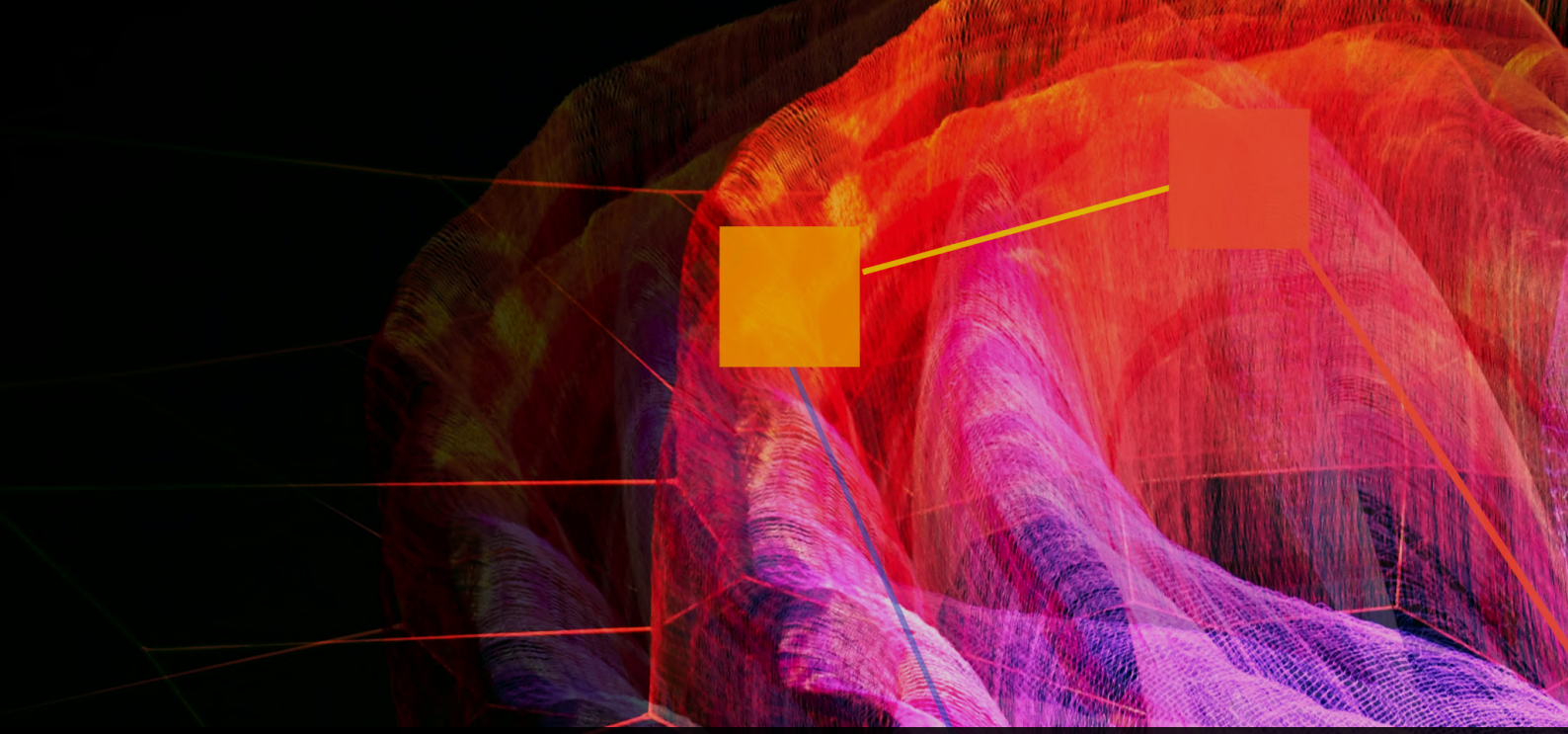


# AUTOMAÇÃO E ORQUESTRAÇÃO

## NA ERA DA TRANSFORMAÇÃO DIGITAL

HIGHLIGHTS

FORTINET VARONIS oramix EXPERT SERVICES

**Oramix | Sistemas de Informação**

www.oramix.pt

MARÇO 2020

# ÍNDICE

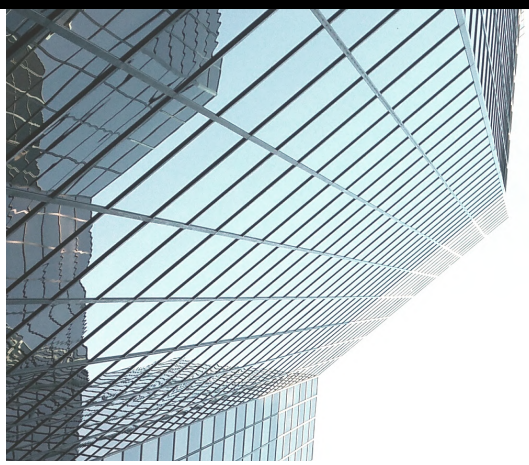


O presente eBook foi desenvolvido no seguimento do evento "Automação e Orquestração na era da Transformação Digital", realizado no Porto e promovido pela Oramix - Expert Services conjuntamente com os seus parceiros de cibersegurança Fortinet e Varonis.

O respectivo conteúdo tem como base as apresentações das soluções apresentadas e outros conteúdos externos dos parceiros, indicados pela respectiva fonte.

