.

2020 ISG Provider Lens™ Leader

O portfólio de DLP da OpenText fornece uma solução robusta para conformidade com a LGPD. Os clientes podem contar com sua ampla rede de parceiros para uma rápida implementação e suporte.

TREND MICRO

Visão Geral

A Trend Micro tem mais de duas décadas de experiência em terminais em escala global, mensagens e segurança na web. Com 6.000 funcionários em 74 escritórios, ela atende a 500.000 clientes (pessoas físicas e jurídicas). Em 2019, a empresa adquiriu a Cloud Conformity. No mesmo ano, conquistou 3.600 novos clientes no mercado de nuvem híbrida. No Brasil, a Trend Micro possui quatro escritórios e 140 parceiros.

Pontos Fortes

Foco na simplicidade: A Trend Micro reduz a complexidade e o custo da segurança dos dados, integrando a funcionalidade de DLP em suas soluções e consoles de gerenciamento existentes. Um plug-in leve permite visibilidade e controle de dados confidenciais, impedindo a perda de dados por USB, e-mails, aplicações de SaaS, web, dispositivo móvel e armazenamento em nuvem. O plug-in de DLP não requer hardware ou software extra. Ele utiliza modelos regionais e de mercados específicos para simplificar a implantação e cumprir as leis locais. A DLP integrada permite uma DLP eficiente.

Capacidade de P&D: A Trend Micro possui 15 centros de pesquisa e desenvolvimento em todo o mundo; mais de 2.200 pessoas são empregadas na pesquisa e desenvolvimento, das quais 450 são especialistas em segurança, dedicadas a descobrir ameaças avançadas e de dia zero e encontrar soluções rapidamente. A empresa está desenvolvendo seu principal produto, o Smart Protection Network (SPN), para fortalecer seus recursos de IA.

Foco na proteção da carga de trabalho: A Trend Micro protege contra ataques na web e roubos de dados, garantindo dados e reputação seguros e conformidade legal. O Trend Micro Cloud One™ fornece segurança de processamento em uma única solução criada especificamente para imagens de servidor, nuvem e contêiner, fornecendo segurança consistente, independentemente do volume ou tipo de carga de trabalho. A recente aquisição da Cloud Conformity aprimorou seus recursos de gerenciamento de postura de segurança na nuvem (CSPM) para identificar e corrigir automaticamente as configurações incorretas da infraestrutura da nuvem, incluindo serviços em nuvem para armazenamento de arquivos e documentos.

Pontos de Atenção

A integração da solução Trend Micro com outras ferramentas de segurança não beneficia os clientes se eles não tiverem padronizado em Trend Micro.

A Trend Micro controla o acesso e a movimentação dos dados, mas não inspeciona os dados para identificar ou ofuscar dados privados.

2020 ISG Provider Lens™ Leader

A Trend Micro fornece soluções de DLP para mais de 300 tipos de arquivos, rastreando todos os dados em movimento para impedir que eles saiam da empresa cliente.

VARONIS

Visão Geral

A Varonis é uma empresa de software que opera em 150 países. Ela se concentra na proteção de dados confidenciais em arquivos e e-mails, como dados confidenciais de clientes, pacientes e funcionários; registros financeiros e propriedade intelectual. A empresa possui mais de 7.000 clientes em setores verticais, como Tecnologia, Bens de Consumo, Varejo, Serviços Financeiros, Assistência Médica, Manufatura, Energia, Mídia e Educação. Ela opera através de 17 parceiros de tecnologia e 13 parceiros de serviços. A maioria desses parceiros opera no Brasil, onde ela possui um escritório comercial em São Paulo.

Pontos Fortes

Portfólio abrangente: As soluções da Varonis verificam e descobrem dados confidenciais, como números de identidade, informações bancárias e dados confidenciais em arquivos. Ela usa 280 padrões (expressões regulares, RegEx) para identificar e classificar dados elegíveis para GDPR. O uso de palavras-chave, proximidade, palavras-chave negativas e algoritmos de validação exclusivos aumentam sua eficácia. Durante a verificação, ela repara automaticamente os direitos de acesso, aplicando um modelo de menos privilégios e revogando o dos usuários que não precisam mais de acesso.

Abordagem única de conscientização de contexto: A Varonis coleta seis fluxos principais de metadados, a saber: permissões, atividade de acesso, telemetria de AD, telemetria de perímetro, classificação de conteúdo e grupos de usuários. Ao combinar metadados, ela prioriza a classificação de risco com base na sensibilidade, exposição e acesso. O monitoramento contínuo identifica usuários que não precisam mais acessar certos dados e seus proprietários, sugerindo alterações nos métodos de acesso. Ela descobre, classifica e bloqueia automaticamente dados confidenciais, regulamentados e obsoletos, garantindo a conformidade legal.

Prevenção de ransomware: A Varonis Data Security Platform detecta e responde a ameaças. O DatAlert identifica mais de 850 variantes conhecidas e ataques de dia zero com análises sofisticadas de comportamento do usuário. Os modelos preditivos de ameaças sinalizam atividades e comportamentos suspeitos que se assemelham ao ransomware, para acionar respostas automáticas que encerram as contas comprometidas antes de qualquer dano, ou reduzem a magnitude do dano.

