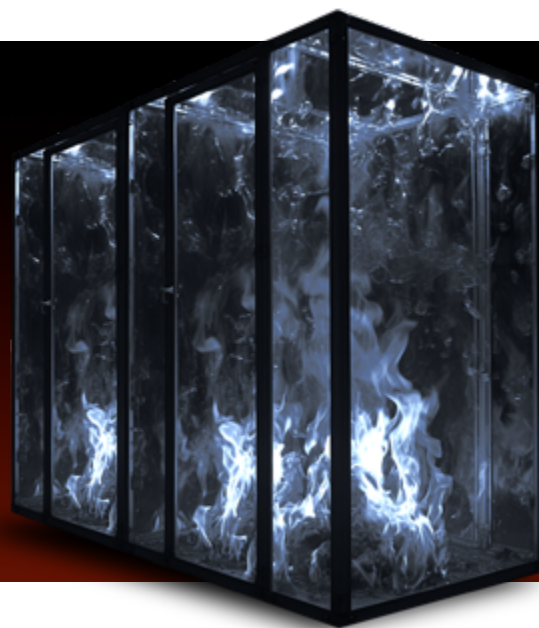




# Datasheet

## RIS - Módulo WAF

[Baixe aqui os datasheets dos outros módulos](#)



Prepara-se e evite ataques em suas aplicações Web, API ou Mobile, com as principais soluções de mercado integradas no RIS, 24x7.

O roubo de informações sensíveis através de explorações Web e os ataques de DDoS são as principais dores de cabeça para os times de Segurança. Mas e se a sua empresa pudesse, de forma rápida, identificar os principais ofensores em tempo real e quando ataques ou tentativas de exploração fossem direcionadas à sua aplicação automaticamente fossem bloqueadas, ficando totalmente transparente para usuários legítimos?

## Entrega

Com o módulo Web Application Firewall do RIS a empresa visualiza em tempo real todos os acessos, ataques e bloqueios que estão sendo realizados pela solução de WAF. Isso a partir de correlação de informações e da identificação dos IPs que mais atacam o ambiente, segmentados por localidade, recorrência e histórico de reputação do IP. O time de SOC da Redbelt trabalha 24h por dia e 7 dias por semana para gerenciar e monitorar todos os alertas que estão sendo gerados e bloqueados pelo módulo, garantindo que nada saia do controle.

## O que é o RIS?

O RIS é a plataforma SaaS desenvolvida pela Redbelt Security que combina inteligência humana e orquestração. Combinando as soluções de diferentes fabricantes com a nossa inteligência, permite concentrar e correlacionar as informações e logs de segurança necessários para um plano de ação.

Possui 4 módulos para ajudar as empresas que desejam reduzir o tempo de resposta aos incidentes e gerenciar o ciclo de vida de vulnerabilidades no seu ambiente. Aqui, falaremos do módulo Vulnerabilidades. Aqui, falaremos do módulo WAF. Conheça os outros módulos [aqui](#).

O módulo de WAF funciona de forma integrada com a solução da Imperva, além de outros fabricantes, caso a empresa já tenha alguma solução de WAF e precise integrá-la com um SOC para monitoramento e gerenciamento contínuo ou ter todos os dados gerenciais gerados pelo RIS.

### **Os dados são importados automaticamente e apresentados em um dashboard gerencial, trazendo informações como:**

- Quantidade total de acessos por período, diferenciando quais acessos foram realizados por bots e quais acessos foram realizados por humanos;
- Aplicação de desafios de captcha ou bloqueio automático caso um ou mais visitantes tentem explorar tentativas de acerto e erro com logins e senhas, sem precisar customizar sua aplicação;
- Total de tráfego e banda poupada do seu datacenter (nuvem ou local) já que a solução de WAF trabalha com CDNs, reduzindo custos;
- Quantidade total de ameaças identificadas e protegidas em todo ambiente e a mesma visão também segregadas por site;
- Indicador contendo os principais países e IPs atacantes, podendo rapidamente identificar se um ou mais países que mais atacam sua empresa, devam permanecer liberados ou serem bloqueados de forma geográfica;
- Funcionalidade de capturar novos ataques de redes globais de inteligência de ameaças e realizar o bloqueio através de blacklists (IoC's), se antecipando antes que eles ocorram;
- Tradução dos ataques de acordo com a OWASP Top 10 ou de ataques conhecidos, para entender o que os atacantes estão querendo fazer com a sua aplicação;
- Cada domínio e subdomínio possui uma visão única e detalhada, com os principais indicadores como: quantidade de acesso, total de tráfego, quantidade de ameaças, principais IPs atacantes etc.

As informações centralizadas auxiliam na tomada de decisões para bloqueios de IPs ou até mesmo regiões geográficas.

Converse com um de nossos consultores. E descubra como o RIS pode elevar a segurança da sua empresa.

**> Converse com um de nossos consultores**