*visão do panorama de segurança*

# ONDE ESTAMOS AGORA



### Evolução da cibersegurança

No fundo, o conceito de Transformação Digital que tanto ouvimos falar vem da transformação dos modelos de entrega de produtos/serviços como resposta ao novos requisitos de velocidade, proximidade, inovação e CX (customer experience), através de tecnologias emergentes como o IoT, Big Data, Machine Learning, Cloud, Mobile, 5G, etc.

Estas tecnologias reinventam a forma como as organizações trabalham e interagem com os seus stakholders (externalfacing). Muitos dos dispositivos, hoje adotados e integrados, estendem-se desde produtos de consumo até aos sistemas de infraestrutura críticos das organizações numa comunicação em ciclo interna-externa.

Esta realidade resulta da complexidade das infraestrutura das organizações e da gestão analítica dos componentes que a constituem e, por consequência, na maior exposição aos riscos de cibersegurança.

### O que muda na segurança?

Os negócios necessitam, mais do que nunca, de ser seguros. Ser seguros de fora para dentro - na proteçao do perímetro e rede; e, com crescente importância, de dentro para fora - no que diz respeito ao armazenamento, transporte e uso dos dados - quer por imposição de regulamentos como RGPD, quer como garantia de confiança para com os seus stakeholders, quanto à sua privacidade e proteção da sua informação.

### Quais os principas desafios?

Logo à partida conseguimos levantar diversos desafios:

Um endereçado à capacidade de **respostas ágeis na operação diária** da segurança, como a criação de regras e a automatização de defesas;

Outro, como a **definição de processos** internos sobre as quais essas regras e automatizações possam atuar;

Outro, como a **prevenção de fuga, roubo ou alteração de dados** produtivos e/ou com informação privada;

Outro ainda, a implementação de uma **visão cooperativa** dentro das organizações, sendo que as ameaças, riscos e outras questões de segurança deverão ser hoje preocupação conjunta tanto dos gestores de negócio como dos departamentos técnicos.

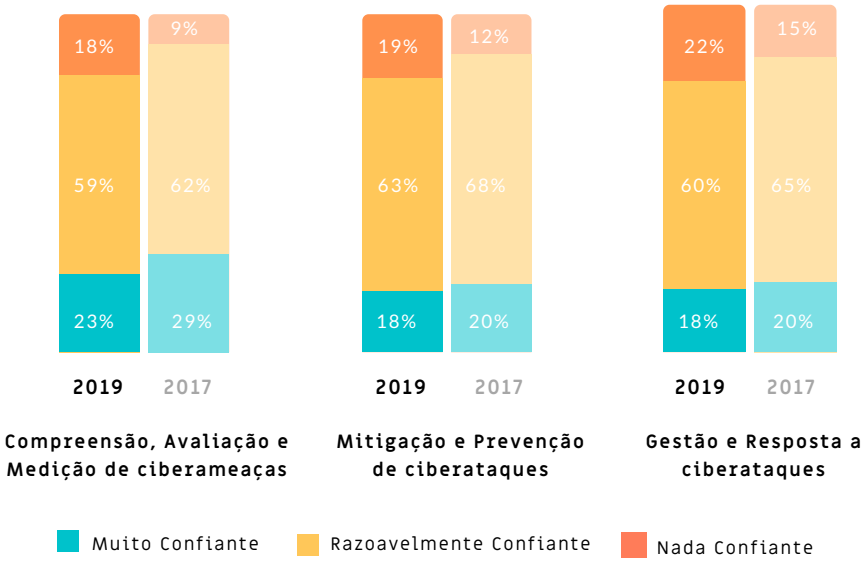
# NÚMEROS QUE FALAM POR SI

*menos*

**30%** de custos operacionais

*ao combinar tecnologias de hiperautomação com processos operacionais redesenhados*

Fonte: Gartner's IT Automation Predictions for 2020, IT Automation Without Boundaries




Fonte: 2019 Global Cyber Risk Perception Survey, Marsh, Microsoft. "Confidence in cyber resilience measures slipped from 2017 to 2019.", pag.6.. (2017: n=1312; 2019: n=1457),

**O risco de cibersegurança é cada vez mais uma prioridade nas organizações, no entanto a confiança nas diferentes medidas de ciber-resiliência está a diminuir.**

Salienta-se a falta de confiança das organizações na capacidade de gerir e prevenir o risco e as ameaças cibernéticas reflecte alguma disparidade.

O declínio de confiança é mais acentuado na área de compreensão, avaliação e medição dos riscos de cibersegurança, nomeadamente no que toca à probabilidade e impacto da exposição dos dados na operacionalização das organizações.

Os dados salientam ainda o gap de confiança na **prevenção e mitigação de ciber-ataques e seus potenciais danos**; e na **gestão de resposta e de recursos** disponíveis na minimização dos impactos e recuperação de incidentes.

