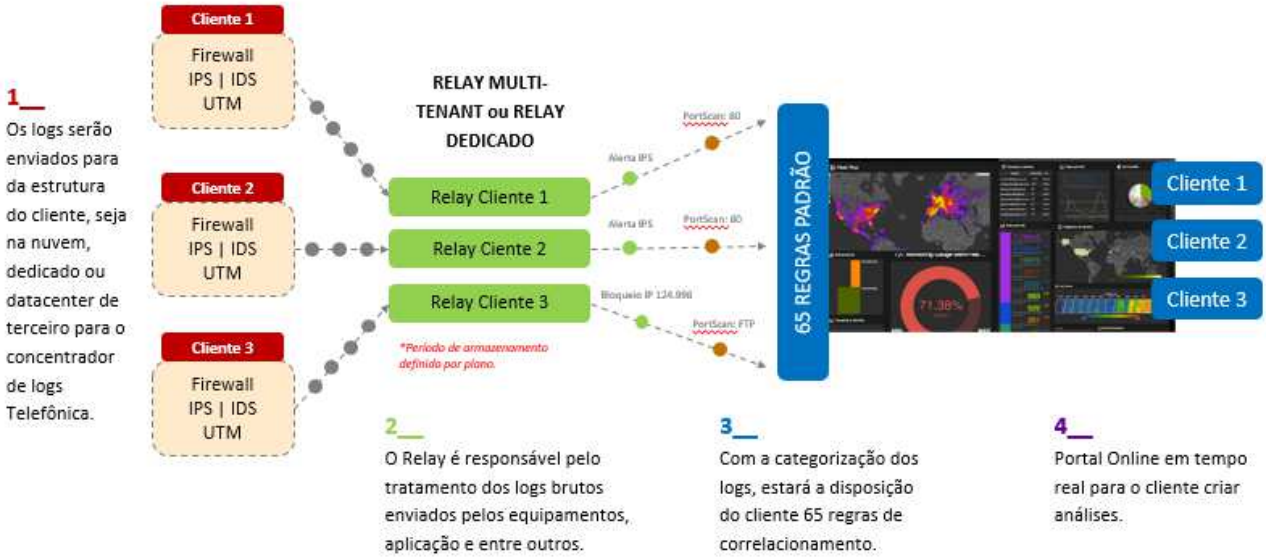
# 1 PROPOSTA DE VALOR




***Security Monitoring*** permite que você tenha uma visibilidade imediata da situação de saúde e segurança do parque da sua empresa. Relatórios em tempo real permitem que você antecipe a manutenção e o redimensionamento de seus recursos de TI e segurança; Os alertas e a correlação de eventos em tempo real permitem que você diminua precocemente os incidentes de segurança e integre seus aplicativos de negócios e os relatórios personalizados proporcionam a capacidade de obter métricas de negócios com rapidez e facilidade.

- **PLANO P:** Presença online da minha empresa, status dos meus PCs e servidores (Servidores de domínio, servidores web, etc ...)
- **PLANO M:** os dispositivos contidos em "Watch your IT" e também o status de seus dispositivos de segurança (Firewall, UTM, Proxy, IDS / IPS e Antivirus).
- **PLANO G:** Monitoramento de todos os equipamentos contidos em "Monitorar sua segurança" e personalização de relatórios e alertas.

**Como isso me ajuda?**

- A detecção em tempo real diminui os tempos de resposta a incidentes.
- Os relatórios pré-configurados permitem que você saiba de imediato o que está acontecendo em todos os dispositivos do seu parque em um portal unificado, sem ter que ir ver o que aconteceu em cada dispositivo e assim reduzir os custos do gerenciamento de TI.

- Alertas pré-configurados baseados em padrões de segurança (por exemplo: categorização enisa) usados no mercado de segurança permitem que você receba alertas diretamente no seu e-mail sobre os incidentes críticos que acontecem em seus computadores com uma recomendação sobre como lidar com o incidente.
- A personalização de relatórios e alertas dá flexibilidade para gerenciar as métricas que são necessárias no dia a dia da sua organização, não apenas relacionadas ao status de TI, mas incluindo as métricas de negócios relevantes em sua empresa. Desta forma, você pode ter uma visão completa do estado do seu negócio e ajudá-lo a tomar decisões

# 2 DESCRIÇÃO DO PRODUTO

***Security Monitoring*** é uma plataforma que permite coletar todos os dados gerados em seus sistemas, infraestrutura de TI, elementos de arquitetura e até mesmo na camada de negócios. Não importa a localização de seus sistemas, estejam eles em seus próprios data centers, em ambientes de nuvem ou em ambientes mistos. Não importa o volume de informações ou o tempo que você precisa para tê-lo totalmente disponível, os dados consolidados estarão sempre disponíveis, enquanto os logs originais permanecerão no sistema, dependendo do tempo de retenção contratado pelo cliente.

