

THREAT INTELLIGENCE EM TEMPO REAL PARA COMBATER AMEAÇAS EMERGENTES



HAL LONAS
CTO
WEBROOT

Hal Lonas, CTO do Webroot, colaborou com a Black Hat, uma organização que se dedica à realização de eventos sobre segurança tecnológica, desde a apresentação de novas pesquisas, desenvolvimentos e últimas tendências, para responder a algumas das mais importantes questões da atualidade da cibersegurança.

PORQUE É QUE AS FERRAMENTAS DE CIBERSEGURANÇA TRADICIONAIS NÃO SÃO SUFICIENTES PARA GARANTIR A DEFESA CONTRA RANSOMWARE, CRYPTOMINING E OUTRAS AMEAÇAS EMERGENTES?

“Essas soluções de cibersegurança apenas são eficazes na proteção contra ciber ameaças tradicionais. Uma abordagem à cibersegurança baseada em assinaturas não é eficaz contra ameaças polimórficas, que atualmente representam mais de 90% dos ataques.”

PORQUE É NECESSÁRIA INTELIGÊNCIA DE AMEAÇAS EM TEMPO REAL PARA DAR RESPOSTA A ESTES ATAQUES?

“No panorama atual da cibersegurança, o mais importante é a informação: ter a inteligência de ameaças correta, no momento certo, para identificação e proteção contra as ameaças assim que ocorrem. Uma abordagem baseada em comportamentos e em machine learning automatizado consegue garantir inteligência em tempo real que se adapta aos ataques modernos, à medida que vão aparecendo.

Quando as empresas procuram soluções de segurança, devem assegurar-se que já vem com inteligência de ameaças em tempo real incluída. Para além disso, a inteligência de ameaças deve ser incorporada numa abordagem de segurança multicamada, que inclui proteção de rede URL e IP, tecnologia anti-phishing, proteção endpoint e ainda treino de consciencialização para a importância da segurança.

A inteligência de ameaças é a base da proteção de todos os utilizadores contra as ameaças atuais, em constante e rápida alteração.”

FALE-NOS SOBRE O SERVIÇO WEBROOT SECUREANYWHERE DNS PROTECTION. QUAL O PROBLEMA QUE ESTA SOLUÇÃO AJUDA OS MSP E PME A RESPONDER?

“Os MSPs e as PMEs precisam de ferramentas de cibersegurança eficazes, que sejam fáceis de instalar e gerir. É por isso que o serviço Webroot SecureAnywhere DNS Protection faz tanto sentido.

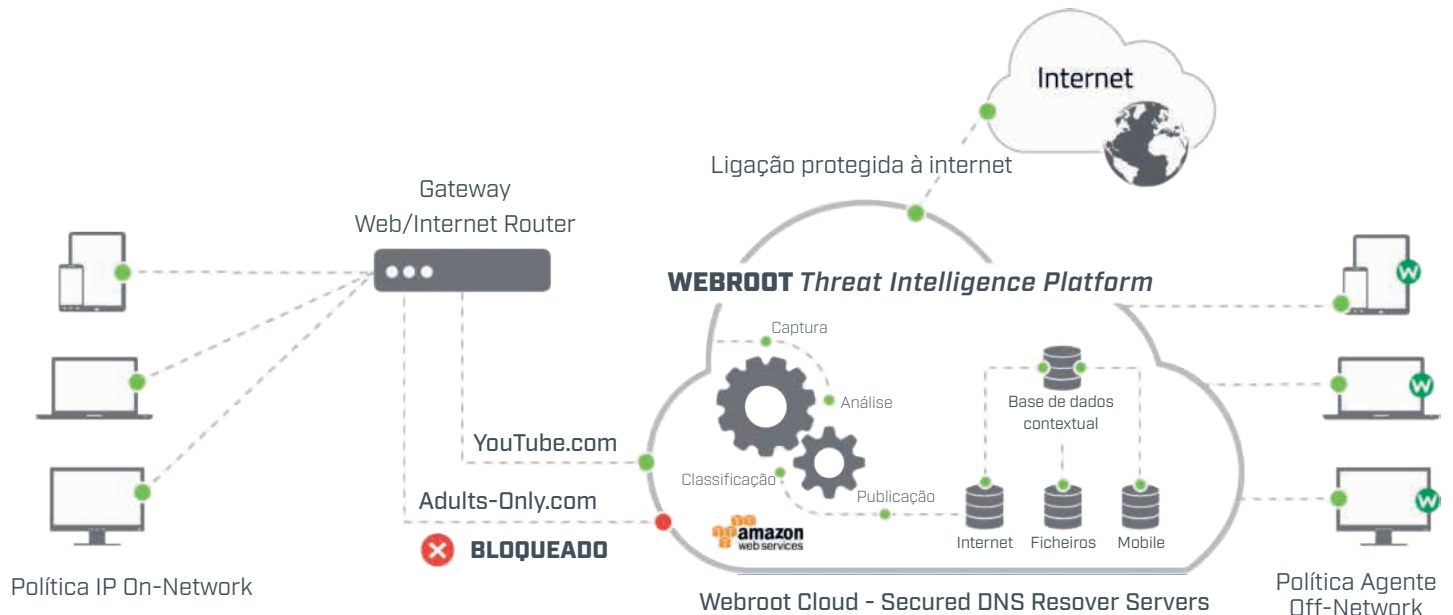
Com os inúmeros ataques a redes de PMEs devido a navegação web não protegida, fazer a filtragem do conteúdo pode ter um impacto significativo na paragem das ameaças antes de entrarem na rede. A proteção DNS, protege todos os dispositivos da rede, incluindo o crescente número de dispositivos IoT, cuja correção após ataque pode ser difícil ou mesmo impossível. A proteção DNS ajuda ainda a proteger a rede de convidados, bloquear URLs maliciosos e proteger clientes, assim como o próprio negócio, das mais variadas ciber ameaças.

