ALERTA SECURITY

FORTIFYDATA

Você sabe o quão difícil é medir a performance de cibersegurança das suas equipes operacionais. Mostrar de uma forma tangível os progressos atingidos e as metas que só podem ser concretizadas com os necessários investimentos é um desafio constante.

A plataforma FortifyData permite que você tenha uma leitura contínua de todas as vulnerabilidades encontradas na sua superfície de ataque, com recursos de cálculo financeiro demonstrando o ROI do investimento necessário e gerindo de forma mais eficaz o orçamento.

ALERTA SECURITY

FortifyData é uma Plataforma Automatizada de Monitorização e Gestão de Riscos Cibernéticos

- Fundada por Especialistas de CyberSegurança
- Com sede em Atlanta, GA e com certificação MBE
- Oportunidade de preencher uma lacuna no mercado com uma plataforma que utiliza dados diretos para uma representação exata dos riscos cibernéticos.
- Finalista dos SC Awards 2022 para Melhor Solução de Gestão de Riscos

ALERTA SECURITY

Razões que tornam Fortifydata única

As empresas que enfrentam hoje os riscos cibernéticos exigem avaliações ao vivo e dados priorizados para obterem melhores resultados

1. Avaliações ativas;
2. Todos as portas, todos os serviços para cada IP de um ativo serão analisadas;
3. Algoritmo próprio que dá prioridade aos riscos e vulnerabilidades de acordo com a sua criticidade;
4. Modelação de risco personalizada para aderir melhor à realidade de negócio de cada empresa;
5. Dados de Threat Intel de ameaças integrados e relacionados com descobertas de ativos específicos
6. Receber resultados de risco contextualizados e conscientes do risco

ALERTA SECURITY

Como é feito?

Monitorização da superfície de Ataque

- FortifyData escaneia ativamente toda a sua superfície de ataque
- Ativos expostos ao exterior
- Ativos internos
- Infra-estrutura shadow
- Cadeia de fornecimento / terceiros
- Detectar automaticamente ativos expostos à Internet.

Como?

- FortifyData procura continuamente novos ativos, conhecidos e desconhecidos, numa base seminal expostos à Internet.
- Outras soluções podem demorar até 4 meses a actualizar novos activos

Pesquisa contínuamente activos expostos na Internet

- Identifica as vulnerabilidades exploráveis para cada ativo.
- O cliente pode atribuir a prioridade de acordo com a criticidade de cada ativo
- Resulta num plano de remediação priorizado