*Os dados resultaram do estudo desenvolvido pela Marsh e pela Microsoft, em 2019, sobre a percepção de ciber risco global.*

# COMO RESPONDER

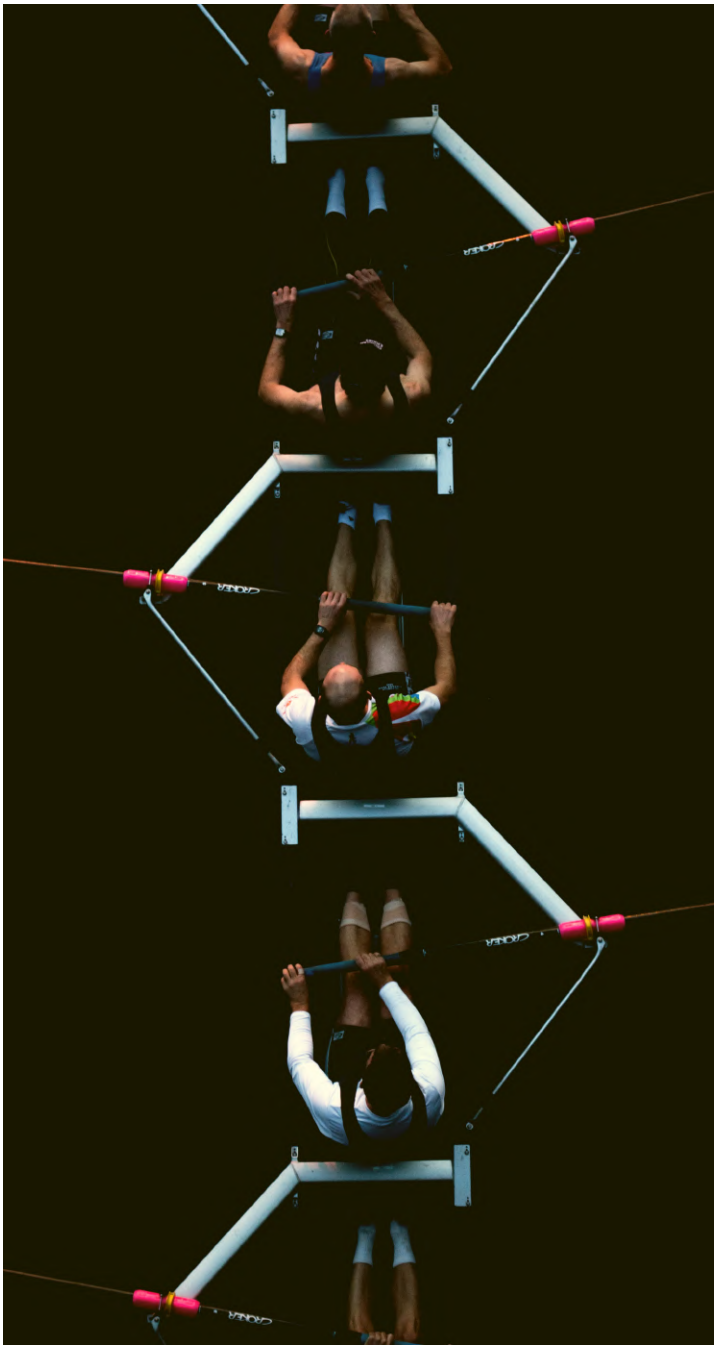
*aos desafios de cibersegurança?*

Com respostas rápidas e estruturadas a questões do dia-a-dia, de forma a podermos assegurar tempos de resposta mais curtos em caso de incidentes. Através da automação e orquestração.

Através uma correta governação e proteção dos dados em todo o seu ciclo de vida: quem acede, onde estão, contêm informação confidencial, são consumidos abusivamente?

## AS FERRAMENTAS DE AUTOMAÇÃO E ORQUESTRAÇÃO

- Mantém ligações entre segurança e ferramentas de análise, como a Fortinet Security Fabric ou a plataforma de segurança de dados Varonis.
- Orquestram processos através da entrega constante de investigação e resposta.
- Guiam e “educam” os analistas através de uma análise step by step / fornecendo os passos seguintes para análise.
- Simplificam operações através de uma interface gráfica user-friendly (GUI).
- Facilitam respostas automáticas, identificando políticas, que bloqueiam ataques.
- Fornecem relatórios de eficácia e produtividade do SOC.



*Automação e orquestração na*

# SEGURANÇA E PROTEÇÃO DA REDE

**"Imaginando que queremos proteger o nosso Rei, começamos por introduzir o perímetro e em seguida o fato protetor do Rei e a sua guarda pessoal."**

Daniel Ferreira, Regional Sales Manager, Fortinet

A proliferação de novas aplicações, dispositivos e de ambientes conectados levam ao incremento de serviços e micro-serviços publicados e, assim, ao **aumento da superfície de ataque**, tornando mais difícil a proteção das redes, sistemas e aplicações que uma **solução de perímetro standard não pode defender.**

**Hoje, muitas vezes, são os cibercriminosos que têm a vantagem da visibilidade.** As organizações necessitam assim de visibilidade durante e depois de um ataque. Esta necessidade torna-se indispensável para protegerem-se de forma eficaz – avaliando riscos, detetando ameaças, protegendo ativos ou respondendo a ataques.

Da mesma forma que os dados precisam de ser protegidos, a segurança deve ser repensada e redesenhada para tentar acompanhar a transformação digital e os ambientes dinâmicos de hoje em dia.

