White Paper

PORQUE PRECISAM AS EMPRESAS DE SEGURANÇA WEB E PROTEÇÃO ENDPOINT?

by George Anderson, Product Marketing Director, Webroot
tradução por Minitel NEXT

INTRODUÇÃO

A utilização da internet representa, hoje em dia, a maior ameaça à segurança dos dispositivos dos colaboradores e da rede da empresa sejam comprometidos. Com a crescente utilização dos dispositivos móveis, este risco agravou-se ainda mais para as empresas.
Um estudo recente da Forrester, revelou que 60% dos colaboradores trabalham a partir de casa algumas vezes por mês e que 38% fazem-no pelo menos 1 ou mais dias por semana. Os riscos da utilização da internet são tão elevados que os especialistas em segurança consideram que é essencial existir uma solução de gateway como primeira linha de defesa.

Durante muitos anos, a segurança web era feita praticamente apenas com filtros URL (controlo dos sites que podem ser acedidos) e, talvez, analisar o tráfego web através de um antivírus de perímetro de rede. No entanto, uma vez que a internet está cada vez mais perigosa, têm emergido soluções de gateway web mais completas, que oferecem funcionalidades de segurança como filtros URL, filtros por tipo de ficheiro, filtros por aplicação e proteção web adicional contra malware.

Alguns dos mais recentes desenvolvimentos em segurança web centram-se nos serviços de segurança baseados em cloud, que movem a segurança web para a camada da internet e param as ameaças antes que alcancem a camada de perímetro de rede DMZ tradicional.
Permitem que as organizações cumpram com o regulamento de proteção de dados e aplicam políticas de utilização web consistentes, independentemente da localização física.

O Webroot SecureAnywhere® Web Security Service foi uma das primeiras soluções de web gateway totalmente baseada em cloud (lançado em 2007).
O serviço atual é completamente diferente do que era na altura, mas ainda disponibiliza uma alternativa eficiente em termos de custos às soluções de segurança web gateway on-premise tradicionais.
Com uma consola de gestão web-based centralizada e fácil de utilizar, este serviço de segurança web elimina a necessidade para qualquer infraestrutura IT on-premise e, juntamente com o seu agente extremamente leve e inviolável, é muito simples de implementar.

Uma gateway de segurança de nova geração não só previne infeções, violações e minimiza a complexidade da gestão da segurança web, como também reduz significativamente os custos operacionais e riscos de proteção dos utilizadores contra ameaças de malware avançado, phishing e outros ataques sofisticados, interceptando-os e parando-os antes de infectarem o utilizador e a rede.

O mais importante é que a segurança web e a utilização da internet devem ser abordadas em separado da proteção endpoint, uma vez que não é realista esperar que a última linha de defesa (segurança endpoint) seja 100% eficaz contra todos os tipos de ameaças web.

PREVENÇÃO DE ATAQUES E FUGAS

A internet é o vector número um de infeções e fugas de dados nas empresas. Por isso, ser capaz de parar com eficácia as ameaças web é vital. O Webroot SecureAnywhere® Web Security Service garante a proteção dos utilizadores contra vírus e spyware. Através das suas camadas de segurança proativa e da utilização da Webroot BrightCloud® Threat Intelligence Platform, os serviços de segurança web preveem e protegem contra ataques avançados e desconhecidos.

A arquitetura cloud permite que os utilizadores sejam autenticados diretamente para maior proteção, independentemente da sua localização física. O agente assegura que os utilizadores não conseguem ultrapassar as políticas de utilização e, por isso, ajuda a aumentar a produtividade e facilita a conformidade com normas e regulamentos legais. Muito eficaz e preciso, o BrightCloud® Threat Intelligence, combinado com a prevenção preditiva de infeções de malware web, são a razão pelo que o Webroot é capaz de deter as ameaças e transformar a internet num local seguro para as empresas.

Prevenção comprovada de vírus e spyware

O Webroot SecureAnywhere® Web Security Service oferece uma prevenção avançada contra malware e spyware. A proteção endpoint de nova geração, incluindo antivírus, prevenção de intrusão de host (HIPS) e deteção de tráfego malicioso, opera numa camada para prevenir infeções, detetar elementos comprometidos e parar ameaças web com inteligência de ameaças em tempo real. Numa outra camada, faz exploração avançada, não recorrendo à atualização baseadaem assinatura e proteção heurística, para além de defesas de propriedade contra JavaScript, Shellcode e scripts entre sites, todos utilizados para lidar e parar ameaças, que são perdidas por muitas outras soluções.