Analisa todas as portas (65536) e serviços de cada activo

O resultado

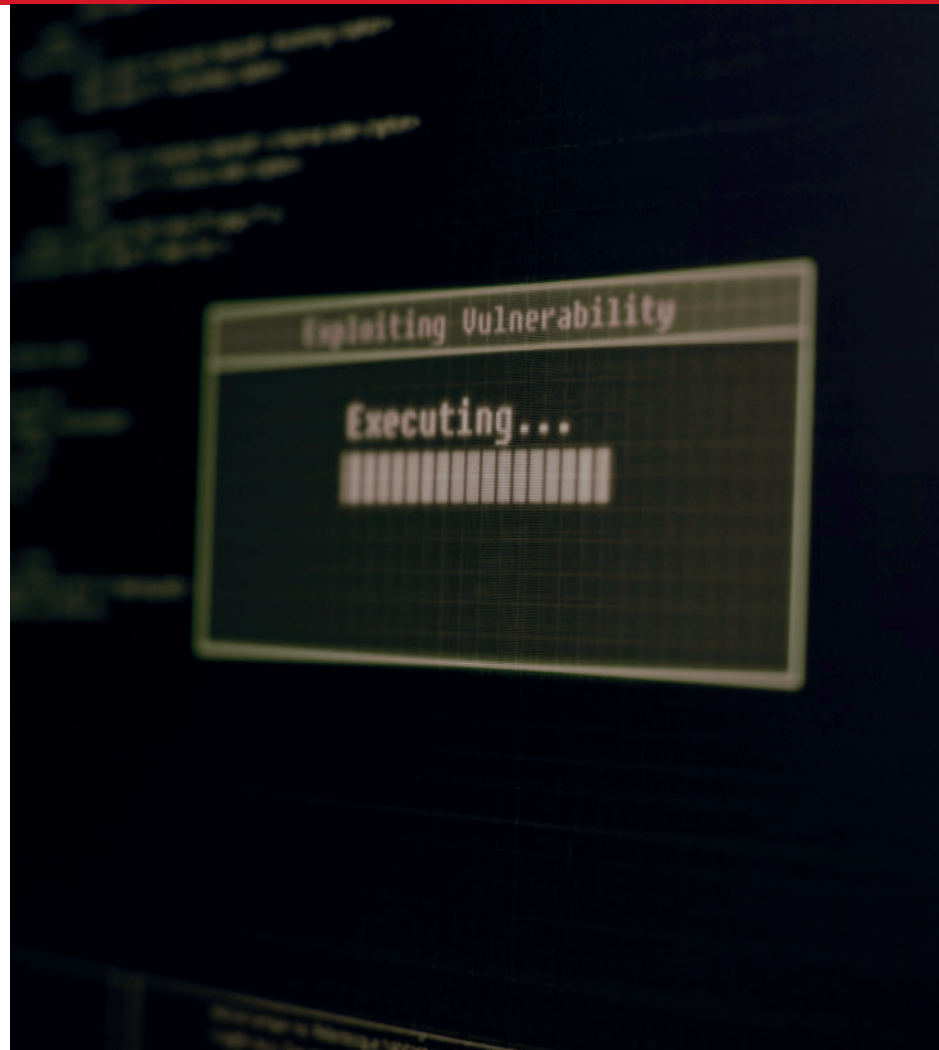
- Ameaças Classificadas e priorizadas;
- Classificação de Segurança Baseada na Avaliação Semanal;
- Identificar as Credenciais da Empresa na Dark e Deep Web
- Qualquer Sistema Comprometido ou Desprotegido

Ameaças classificadas e priorizadas

Ameaças classificadas e priorizadas

As ameaças são apresentadas de acordo com os CVSS scores, ou seja, com o potencial impacto e a probabilidade de ocorrência do mesmo.

O valor agregado é dar prioridade a todas as suas atividades de mitigação de riscos, fornecendo informações atualizadas sobre como os hackers podem explorar a sua rede e os seus ativos e quais os pontos que devem ser remediados primeiro.



Um score de Risco mais preciso e representativo da realidade do seu negócio.

- Fortify Score é baseado em dados de avaliação do seu ambiente;
- Recebe uma pontuação de risco cibernético baseada em avaliações semanais;
- Remediações imediatas com actualizações da pontuação imediatas;
- Compare a sua pontuação com a performance media da sua indústria