Para MSPs e PMEs, a proteção DNS é incrivelmente fácil de instalar, configurar e gerir, sendo outra ferramenta crítica para a abordagem de segurança em camadas.



SOLUÇÕES DE SEGURANÇA DE NOVA GERAÇÃO

WEBROOT SECURE ANYWHERE® DNS PROTECTION



Reduz em mais de 85%
as ameaças que
infetam a rede

Filtragem de sites de
risco com quase
nenhuma latência

Baseado em cloud,
sempre atualizado, eficaz
em ataques zero day

Políticas de utilização
web e visibilidade
sobre o tráfego

BENEFÍCIOS PARA MSP

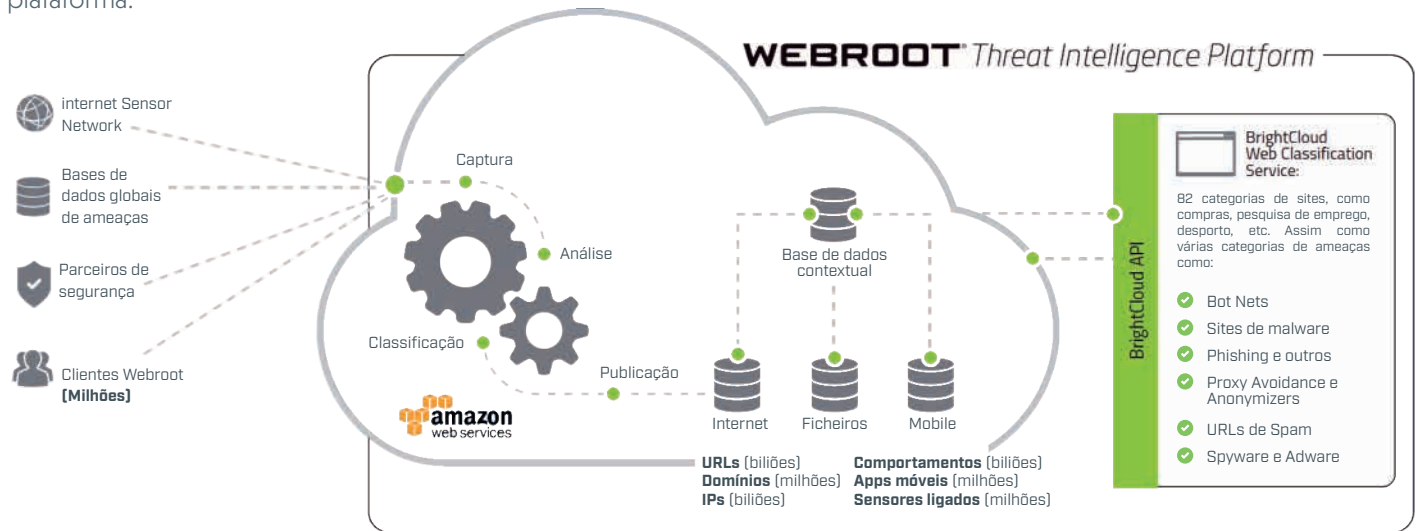
- » Fácil de implementar e gerir
- » Opções de faturação flexíveis
- » Consola única de gestão para proteção endpoint e de rede
- » Aumento de receitas com uma oferta de serviços complementar
- » Consola única de gestão para proteção endpoint e de rede
- » Aumento da produtividade e menos tempo a perseguir ocorrências de segurança
- » Proteção exata e em tempo real
- » Visibilidade de ameaças web e controlo da utilização