BrightCloud® Threat Intelligence para ameaças desconhecidas

O Webroot SecureAnywhere® Web Security Service disponibiliza camadas de proteção adicionais através da plataforma de inteligência de ameaças BrightCloud®, que cruza dezenas de milhões de informações sobre ocorrências de malware e aplicações duvidosas, monitorizando biliões de endereços IP e URLs todos os dias. Com estas informações, desenvolve uma inteligência de ameaças preditiva, contextual e em tempo real, capaz de detetar um largo espectro de vectores e que permite que o Webroot implemente estratégias de defesa profunda em apenas alguns instantes, contra tráfego malicioso para dentro e fora da cloud.

A inteligência de ameaças contextual é a única forma de combater eficazmente os cibercriminosos modernos e de dar segurança às empresas. É isto que torna esta inteligência de amaças não só um repositório de dados seguros baseado em cloud, mas também numa das mais eficazes plataforma de combate a ameaças em tempo real da sua categoria.

Os números são avassaladores. A plataforma de inteligência de ameaças BrightCloud® faz o scan completo do endereço IPv4 mais de três vezes por dia para classificar continuamente e com precisão inúmeros URLs, endereços IP e domínios. Analisa milhões de novos ficheiros, updates e apps, procurando comportamentos maliciosos e estudando as maiores tendências de malware baseadas na informação recolhida de milhões de endpoints, redes e dispositivos. Tudo isto, e mais, é utilizado para enriquecer constantemente a plataforma BrightCloud® e permite que a Webroot proteja as empresas de forma preventiva e com enorme precisão, contra ataques Web avançados e sofisticados. Esta plataforma é, literalmente, uma sandbox em tempo real de toda a internet, convertida em inteligência de ameaças.

A maior e mais precisa base de dados de categorização de URLs

O Webroot Web Security Service utiliza o serviço de classificação web da BrightCloud® para controlar centenas de milhões de websites, de forma a proteger os utilizadores de serem expostos a spyware, drive-by malware e muitos outros tipos de código malicioso com que se deparam ao utilizar a internet. Infelizmente, mesmo sites legítimos estão frequentemente comprometidos nos dias de hoje e, muitas vezes, alternam rapidamente entre conteúdo malicioso e benigno para evitar deteção.

O Webroot BrightCloud® Web Classification Service tem registo e classificação de mais de 600 milhões de domínios, descritos em mais de 83 categorias. Trata websites em mais de 45 línguas e analisa mais de 740 milhões de endereços IP, descobrindo mais de 85 000 novos endereços IP maliciosos por dia.

Esta classificação extremamente detalhada garante aos administradores um controlo granular sobre os acessos dos utilizadores aos websites, permitindo reforçar políticas flexíveis e com relatórios precisos da gestão da utilização da internet.

Com a cobertura mais compreensiva e eficaz da Internet do mundo, é simples para um administrador criar políticas de acesso à web que são especificamente concebidas para ir ao encontro dos requisitos legais e de conformidade. A classificação rigorosa inicial significa que serão necessárias apenas pequenas reclassificações, reduzindo o suporte necessário aos colaboradores.