**"Cada dispositivo conectado e cada aplicação, deve ser constantemente monitorizado."**

Carlos Caldeira, Cybersecurity Manager, Oramix

oramix EXPERT SERVICES | FORTINET

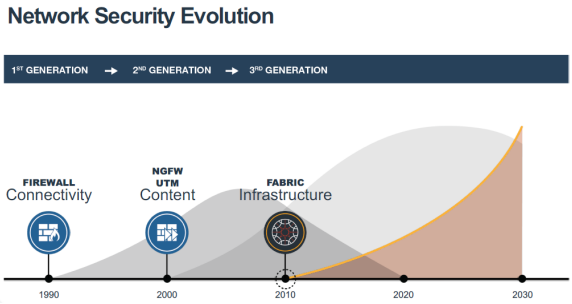
**parceiros de cibersegurança na componente Proteção de Perímetro e Conteúdos**

# FORTINET SECURITY FABRIC

*nova geração de segurança da rede*

Em sequência do panorama atual da expansão da superfície de ataque, hoje mais complexa e vulnerável, provoca a necessidade de uma **Segurança de Redes de 3ª geração** que nos simplifique e nos dê confiança na nossa experiência operacional diária.

O **Fortinet Security Fabric** é a solução que dá resposta a este mundo hiperconectado, proporcionando uma arquitectura inteligente de segurança, que centraliza e integra outras ferramentas e nos auxiliam na deteção, monitorização, bloqueio e resolução de eventos em qualquer lugar da rede numa só plataforma, em tempo real.




Fonte: Next-Generation Firewall Test (2019), Fortinet.

**9** Nss Labs recomendações

*Nova Geração de Firewalls recomendada pela 6ª vez consecutiva*

**99%**

*Eficácia de taxa de bloqueio*

***2020 Gartner Peer Insights Customers' Choice***

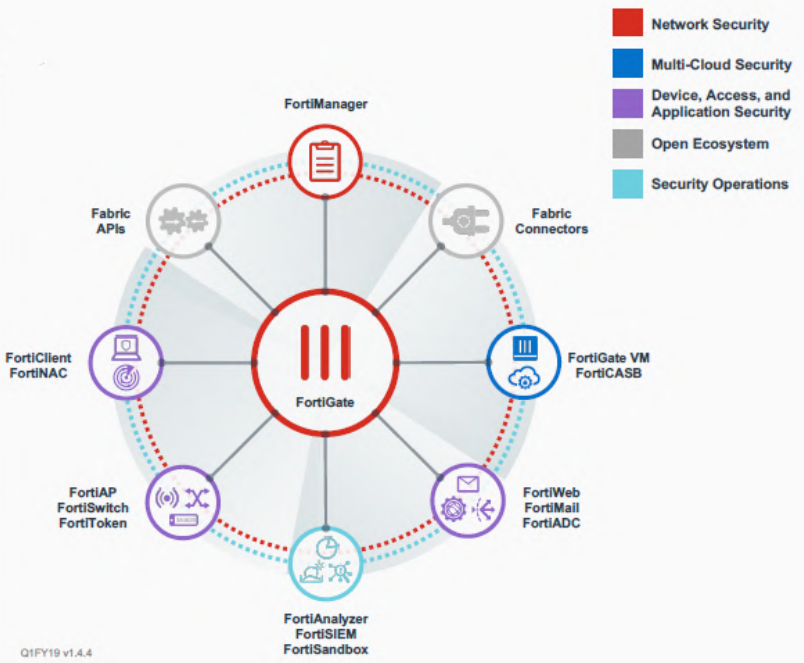
*para Network Firewalls*

Fonte: Fortinet Named a 2020 Gartner Peer Insights Customers' Choice for Network Firewalls, Fortinet.

**Amplitude** → Visibilidade de total da superfície digital

**Integração** → Prevenção, por meio de AI, entre todos os dispositivos, redes e aplicações

**Automatização** → Simplificação da operacionalização, orquestração e resposta




Pedir Demo

# PLATAFORMA SECURITY FABRIC

Estamos dentro do Security Fabric. Aqui, temos acesso a toda a informação e conseguimos chegar a qualquer lado.

### Informação em tempo real, num só lugar

A sua operacionalização torna-se simplificada e mais intuitiva, através do dashboard iterativo, que nos permite visualizar e controlar a informação de toda a rede em tempo real, a partir de um só lugar.

### Conseguimos visualizar a sua composição

(Exemplo)

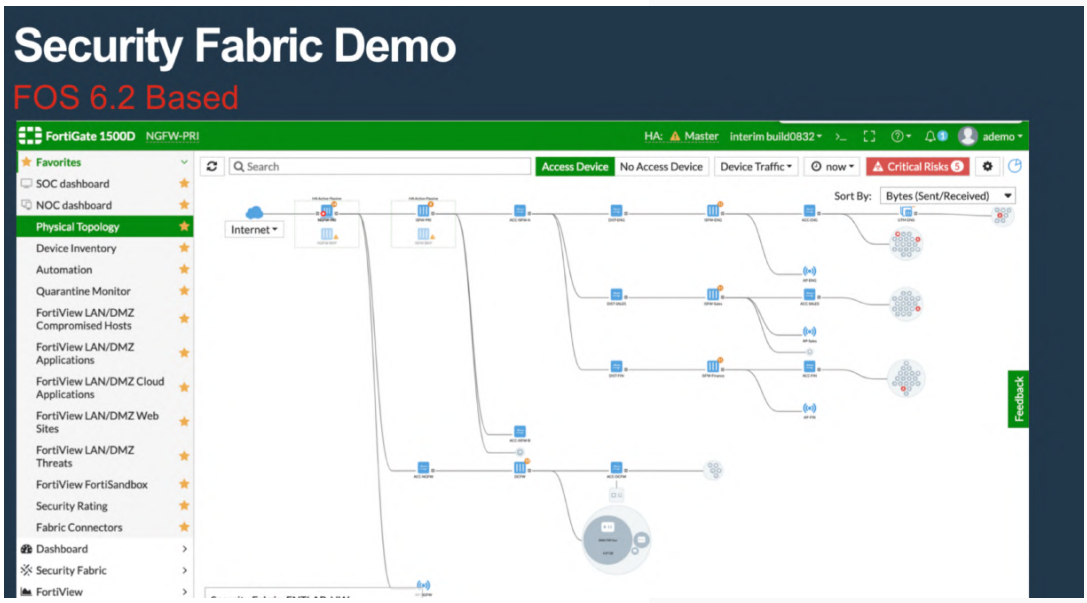
- 1 FortiGate
- 1 Firewall
- 1 concentrador de logs (FortiAnalyzer)
- 1 Sandbox (FortiSandbox)
- 1 Switch (FortiSwitch)
- 2 Access Points (FortiAP)