Com o Security Monitoring você terá todas as informações disponíveis para consulta, análise, correlação, alertas, geração de Dashboards, etc. Tudo em tempo real e com um desempenho nunca antes visto.

**Os principais benefícios oferecidos pelo atendimento ao cliente são:**

- Controle Através de relatórios on-line e notificações em tempo real para os responsáveis de TI e segurança na empresa tempo, recursos da empresa será sempre supervisionado e qualquer incidente que é detectado será notificado para os cuidados de Uso eficiente adequada dos recursos da empresa. O pessoal de TI e segurança da informação não terá que se dedicar grandes esforços a análise de logs ou comportamentos de equipamentos, se você não pode se concentrar e ser mais eficientes na sua gestão do trabalho e segurança de TI e gestão de informações na empresa, bem como mitigar esses riscos detectados.
- Facilidade de uso A ferramenta é fácil de usar e possui uma interface gráfica intuitiva que se adapta ao perfil da empresa. Através da interface web, o cliente também pode criar novos indicadores, relatórios e alertas que se adaptam às suas necessidades específicas, todos on-line e em tempo real, sem a necessidade de desenvolvimento.
- A funcionalidade oferecida pelo serviço e apresentada no portal de serviços é a seguinte:
- Página inicial (Iniciar) Ele contém alertas de alto nível de informação (nos últimos 5 alertas gerados), dados de volume (Gbytes) a ser recebido na conta de cliente, o tipo de eventos recebidos pela tecnologia (distribuição em%) e uma medida final números de eventos recebidos nos últimos 15 segundos.

## Relatórios

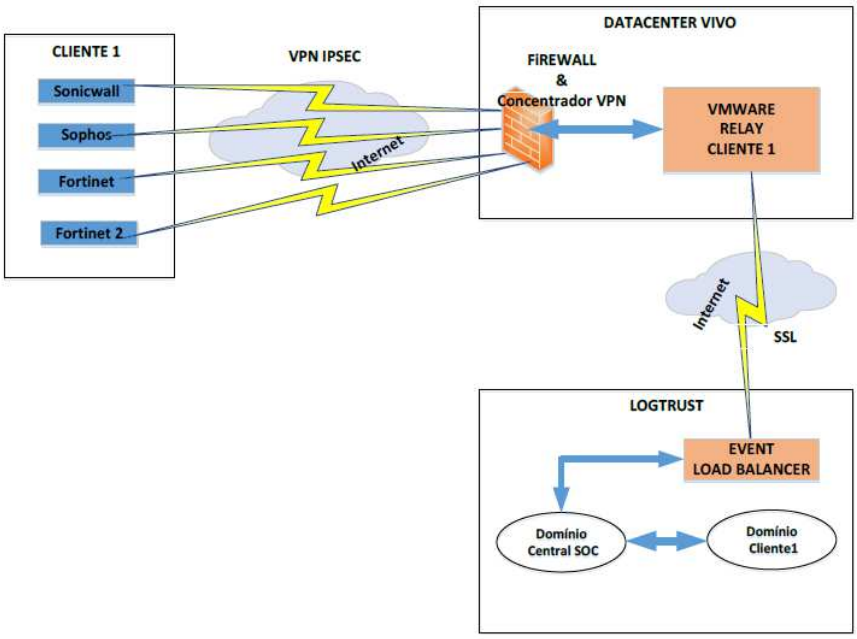
- **Monitor de Presença.** Oferece uma visão do status e da qualidade do acesso à Internet e da presença do site da empresa (indicadores relacionados ao site - ou páginas da web)
- **Monitor de Saúde do Equipamento.** Resumo gráfico da carga e uso dos principais recursos do equipamento supervisionado (CPU, memória, espaço em disco, etc.)
- **Monitor de eventos de segurança.** O volume de alertas relacionados à segurança

no equipamento produzido é mostrado em uma lista e graficamente

- **Dispositivos.** Nesta categoria, um relatório específico de cada tecnologia suportada é exibido nativamente.
    - Configuração. Nesta seção o cliente pode configurar / customizar alguns parâmetros de serviço, baixar SW, acessar seções para configurar e criar seus próprios relatórios (dashboards)
    - Alertas aqui, o usuário tem acesso ao relatório de alerta que inclui todos os tipos de alertas, não apenas alertas de segurança.
    - Gerenciamento de log. Esta seção dá acesso à funcionalidade de gerenciamento logístico, onde ou o cliente tem à sua disposição ou poder de recuperar e analisar determinados logs retidos por meio de consultoria. Você também pode ver esses resultados em gráficos e relatórios personalizados (painéis)