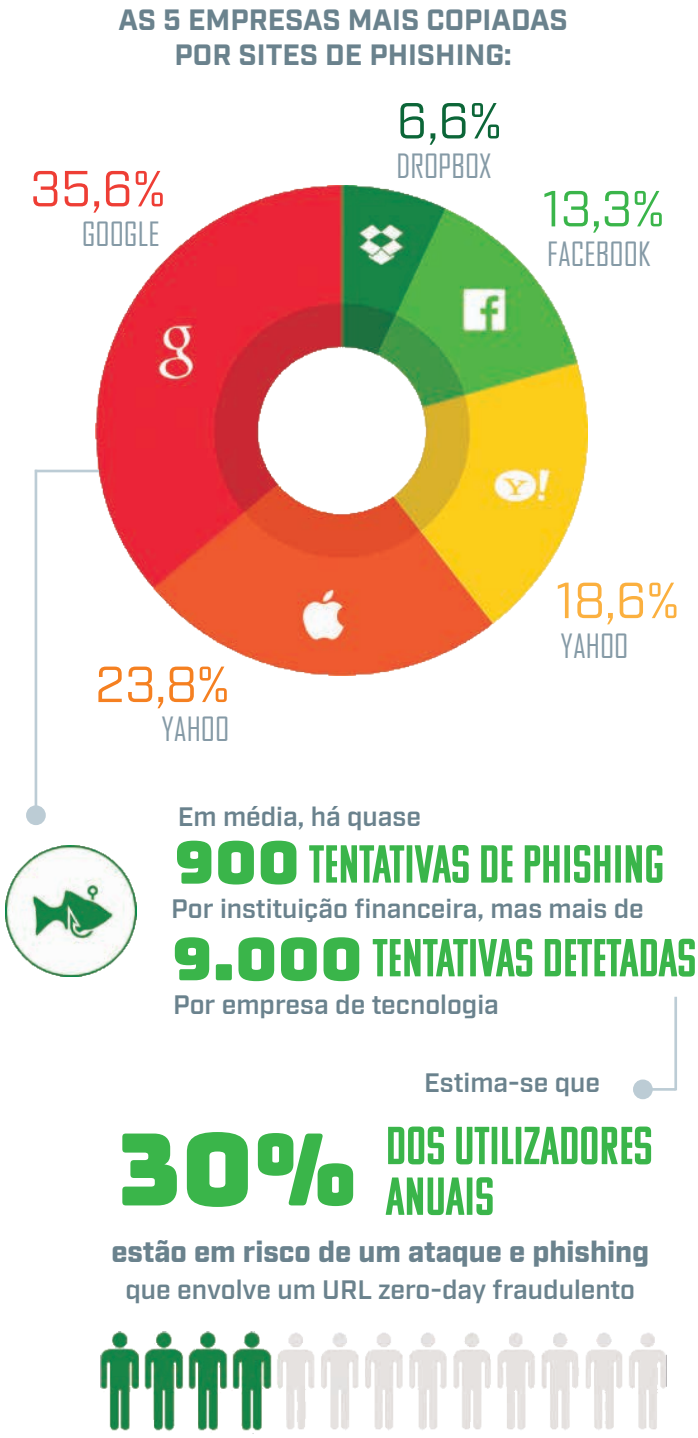
Proteção única e em tempo real contra phishing

Os ataques de phishing e de spear phishing que ocultam URLs da internet e tentam roubar informação sensível aos utilizadores são a tática mais bem sucedida dos cibercriminosos para entrarem na rede das empresas. Um estudo do Webroot mostrou que 30% dos seus utilizadores web estavam em risco de um ataque de phishing ou spear phishing.

O Webroot SecureAnywhere® Web Security Service utiliza uma avaliação de propriedade única e em tem real, para garantir que os utilizadores estão sempre ligados a websites genuínos e não a interagir com sites de phishing.

Para além disso, para mitigar as perdas de dados e proteger os utilizadores contra conteúdos inapropriados, podem ser ativados filtros baseados nas aplicações web, tipos de ficheiros, tamanho do ficheiro e outros.

30% dos utilizadores acedem a URLs de phishing ou suspeitos



Agente inviolável

Os utilizadores mais engenhosos tentam, muitas vezes, contornar a monitorização utilizando proxys. Tal como outras ameaças de segurança web, os sites proxy são bloqueados pelas políticas de filtragem de URLs, mas podem aparecer tão rapidamente que podem mesmo assim conseguir contornar a monitorização.

A tecnologia de propriedade Webroot é concebida especialmente para parar qualquer tentativa de ultrapassagem as políticas de controlo, identificando mesmos os sites proxys mais recentes

MINIMIZAÇÃO DA COMPLEXIDADE DA GESTÃO

Um dos principais objetivos do Webroot Web Security Service é a minimização da complexidade associada à gestão da segurança web (particularmente para organizações com múltiplas localizações e/ou uma grande força móvel), melhorando a segurança e a visibilidade dos utilizadores, aplicando políticas de controlo flexíveis e reduzindo os custos operacionais.

Este serviço disponibiliza uma consola de gestão baseada em cloud, segura e centralizada, disponível onde quer que esteja, através de um browser web. Foi desenvolvida para ser intuitiva e simples de utilizar, facilitando a gestão e aplicação das políticas de controlo granular. Acesso em qualquer momento e local à consola para configuração, gestão de utilizadores, reporting e gestão de políticas, assim como atribuição de permissões de acesso baseadas nas funções dos colaboradores.

Gestão Web simplificada

A abordagem de segurança web baseada em cloud permite uma visibilidade total dos utilizadores, independentemente da localização, com um maior descanso na gestão, que não é normalmente encontrado nas soluções on-premise. Ao contrário da abordagem on-premise, o Webroot não obriga os utilizadores a utilizar uma VPN para aceder à web através da network, reduzindo a sua performance. Em vez disso, os utilizadores podem autenticar-se em qualquer local, eliminando os custos excessivos de configuração de segurança web em vários escritórios.