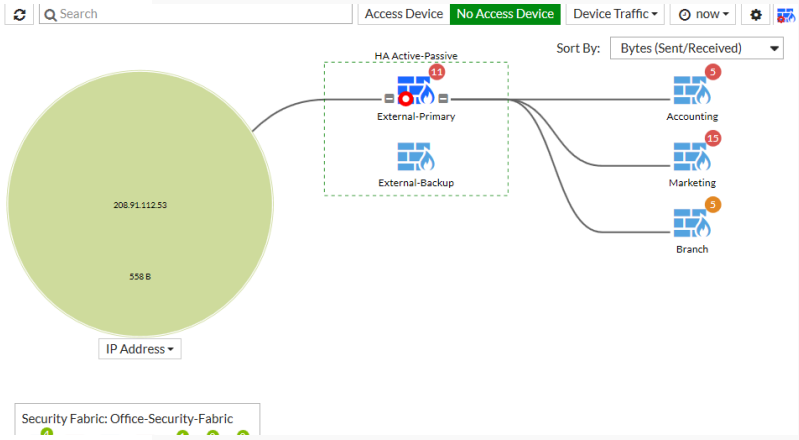
### Personalize o dashboards, adicionando ou removendo funcionalidades

A interface do Security Fabric permite ainda adicionar, mover e remover widgets de funcionalidades:

- Estado de segurança dos diferentes componentes,
- Relatórios do estado de segurança de indústria e dentro da região,
- Largura de banda a decorrer num determinado interface,
- etc.

### Veja como funciona




Pedir Demo

Fonte: Fortinet Help: FortiView Physical and Logical Topology pages, Fortinet.

*Automação e orquestração no*

# GOVERNO, CLASSIFICAÇÃO E PROTEÇÃO DOS DADOS

Aos dias de hoje, e enquanto executivos de gestão e profissionais responsáveis pela integridade, funcionamento e segurança das infraestruturas das organizações, não nos basta a proteção do perímetro confiando que o perigo não irá penetrar.

É sabido que os dados são cada vez mais o ponto fulcral do negócio, na criação de valor. Seja em qual for o sector de actividade, é exigida segurança em todo o ciclo de vida dos dados, onde quer que estes circulem ou se encontrem alojados.

A simples identificação, classificação e monitorização dos dados sensíveis em tempo real, é o ponto de partida fundamental na proteção e bloqueio da fuga de informação confidencial e na garantia das exigências de conformidade regulamentares.

A partir da abordagem focada nos dados, as organizações conseguem obter um melhor conhecimento sobre eles (quais os dados, quando e onde são acedidos, por quem e qual o comportamento dos utilizadores), e assim uma melhor e mais profunda proteção dos mesmos.

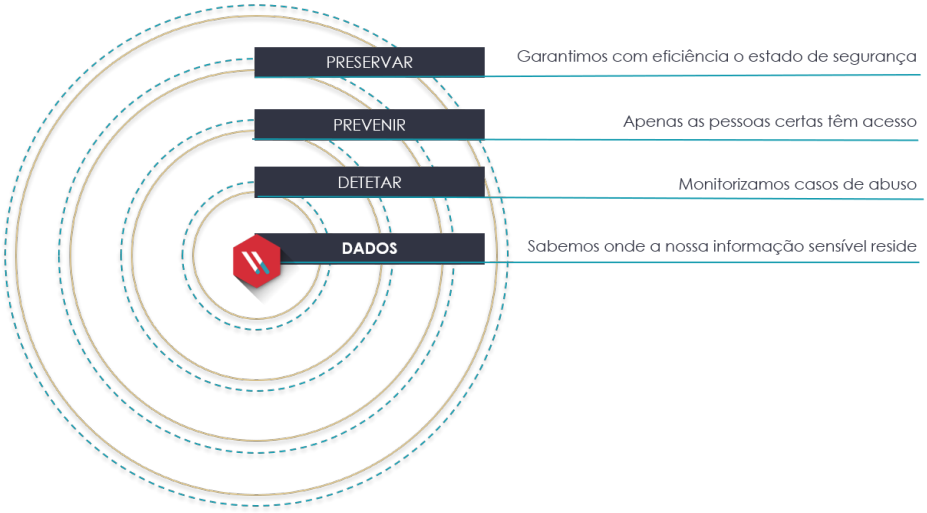
**"A proteção dos dados deve ser prioridade, pelo que todos os contextos onde são usados, transportados e mantidos devem ser contemplados"**

Carlos Caldeira, Cybersecurity Manager, Oramix


oramix EXPERT SERVICES | VARONIS

**parceiros de cibersegurança na componente Proteção e Classificação de Dados**

# VARONIS: SEGURANÇA CENTRADA NOS DADOS




Pioneira na segurança global e centrada nos dados, a Varonis reúne comportamento, governo, conformidade, classificação de dados e analytics numa única solução.