# 2 ARQUITETURA DO SERVIÇO

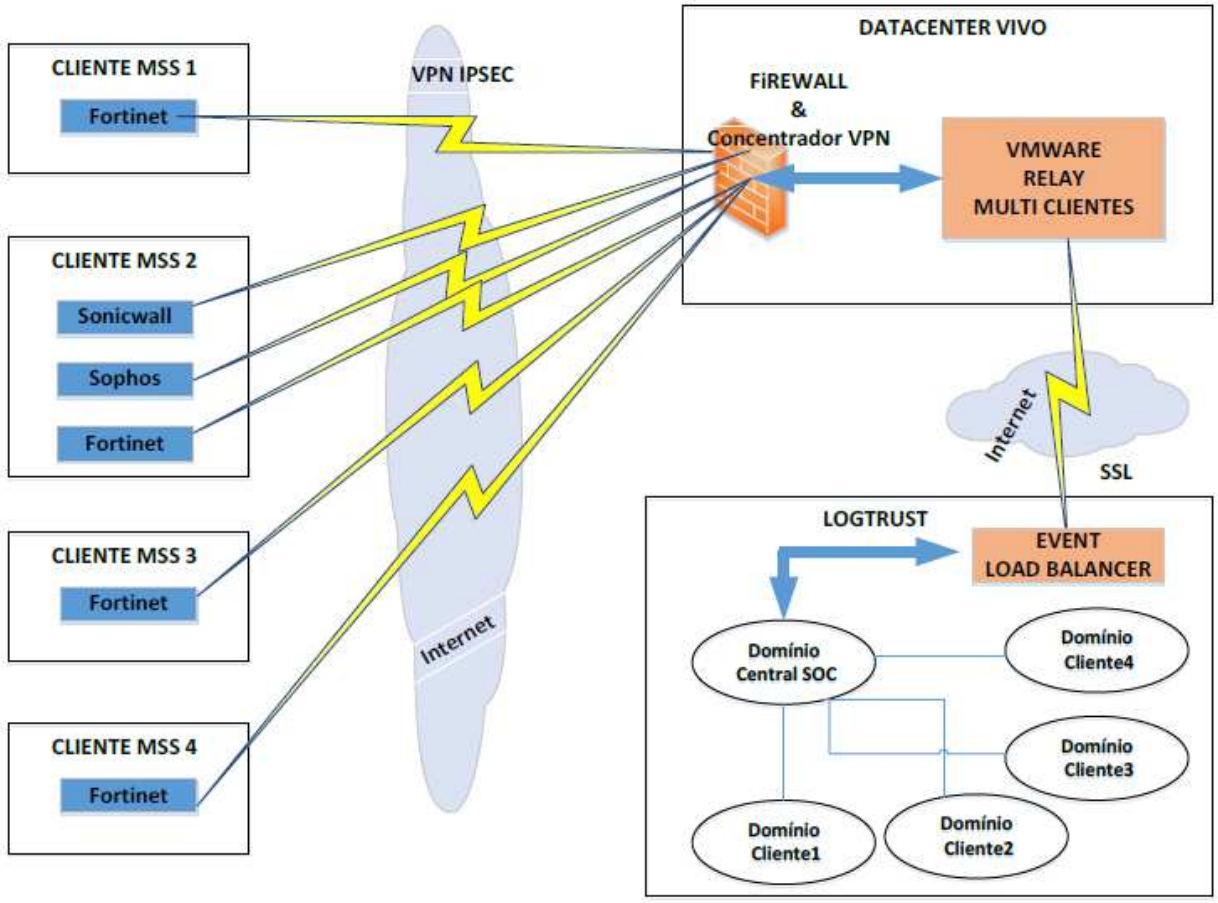
## 2.1 RELAY DEDICADO




Este cenário contempla 1 Relay por cliente, no qual recebe o log de cada equipamento em diferentes portas UDP. Após estabelecida essa comunicação do Relay com os dispositivos para receber logs, ocorrerá a comunicação com a nuvem da LOGTRUST via protocolo SSL/TLS over Internet, onde é necessária realizar as liberações de entrada e saída do tráfego no firewall.

Relay irá atuar apenas como “encaminhador” dos logs de forma a não armazenar os logs e consequentemente ocupar pouco espaço de hardware.