Pontos de Atenção

A Varonis não fornece uma lista de parceiros e distribuidores de serviços locais. A empresa poderia ter uma melhor posição no mercado brasileiro se tivesse uma melhor estrutura de pré-vendas e suporte pós-vendas para melhor reconhecimento da sua marca.

2020 ISG Provider Lens™ Leader

O portfólio abrangente da Varonis fornece conformidade e reduz o risco de acesso injustificado a informações e vazamentos de dados.

Metodologia

METODOLOGIA

TÍTULO 2

O estudo de pesquisa "ISG Provider Lens™ Cyber Security - Solutions & Services 2020" analisa os fabricantes de software e prestadores de serviços de relevantes no mercado brasileiro, com base em um processo de pesquisa e análise em várias fases, e posiciona esses fornecedores com base na metodologia ISG Research. O estudo foi dividido nas seguintes etapas:

1. Definição da ISG Provider Lens™ Cyber Security - Solutions & Services, mercado Brasil
2. Uso de pesquisas baseadas em questionário de fabricantes e prestadores de serviços em todos os tópicos de tendências
3. Discussões interativas com prestadores de serviços/fabricasntes sobre recursos e casos de uso
4. Utilização dos bancos de dados internos da ISG e do conhecimento e experiência do consultor (sempre que aplicável)
5. Análise e avaliação detalhadas de serviços e documentação com base nos fatos e números recebidos de fornecedores e outras fontes.
6. Uso dos seguintes critérios-chave de avaliação:
   - Estratégia e visão;
   - Inovação;
   - Reconhecimento da marca e presença no mercado;
   - Cenário de vendas e parceiros;
   - Amplitude e profundidade do portfólio de serviços oferecidos;
   - Avanços tecnológicos.

Autores e Editores

Pedro L. Bicudo Maschio, Autor

Analista de Destaque

Analista e autor de destaque, Pedro Bicudo traz uma vasta experiência em pesquisa dos mercados de serviços do SEMEA (Sul da Europa, Oriente Médio e África) e América Latina. Com mais de 30 anos de experiência em sourcing, ele desenvolveu avaliações de fornecedores, além de programas de reestruturação de contratos, escopo de serviços e benchmarking de TI para diversos mercados verticais nas Américas e APAC. Antes de ingressar na ISG, Pedro foi sócio da TGT Consult e vice-presidente de divisão na Gartner Inc., responsável pelos negócios de consultoria na APAC e na América Latina.

Ron Exler, Analista de Contexto Corporativo e Visão Geral Global

Analista principal, ISG Research

O Sr. Exler é analista principal da ISG Research, com foco nas influências disruptivas e progressivas nos negócios - e nas experiências de seus clientes - do Digital Workplace, da Internet das Coisas (IoT), da Inteligência de Localização e da modernização de aplicativos. Ron cria relatórios de pesquisa em andamento da ISG, fornece contribuições de contexto corporativo para o ISG Provider Lens e lidera outras pesquisas envolvendo transformação digital corporativa. Ron faz a ponte entre negócios e tecnologia através de análises ativas e comunicações claras de problemas e oportunidades.

Autores e Editores

Jan Erik Aase, Editor

Diretor e Analista Principal

O Sr. Aase possui uma vasta experiência na implementação e pesquisa de integração de serviços e gerenciamento de processos de TI e de negócios. Com mais de 35 anos de experiência, ele é altamente qualificado para analisar tendências e metodologias de governança de fornecedores, identificar ineficiências nos processos atuais e assessorar o setor. Jan Erik possui experiência nos quatro lados do ciclo de vida de fornecimento e governança de fornecedores - como cliente, analista do setor, prestador de serviços e consultor. Agora, como diretor de pesquisa, analista principal e chefe global da ISG Provider Lens™, ele está muito bem posicionado para avaliar e relatar o estado da indústria e fazer recomendações para empresas e clientes de provedores de serviços.

ISG Provider Lens™ | Quadrant Report
Agosto 2020

ISG (Information Services Group) (NASDAQ: III) é uma empresa global líder em consultoria e pesquisa de tecnologia. Uma parceira de negócios confiável para mais de 700 clientes, incluindo 75 das maiores 100 empresas do mundo, a ISG é comprometida em ajudar corporações, organizações do setor público e fornecedores de serviços e de tecnologia a alcançar a excelência operacional e crescimento mais rápido. A empresa se especializa em serviços de transformação digital, incluindo serviços de automação, análises de dados e nuvem; consultoria de fornecimento; governança gerenciada e de risco; serviços de fornecimento de rede; estratégia de tecnologia e design de operações; gerenciamento de mudança; inteligência de mercado, pesquisa e análise de tecnologia. Fundada em 2006, com base em Stamford, Conn., a ISG emprega mais de 1.300 profissionais, operando em mais de 20 países – uma equipe global conhecida por seu pensamento inovador, influência no mercado, expertise profunda em indústria e tecnologia, capacidades analíticas e de pesquisa de qualidade internacional com base nos dados de mercado mais abrangentes da indústria.