Varonis proporciona uma monitorização e proteção integrada dos dados dentro das organizações, desde a deteção de ameaças internas e externas à rápida resposta, mantendo um estado de segurança contínuo sem esforço manual.

Esteja confiante no compliance do seu negócio! Irá ter visibilidade detalhada da informação necessária à priorização dos riscos e à comprovação de compliance. A partir da avaliação de risco automatizada irá diagnosticar e responder a uma infinidade de questões nos três casos de uso: **Proteção de dados, Compliance e Deteção e Resposta a ameaças.**

**"Não sabemos quem irá atacar ou que exploits irão usar, mas sabemos o que os atacantes querem - os seus dados. Varonis é diferente porque começamos na securização e visibilidade dos dados."**

Varonis

***More five star reviews than any other File Analysis or UEBA solution***

Gartner peerinsights

**+339 milhões**

*ficheiros sensíveis abertos a grupos globais*

*mais de*

**75%**

*dos dados acedidos são obsolutos*

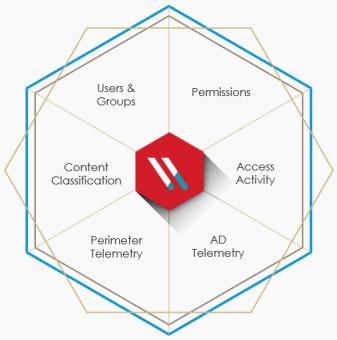
Fonte: Amostra de Avaliação de Risco de Dados, Principais resultados, Varonis

Fonte: More five star reviews than any other File Analysis or UEBA solution, 2019.

**Visibilidade e proteção dos dados em qualquer repositório (on-premise e em cloud)**

Office 365 · entre outros... · box · NetApp · SharePoint · Exchange

**ANÁLISE E AUTOMAÇÃO**




**Proteção Dados**

- Identificação dos dados confidenciais existentes (PCI, SOX, PII, etc.)
- Localização e Exposição dos dados
- Quais os dados usados e não usados
- A quem pertencem e quem acede a esses dados
- Bloqueio/arquivo de dados
- Emissão de relatórios

**Compliance**

- Onde reside informação sensível
- Quais os dados obsoletos
- Eliminação de dados e/ou acessos
- Comprovação de compliance

**Deteção e Resposta**

- Casos de abuso e comportamentos estranhos
- Informação detalha de eventos
- Dificuldade de recuperação
- Sistemas de alertas
- Revisões periódicas

**Pedir Demo**

# PLATAFORMA VARONIS

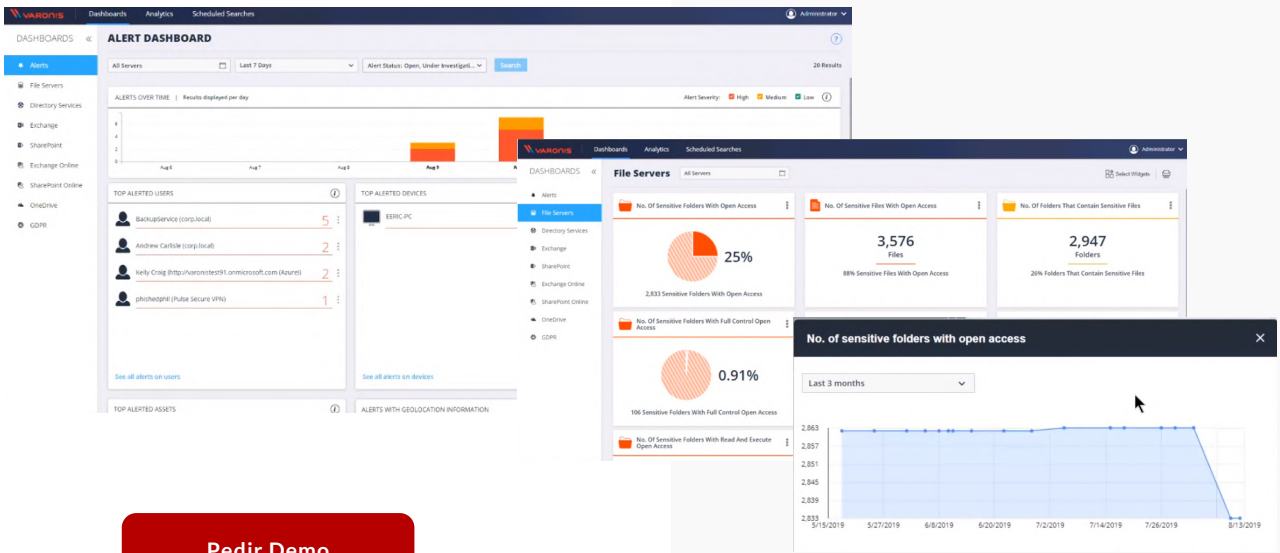
### Visibilidade e contexto

Os **dashboards** gráficos reúnem visibilidade e contexto de toda a atividade dos dados provenientes do Active Directory e de dispositivos de perímetro (como DNS, VPN, proxis, etc.).