ALERTA SECURITY

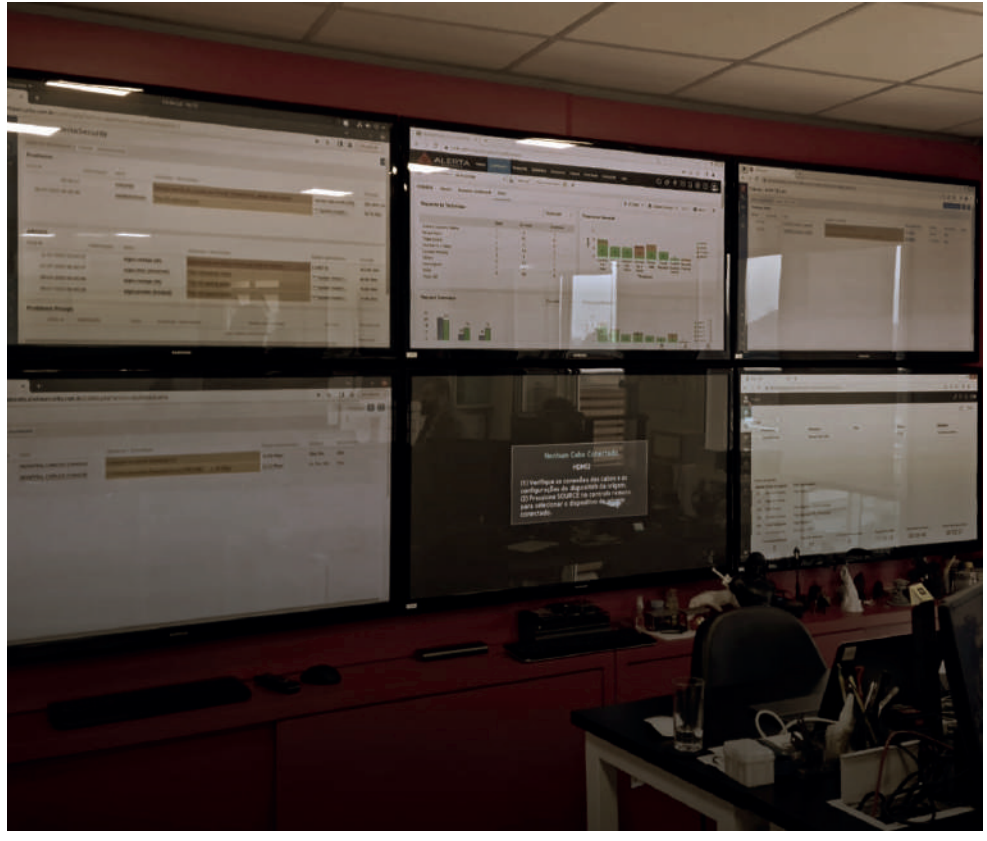
Informação da Dark e Deep Web

Identificar credenciais e senhas vazadas na Dark e deep web:

- Registos / Dados de clientes
- Emails corporativos
- Passwords da empresa

Encontrar sistemas comprometidos

- Lista dos ativos comprometidos e origem do problema;
- Software malicioso em ativos da empresa
- Servidores C2 e botnets



Portfólio de produtos da FortifyData

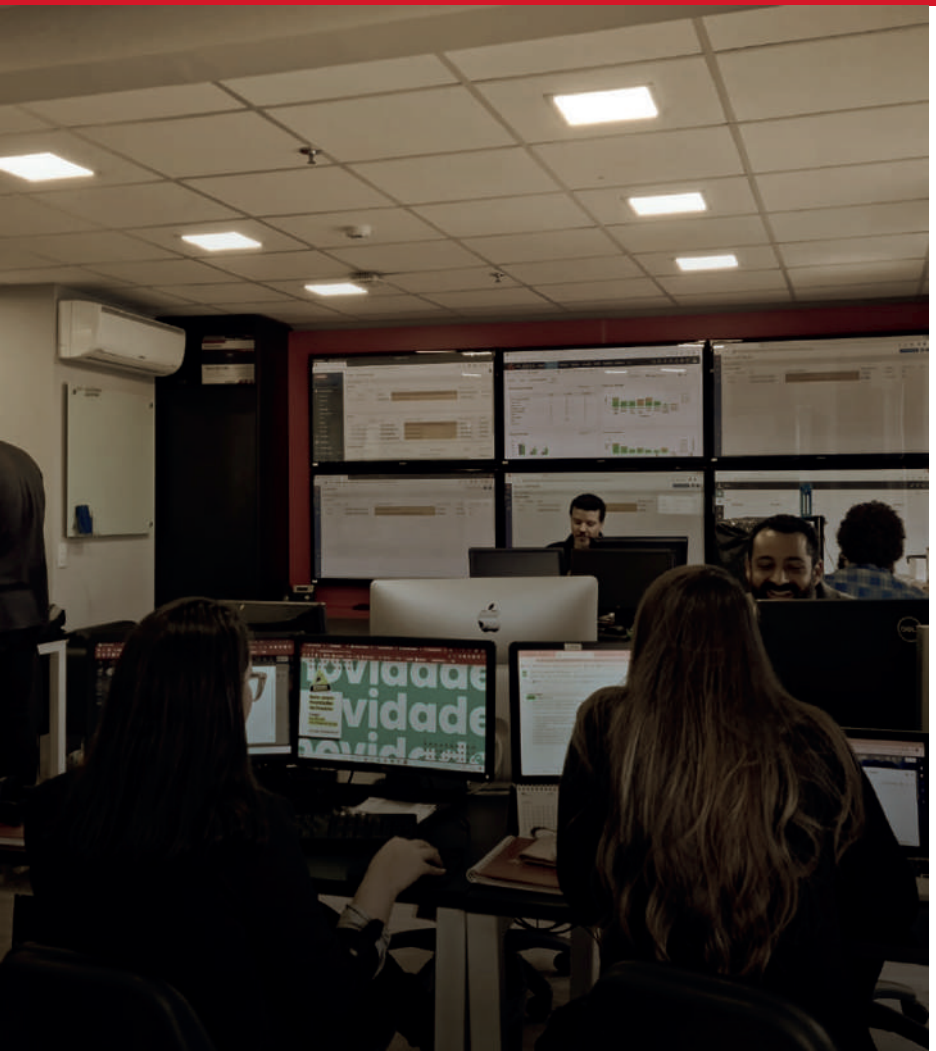
Monitorização da Superfície de Ataque – Duas famílias de produtos