BENEFÍCIOS PARA PME

- » Reduz o riscos de rede e do utilizador
- » Melhora a velocidade da rede e a postura de segurança da empresa
- » Para as ameaças antes de atingirem os endpoints ou os utilizadores
- » Resposta eficaz às necessidades de cibersegurança atuais das empresas portuguesas
- » Solução de segurança que ajuda a garantir o cumprimento do GDPR.

WEBROOT® THREAT INTELLIGENCE PLATFORM

Plataforma avançada de Inteligência em tempo real, captada globalmente através de endpoints de rede e dos parceiros fornecedores de tecnologia. Bastam apenas 5 minutos da descoberta até à proteção universal. É eficaz mesmo em ataques Zero-Day, graças ao feedback global de inteligência valiosa que recebe em loop e que enriquece constantemente a plataforma.



Altamente automatizado, machine learning massivo, avançado e com variadas origens

Ficheiros e apps classificados mais depressa e com muito maior precisão

Sistemas de lowtouch que necessitam de interação humana mínima

Centenas de modelos de classificação alojados em Hadoop para cobrir diferentes tipos de ameaças e conteúdos linguísticos

Publicação de milhões de atualizações diárias sobre novas ameaças e reputações de URLs, IPs, apps e ficheiros

5ª geração de machine learning - analisa e produz Threat intelligence contextual e segurança em diversos vetores em segundos

PRODUTOS INTEGRADOS EM PLATAFORMA COMPROVADA

| PROTEÇÃO ENDPOINT | PROTEÇÃO DE REDE | PROTEÇÃO DO UTILIZADOR | BRIGHTCLOUD® THREAT INTELLIGENCE | FUTUROS PRODUTOS |
|--|---|------------------------|----------------------------------|------------------|
| <p>Produtos/serviços</p> <p>Processamento</p> <p>Dados</p> <p>Infraestrutura</p> | <p>Autenticação, licenciamento, business Intelligence, serviços endpoint, serviços e suporte ao cliente, sensor telemetry</p> <p>Machine learning, IP scanning, sensores, classificadores, treino, análise contextual e análise de comportamento</p> <p>Comportamento de produto e dados sobre as ameaças, inteligência das ameaças, cliente, status do produto, licenciamento, e-commerce</p> <p>AWS (utiliza 4000 servidores, 40 serviços cloud – incluindo EC3, S3, Elastic search DDS, cloudera, Hadoop, Cassandra, New Relic e outros)</p> | | | |

WEBROOT: COMO SE DIFERENCIA?

O Webroot destaca-se enquanto marca e fornecedor de confiança para soluções de segurança B2B, disponibilizando uma plataforma unificada para Endpoint, Proteção DNS e treino de segurança.

Há mais de 10 anos a ajudar os MSP a criar e dimensionar as suas ofertas de segurança, com as soluções inteligentes do Webroot tem a garantia de:

- ✓ Instalação em apenas alguns minutos e muito fácil de gerir
- ✓ Configuração e report fácil e rápido através da consola ou API
- ✓ Filtragem de todos os requisitos DNS através do DNS Protection
- ✓ Serviços BrightCloud Threat Intelligence
- ✓ Categorização e análise da maior base de dados URL deste género, em tempo real
- ✓ Configuração e report fácil e rápido através da consola ou API
- ✓ Análise contextual para criar uma visão mais profunda dos ficheiros interligados e sites na Internet

O Webroot desenvolve soluções premiadas, que merecem a confiança de fornecedores de segurança líderes como a Palo Alto, F5, Cisco, HPE e muitas outras.