## 3 RELAY COMPARTILHADO




Este cenário contempla 1 Relay para múltiplos clientes, no qual recebe o log de cada equipamento em diferentes portas UDP e o Data Management diferencia os clientes por IP ou hostname ou virtual domain de cada dispositivo. Após estabelecida essa comunicação do Relay com os dispositivos para receber logs, ocorrerá a comunicação com a nuvem da LOGTRUST via protocolo SSL/TLS over Internet, onde é necessária realizar as liberações de entrada e saída do tráfego no firewall.

O Relay irá atuar apenas como “encaminhador” dos logs de forma a não armazenar os logs e consequentemente ocupar pouco espaço de hardware no cluster VMWARE e Storage.
A partir da Gerência do Data Management com um Domínio Central + Múltiplos Domínios, foi

possível identificar a possibilidade da realização de configurações para disponibilizar, no Domínio Central, as informações de Alertas e Dashboards desejados dos múltiplos domínios.

## 4 PLANOS E MODALIDADES

O serviço é oferecido em diferentes pacotes comerciais para melhor se adaptar às necessidades dos clientes de acordo com seu perfil e necessidades. Desta forma, os seguintes pacotes são definidos:

- **PLANO P**
  - **ARMAZENA:** Saiba onde os visitantes se conectam à Web e qual é o status e o uso dos equipamentos de TI da empresa. Receba notificações se os incidentes forem identificados.

- **PLANO M**
  - **MONITORA:** Monitorar e monitorar a atividade das equipes de segurança e TI da empresa. Notificações em tempo real baseadas em técnicas de correlação em caso de identificação de incidentes.

- **PLANO G**
  - **GESTIONA:** Analisar e conhecer o funcionamento da segurança e dos negócios da empresa utilizando business intelligence facilitando um gerenciamento baseado em dados reais.

## 5 CONSOLE ÚNICA

Um caso muito interessante do ponto anterior é a funcionalidade única do console.

Hoje, dentro de uma organização, temos muitos consoles para analisar o mesmo tipo de informação, dependendo do fabricante, como no caso dos firewalls. Gerenciar vários consoles, instalar software em cada posição, atualizá-lo e manter privilégios de acesso e administração de usuários corretos é uma tarefa que consome uma quantidade muito grande de tempo e recursos.

Com monitoramento de segurança, todos os usuários terão acesso via web ao nosso serviço para consumir todos esses dados será muito fácil de gerenciar privilégios, aprender o que você pode ver cada um com filtros adequados pré-configurados e saber o que e consultas por isso que eles têm realizado fizeram. Tudo perfeitamente auditado e sob controle.

Você pode até usar o monitoramento de segurança como parte de seus diferentes sistemas de alerta e integrar os alertas gerados por outros produtos como mais uma fonte de informações.

## 6 INFORMAÇÃO ESTRUTURADA

Não apenas informações estruturadas podem ser integradas e analisadas em nossos sistemas.

Também o formato de informação carente pode ser integrado, analisado e extrair os dados de valor de forma simples e eficaz.

Você pode integrar eventos não estruturados, definir operações de filtragem, expressões regulares e muito mais, até extrair as informações relevantes para sua empresa. Desta forma, ele irá gerar visualizações virtuais de tabelas com informações não estruturadas, nas quais novas colunas são geradas em tempo real, permitindo que aproveitem ao máximo as valiosas informações geradas em sua empresa.

## 7 PRIVILEGIOS DE ACCESO GRANULARES

Devido à diversidade de informações coletadas e suas sensibilidades, você pode limitar seu acesso por perfis e funções de maneira simples e fácil.

## 8 ANÁLISES DE COMRPORTAMENTO

***Security Monitoring*** oferece toda uma estrutura de Geolocalização de endereços IP que você pode usar a qualquer momento com qualquer um dos seus dados. Essa estrutura permitirá que você, por exemplo, calcule os perfis de conexão de seus usuários com a granularidade que você decidir (país, região ou cidade), armazene esses padrões comportamentais de forma histórica e que sejam realimentados em cada conexão e gere alertas em caso de discrepâncias. Da conexão atual com o perfil do usuário.

Não só será capaz de gerar alertas quando detectar conexões estranhas por países, ISPs estranhos, etc; Você será capaz de saber o que é habitual para cada um dos seus usuários e detectar padrões de ataque muito mais sutis e com muito menos falsos positivos.

## 9 CUMPRIMIENTO DE NORMATIVAS

A maioria das regulamentações de TI / segurança exige que os dados sejam retidos por períodos específicos de tempo, proteção, monitoramento e controle de acesso e uso de informações confidenciais e monitoramento de registros.