Monitorização da Superfície própria/ativos externos

- Todas as avaliações de portas e protocolos
- Frequência de avaliação completa a cada 7 dias
- Modelação de Pontuação de Risco Empresarial
- Remediação da equipa colaborativa

Monitorização da superfície de ataque em Terceiros

- Compreender como terceiros afetam o seu risco
- Modelação de risco personalizada disponível para terceiros
- Frequência de avaliação completa < 30 dias
- Pontuação da exposição ao risco com base na superfície de ataque externa



Monitorização de risco – Superfície Imediata

• Visibilidade - Veja o que os hackers podem ver da sua organização e prepare-se!

• Contínuo - Atualizações de 7 em 7 dias porque em TI as coisas podem mudar muito rapidamente

• Priorização - tarefas de remediação priorizadas com base no nível de criticidade de cada activo

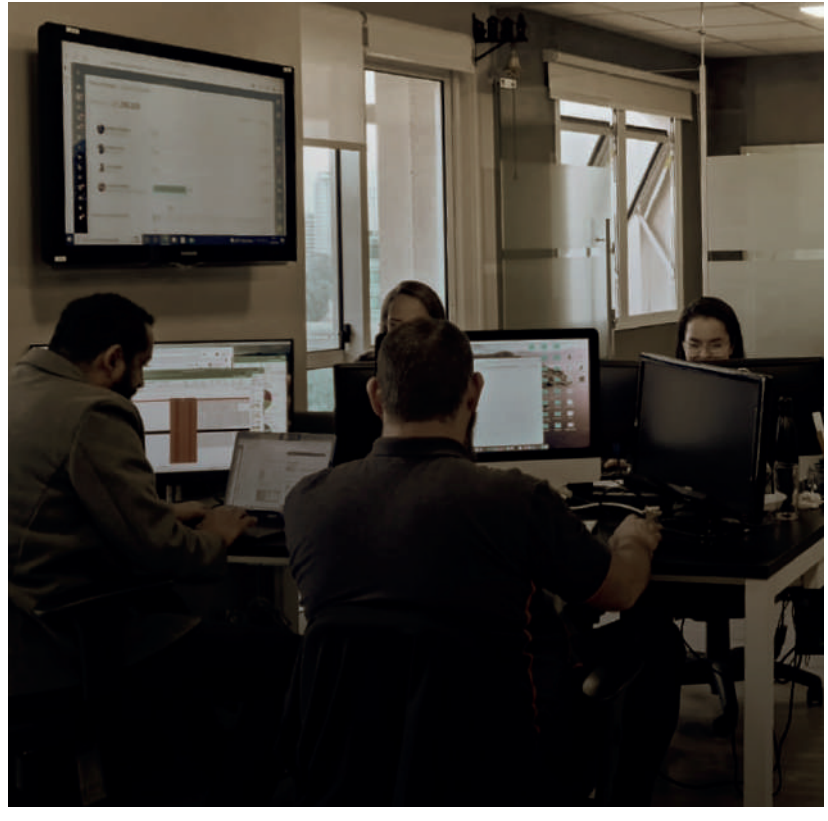
• Conformidade - Verifique a conformidade da sua infra-estrutura com várias normas

• Inventariação de activos externos. Tenha informações atualizadas sobre o inventário dos seus activos expostos ao exterior

Monitorização dos riscos internos

Verificar regularmente os bens e dispositivos internos:

- Ameaças à segurança interna
- Acesso não autorizado
- Requisitos de conformidade com normas ISO
- Má configuração dos seus dispositivos internos



Monitorização da Cloud

- Identificar falhas de segurança, vulnerabilidades e problemas de má configuração, receber recomendações de Hardenning para AWS, Azure, Google Cloud ou Oracle Cloud
- Armazenamento de dados não criptografados
- Falta de políticas de privilégios mínimos
- Políticas de senha insatisfatórias ou falta de FMA
- Cópias de segurança e restauro mal configuradas
- Exposição de dados e escalada de privilégios
- Monitorize a sua Cloud para o não cumprimento dos requisitos PCI, HIPAA
- Ter acesso à base de conhecimentos para atenuar rapidamente os problemas no AWS, Azure, Google Cloud ou Oracle Cloud

Gestão de risco de terceiros

Porque é importante a Gestão de Riscos de Terceiros?

O risco cibernético de terceiros é agora o Risco Cibernético Empresarial

As empresas dependem de uma rede de relações interligadas (APIs, partilha de dados, acesso ao portal, etc.)

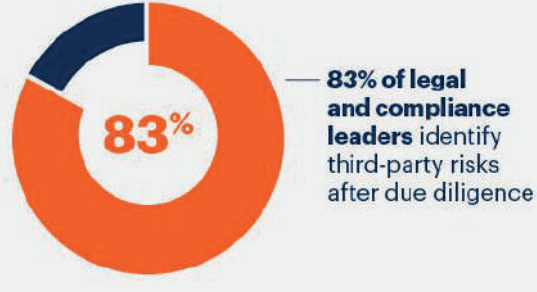
Os seus riscos dos seus vendors, são os seus riscos

55%

"Forrester data reveals that 55% of security pros reported their organization experienced an incident or breach involving supply chain or a third-party provider in the past 12 months,"

Source: Predictions 2022: Cybersecurity, Risk and Privacy, Forrester Research, Inc., Oct. 28, 2021

FORRESTER®

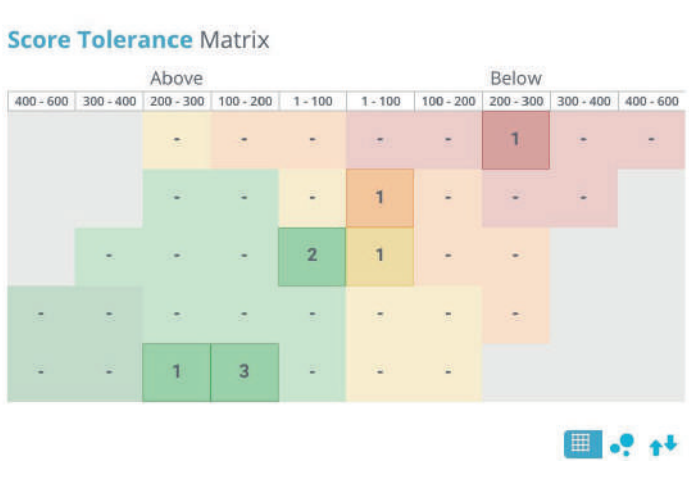


Gartner.

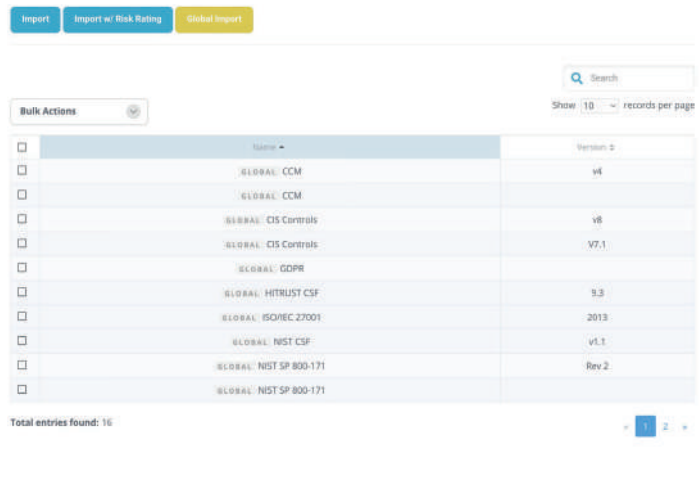
Gestão de risco de terceiros

Dois componentes importantes para abordar a Gestão de Risco de Terceiros

1. Superfície de ataque externo - visibilidade contínua do risco cibernético
2. Questionários - Acabaram-se as folhas de cálculo; auto-validação técnica