Conseguimos ter uma **"big picture"** do que se passa no ambiente e qual exposição de toda informação sensível e não sensível, independentemente do numero de servidores, num único ponto de vista.

- Informação viva vs informação que nunca se toca
- Dados sensíveis, confidenciais e obsoletos
- Pastas , Arquivos e permissões
- Nº de pastas sensíveis abertas a toda organização
- Ficheiros corrompidos
- Contas de utilizador (humano ou máquina) e de grupo
- Contas de utilizador com passwords sem data de validade
- Utilizadores ativos e/ou já não pertencentes à organização
- Atividade e comportamento de dados, utilizadores e dispositivos
- ...

### Veja como funciona




Pedir Demo

### Análise de situações específicas

Queremos visualizar um cenário específico? Basta, na componente de análise, pedir que a plataforma encontre toda a informação, ao indicar o conceito de pesquisa (exemplo: "faturas") e adicionando filtros.

### Alertas e notificações para decisões mais rápidas e conclusivas

A plataforma alerta-nos para eventos significantes que merecem detalhe e análise, mas de forma fácil de investigar para que saibamos qual a ação prioritária.

### Análise aprofundada

O plataforma fornece-nos detalhes aprofundados da respectiva atividade para fazer uma análise mais completa.

1. Identificação de ocorrência suspeita/invulgar
2. Auditoria e registo de atividade
3. Resolução, eliminação, bloqueio, quarentena

Uma vez identificado um "culpado", procedemos a auditoria da pasta e de toda a sua atividade, para assim definir qual a resolução a dar.

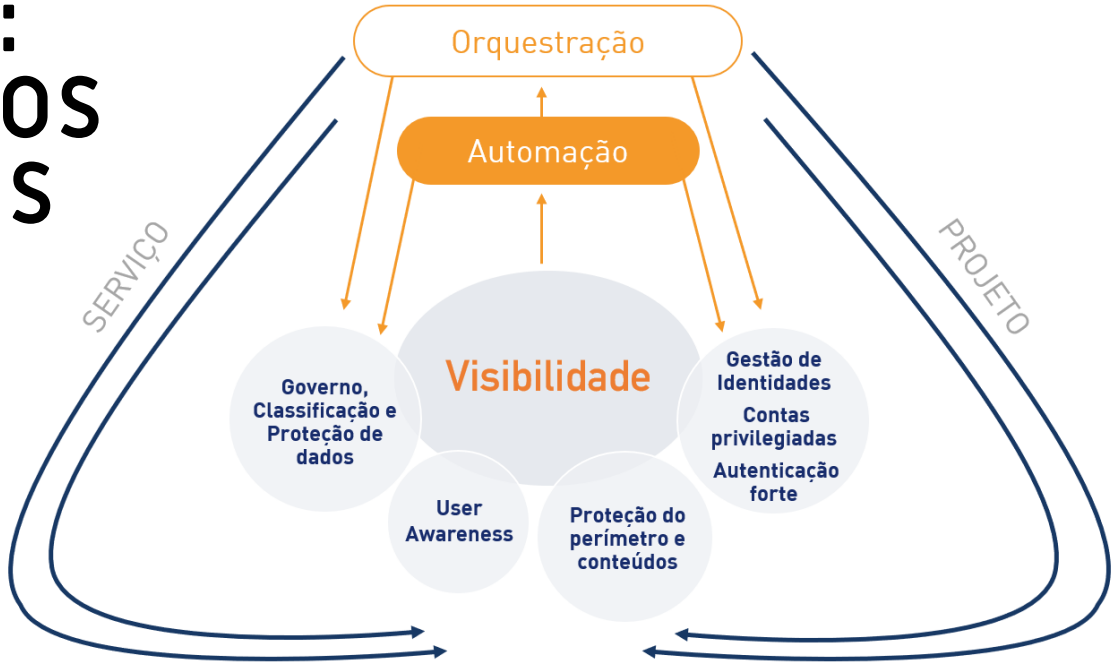
### Automação na proteção, resolução e performance

A operação diária e o combate sistemático ao risco torna-se mais simples e intuitivo através da automatização de processos, tarefas, alertas, permissões, repostas, etc.

Fonte: Data Security Platform, Varonis.

# ORAMIX: OS NOSSOS SERVIÇOS

*de cibersegurança*




Temos uma visão holística sobre a cibersegurança. Os nossos serviços têm como base pessoas, processos e tecnologia e estão definidos em **5 Soluções Funcionais**:

### Governação Classificação e Proteção de Dados

Controlo integrado e visibilidade global dos dados on-premise, em cloud, estruturas sharepoint e NAS. Conhecimento integral da informação, inclusive a sua classificação, integração com outras plataformas e o seu bloqueio.

### User awareness

A literacia digital tem uma grande importância no que se refere à cibersegurança. Esta solução é transversal aos diversos grupos de colaboradores internos de uma organização, permitindo a sua educação relativamente a temas como spam, phishing e regras de acesso a conteúdos online.