Atender a esses requisitos pode ser caro para uma organização: ela pode criar processos e despesas redundantes. Algumas empresas compram software de gerenciamento de registros SIM / SIEM e armazenamento relacionado para estar em conformidade, mas com valor operacional limitado. Uma auditoria pode gerar um grande número de solicitações de dados manuais, distraindo o departamento de TI e aumentando os custos ...

Com o Security Monitoring, você pode enfrentar esses desafios e cumprir várias regulamentações usando a mesma plataforma.

- Não é necessário adquirir armazenamento interno caro. O serviço será fornecido a partir de um nó dedicado ao serviço dentro do Telefónica VDC. O Security Monitoring só usará a infraestrutura do nó para coletar, armazenar, consultar e correlacionar seus dados.

- Você paga apenas pelo que consome. Seu preço é de € 0 para pessoal administrativo, manutenção e aquisição de licenças, hardware e servidores.

- Índice de dados em tempo real que permite procurar alertas e gerar relatórios sobre todas as informações.

- Com nossa poderosa ferramenta de divulgação, você pode demonstrar facilmente sua conformidade. Você pode criar quantos relatórios forem necessários.

- Cumprir com os requisitos de monitoramento automático de eventos de segurança, programar e configurar alertas para qualquer pesquisa.

***O Monitoramento de Segurança ajuda a cumprir as seguintes leis e regulamentos:***

- PCI- DSS
- FISMA
- HIPAA
- Directiva sobre conservación de datos de la UE (DRD)

## 10 ALERTAS PRECONFIGURADAS

Além de todas as métricas e alertas que você mesmo pode fazer, o sistema incorpora desde o primeiro momento uma galeria de aplicativos com mais de cem alertas de segurança, monitorando ataques na camada web, anomalias, etc.

**Alertas que você pode ativar com um clique e ter informações valiosas a partir do primeiro segundo.**

- Sistema de Monitoramento
- Gerenciamento de alertas
- Relatório de Firewall
- Biblioteca de Alerta de Ataque
- Biblioteca de alertas de sistemas operacionais
- Biblioteca de alertas de servidores da Web
- Biblioteca de alertas para servidores de aplicativos
- Antivírus
- Diretório Ativo
- Ids / Ips
- Monitoramento
- Outros alertas
- Proxy
- Roteador
- Servidor web
- URLs

- UTM

# 3 OFERTA ECONÔMICA

O serviço oferecido ao cliente "CLIENTE" é composto por:

- **PACOTES:**

  Os pacotes incluem mais funcionalidades até a opção "Premium" (Gerenciar sua Segurança) o pacote que oferece funcionalidade completa, incluindo a possibilidade de incorporar fontes próprias e criar relatórios e alertas personalizados.

  O equipamento que pode ser monitorado é determinado pela modalidade de serviço escolhida e, consequentemente, o acesso a todas as funções e informações incluídas será habilitado no portal de serviços.

**Equipamento monitorado por pacote:**

- **PLANO P**: Router, un dominio web, PC´s, Servidores y Servidores Web.
- **PLANO M**: Router, un dominio web, PC´s , Servidores, Servidores Web, Firewalls, Antivirus, UTM, Proxy, IDS/IPS.
- **PLANO G**: Igual que Stardard.

**Armazenamento de Logs**:
Existem vários prazos disponíveis para armazenamento dos logs coletados no ambiente do cliente.

- 6 Meses
- 12 Meses
- 24 Meses
- 36 Meses

4

# 5 PROVISIONAMENTO DA SOLUÇÃO

Atualmente, o serviço de monitoramento de segurança é provisionado individualmente para a infraestrutura do cliente.

A solução tecnológica é baseada em um modelo de nuvem, sem pontos únicos de falha e resultou em pelo menos dois locais por considerações de continuidade de negócios, permitindo oferecer um serviço que utiliza um modelo de economias de escala para a partilha de infra-estrutura entre os vários clientes e vários países.

O serviço é fornecido a partir de um nó global localizado na nuvem pública da Telefónica localizada na Espanha, no data center de Alcalá de Henares. (VDC)

Dispositivos clientes, por meio de agentes e o relé enviar logs de segurança para o centro de dados usando uma conexão SSL com um certificado único para o cliente, o que significa dizer que cada cliente tem seu próprio espaço dentro da candidatura.

Todos os recursos e configurações para funcionamento da plataforma são realizadas pela equipe SOC eo prestador de serviços, que são responsáveis pelo serviço de suporte.