Verifique continuamente os seus Vendors críticos para Cyber-Risk

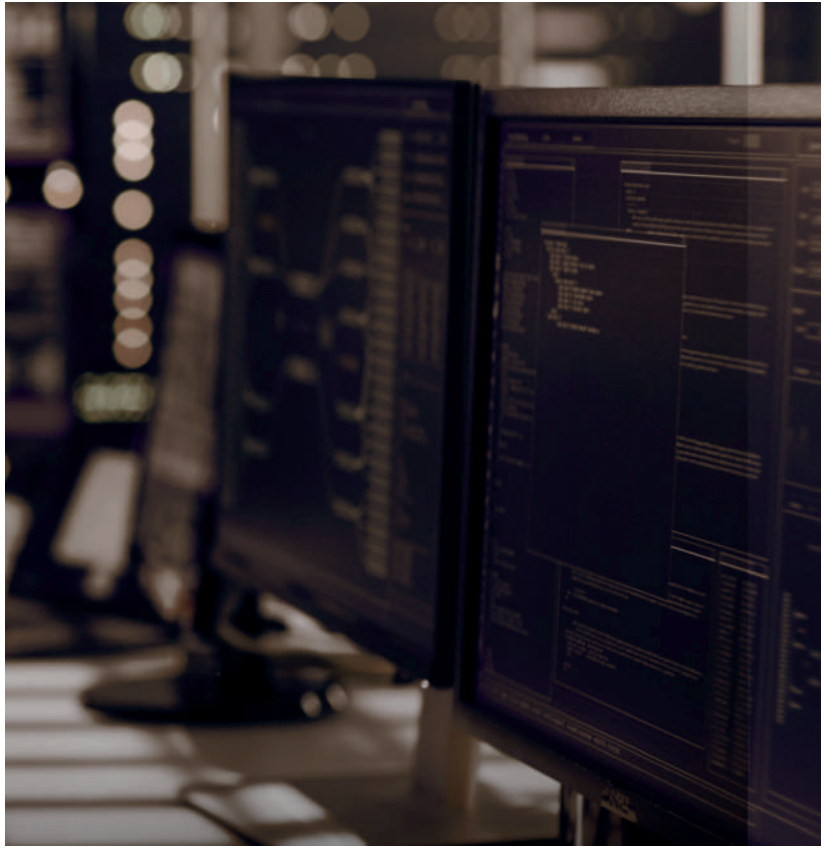


Due diligence – Enviar Questionários e deixar as folhas de cálculo para trás

Gestão de risco de terceiros – Auto-validação de Questionários

O envio de questionários e a plataforma valida automaticamente os componentes técnicos com base nas avaliações, poupando tempo no processo de revisão.

Globalmente, estima-se uma redução de 40% no tempo gasto pelo pessoal utilizando uma ferramenta automatizada de gestão do questionário, em comparação com a revisão manual da folha de cálculo.