### Gestão de Identidades e Contas Privilegiadas

O ciclo de vida das identidades e palavras-chave nas organizações é, hoje em dia, um dos fatores importantes para mitigação de riscos internos. A conta de um colaborador deve ser criada através de um fluxo de aprovações, definindo um perfil que será alterado ao longo da sua permanência e quando este sai deve ser revogado. No caso de soluções de gestão de contas privilegiadas, estas devem ser permanentemente alteradas e guardadas de uma forma segura, permitindo a sua restreabilidade.

### Proteção do Perímetro e Conteúdos

Proteção do perímetro, independentemente de tratar-se de cloud privada, pública ou híbrida, com garantia de redundância de serviços, ligações e datacenters e publicação segura de serviços.

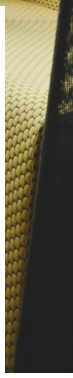
Proteção de dispositivos, a qualquer hora/lugar. Com recurso de AI, ML e Sandboxing, protege sistematicamente dados e responde a ameaças não conhecidas quase por imediato.

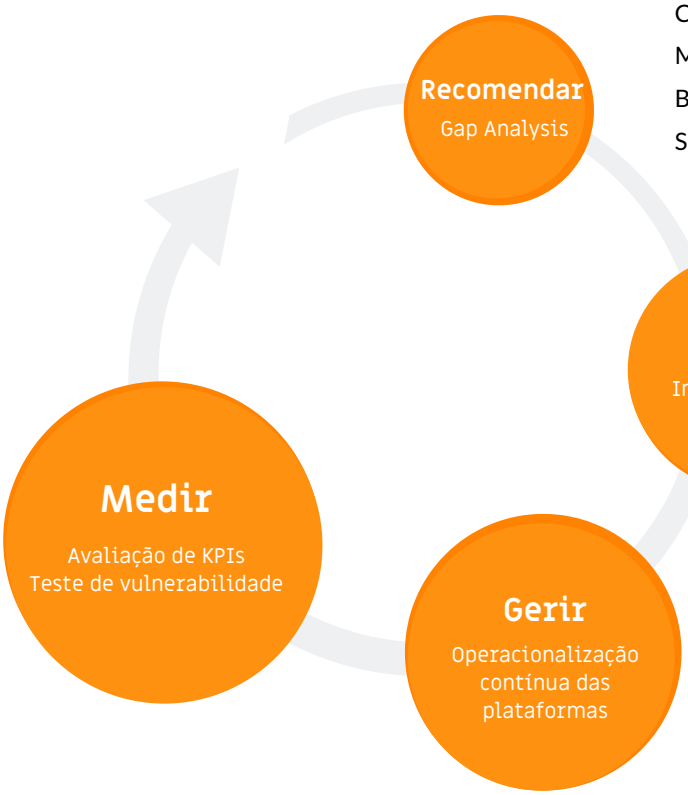
### Visibilidade, Automação e Orquestração

A visibilidade só é atingida com a existência e correlação de eventos de diversas plataformas, através de tecnologias como ML e AI, que permite a restreabilidade e a aprendizagem de comportamentos dos utilizadores e seus dispositivos e, perfis de tráfego dentro de uma rede.

# E QUANTO À ENTREGA DAS SOLUÇÕES?

**A Oramix segue uma abordagem de continuidade na entrega das soluções, de forma maximizar os resultados do seu negócio.**






- Levantamento de necessidades
- Definição e implementação de processos de desencadeamento de incidentes e resposta, e de governo e classificação de dados
- Casos de uso a serem acautelados com orquestração
- Métricas e resultados esperados
- Boas-práticas
- Soluções para caso de uso

- Definição de componentes de automação e orquestração
- Definição de fluxos e categorias

- Resposta orquestrada e simplificada a incidentes
- Visibilidade global de eventos e incidentes (SOC)
- Casos de uso resultados
- Definição de regras nas soluções

Fale connosco

# CONSIDERAMOS AS BOAS PRÁTICAS

- Ferramentas de automação e orquestração melhoram a produtividade dos analistas, não os substituem.
- Estas devem estar presentes em todos os processos da organização, e não apenas em TI.
- Automatizar e orquestrar tarefas repetitivas, de alto esforço manual e processos de baixo risco.
- Começar por “baby steps”. Definir pequenos passos e, aos poucos, integrar processos de maior complexidade e actividades de remediação.
- Manter um número racional e operacional de classificadores de dados.

Fale connosco

**Uma ação manual que demora cerca de 25 MINUTOS pode ser automatizada e executada automaticamente em menos de 1 MINUTO**

## Sobre a Oramix

A Oramix é uma organização especializada em serviços digitais, com presença física em Lisboa e no Porto.

Os 20 anos de experiência já consolidada e o constante desenvolvimento de competências em diversas áreas - integração digital, gestão de dados, consultoria em administração de sistemas e segurança – permite gerar valor aos seus clientes ao adequar, da melhor forma, a sua oferta às necessidades e desafios crescentes de complexidade, desempenho, segurança e inovação atuais das organizações.

Este posicionamento dá-nos vantagens face à transversalidade do conhecimento de tecnologias e processos dentro de uma organização, no que toca a uma visão holística dos serviços que prestamos conjuntamente com cibersegurança.


**Oramix | Sistemas de Informação**

Lagoas Park | Edifício 8, Piso 1 | 2740-244 Porto Salvo | Portugal

(+351) 214 239 345 | fax: (+351) 214 239 347 | oramix@oramix.pt

**www.oramix.pt**