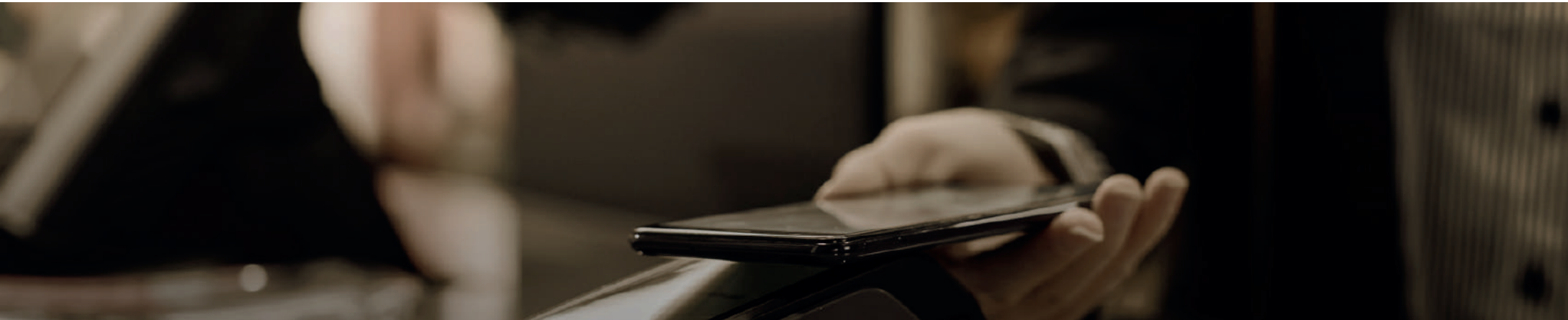


Gestão de risco de terceiros Ferramentas de colaboração

- Pode partilhar gratuitamente as descobertas dos seus vendors críticos com eles.
- Monitorize o seu progresso para conformidade com o seu programa TPRM e/ou com normas ISO entre outras(PCI, NIST, CSA, etc.)
- Criar e rastrear tarefas para os seus vendors mitigarem os riscos verificados
- Validar os seus esforços de remediação e ver atualizações da pontuação de referência quando implementadas
- Todas as interações serão registadas na plataforma para efeitos de responsabilidade futura.

Casos prácticos

- Gestão Cibernética de Riscos Empresariais
- Gestão de Superfícies de Ataque
- Inventário de bens
- Riscos Cibernéticos Internos
- Gestão da Vulnerabilidade
- Risco de segurança da aplicação
- Gestão da Postura de Segurança na Nuvem
- Classificação de Segurança
- Cyber Risk Quantification / Análise de Impacto Financeiro
- Integrando / Combinando Inteligência de Risco
- Gestão dos riscos da cadeia de fornecimento
- Gestão de Riscos Cibernéticos de Terceiros
- Gestão do Questionário
- M&A Due Diligence



Há concorrência?

ALERTA SECURITY

	Attack Surface Management		Security Ratings
	FORTIFYDATA		
	Enterprise Attack Surface Management	Third-Party Attack Surface Management	Security Ratings Reputational Risk
Live Data Assessment	✔	✔	✘ OSINT - historical leased data feeds, ✘ 30-120 days late on arrival
Complete Assessment – All Ports and Services	✔	✔	✘ < 20% Attack Surface
Findings Transparency & Context	✔	✔	✘ No Asset Representation
Data Accuracy	✔	✔	✘ IP Misattributions leading to false positives
Auto-Asset Discovery	✔	✔	✘ Up to 4 months to update and discover new assets
Customizable & Representative Scoring	✔	✔	✘ One Rigid Scoring Model, Inaccurate risk representation

ALERTA SECURITY

	FORTIFYDATA	EASM Competitors
Public Facing Discovery	✔	✔
External Attack Surface Management	✔	✔
Integrated Internal Attack Surface Management	✔	X
Internal Network Asset Discovery	✔	Limited
Customizable Data and Asset Classification (Internal and External)	✔	X
Assessment Frequency	Weekly	≥ Bi-Weekly
Total Risk Management and Reporting	✔	X
Cyber Threat Intelligence	✔	X
Cloud Security Posture Management	✔	X
3rd and 4th Party Attack Surface Management	✔	X
Task Management and Worfklows	✔	X
Compliance Questionnaire Validation	✔	X

ALERTA SECURITY

A La Carte or All-In-One	FORTIFYDATA	BITSIGHT	SecurityScorecard	riskrecon mastercard
Cyber Risk Scoring	✔	✔	✔	✔
Day One Attack Surface Data	✔	30-120 Days Old	30-120 Days Old	30-120 Days Old
Automated Asset Discovery	✔			
Customizable Scoring	✔			Limited
Internal Assessment	✔			
Questionnaire Management	✔	✔	✔	✔
Auto - Validation	✔			
Compliance Management	✔	Manual - Limited		
Cloud Assessment	✔			
ALE / Risk Register	✔	Partnered Add On		

Dúvidas?

Para mais informações acesse:

www.alertasecurity.com.br

comercial@alertasecurity.com.br