Sem segurança web baseada em cloud, o crescente uso da internet para aceder a aplicações empresariais, o dramático aumento dos acessos e trabalho remotos e a utilização de vários dispositivos móveis para acesso à rede podem tornar-se problemáticas para os administradores de IT.

Para além do enorme risco de infeções, o problema que hoje enfrentamos é como devemos proteger os utilizadores e aplicar políticas de utilização web, mantendo a produtividade e os benefícios associados à utilização da internet.

Controlo Granular

A proteção contra malware é um dado adquirido, mas a gestão da segurança web também significa ser capaz de filtrar os conteúdos que entram e saem da empresa. Significa ainda conseguir controlar (até ao nível do utilizador individual, se necessário), através de filtros URL, as categorias do website que o colaborador pode, ou não, aceder.

No entanto, uma granularidade real permite ainda implementar políticas que delimitem quanto tempo por dia - e quando - o colaborador pode aceder a certas categorias do site. Para ainda mais flexibilidade, o administrador pode ainda bloquear certos websites, mas permitir que os utilizadores os desbloqueiem.
No que toca às redes sociais, é possível definir que aplicações são permitidas num determinado site e quando são permitidas, assegurando que a utilização é apropriada e a produtividade é mantida.

Serviço garantido, com suporte de excelência

Uma das principais diferenças na aquisição de uma solução de segurança web baseada em cloud é que não existe nem software nem hardware on-premise. A manutenção operacional normal dos updates de segurança, patching e suporte de hardware ficam também obsoletos. Não há necessidade de de poupar para uma solução de alta disponibilidade ou de disaster recovery, visto que já estão incluídas com as soluções de segurança cloud do Webroot.

O Webroot oferece ainda o Service Level Agreement (SLA), que analisa o tempo de atividade do serviço, a deteção de vírus e spyware conhecidos, tempos de resposta em caso de falha no serviço, tempo para aplicação de políticas e outras salvaguardas necessárias quando a infraestrutura IT é gerida por terceiros, em vez de pela empresa.

O Webroot Security Services também oferecem os melhores standard de SLA e tempos de resposta do suporte da indústria.

Logging inviolável e gestão de relatórios agendada

Como a utilização web pode envolver questões legais, de conformidade com regulamentos e ações disciplinares de utilizadores, é vital que sejam mantidos relatórios completos do tráfego web dos utilizadores e administradores, quando utilizam a consola web.

O Webroot SecureAnywhere® Web Security Service elabora os dois relatórios e, ao contrário do que acontece com muitas outras gateways de segurança web, ficam instantaneamente disponíveis durante 12 meses, evitando demoras no reporting ou nas investigações. Este serviço oferece ainda log reporting e exportação para SIM/SIEMS.

Dada a visibilidade disponibilizada pelo Webroot SecureAnywhere® Web Security Service, gerentes individuais, ITs e outros departamentos podem ver e compreender o comportamento dos utilizadores online, através dos relatórios disponibilizados pela management console. Para poupar tempo e esforço, os relatórios criados podem ser guardados, para que não seja necessário recriá-los todas as vezes. Podem ainda ser atribuídos, agrupados e enviados para uma lista de circulação pré-determinada em períodos de tempo fixos. Toda esta automação minimiza o tempo gasto na administração e a gestão dos relatórios é mais oportuna e padronizada.

RISCO OPERACIONAL REDUZIDO

Existem alguns riscos operacionais consideráveis associados à segurança web. Alguns utilizadores ressentem a monitorização, uma vez que evita que tenham comportamentos inapropriados ou percam tempo em período laboral. Por estas razões, procuram formas de contornar as políticas de segurança, o que representa riscos elevados de segurança e de conformidade.

O Webroot SecureAnywhere® Web Security Service foi especificamente concebido para evitar as tentativas destes colaboradores e assegurar que todo o tráfego web é direcionado, monitorizado e reportado através do serviço de segurança web.

Isto é também importante para reduzir os custos operacionais com utilizadores remotos e garantir a conformidade.

Desktop Web Proxy

Uma das principais formas como o Webroot reduz custos operacionais e evita o contorno das políticas é através da configuração do agente Desktop Web Proxy (DWP). Esta funcionalidade fácil de instalar e inviolável assegura que todos os colaboradores são direcionados pelo Web Security Service.
Autentica com transparência os utilizadores, ajuda-os a utilizar de forma inteligente hotspots em hotéis e outras situações complexas de login, para além de impedir que os utilizadores remotos adulterem as configurações do navegador.

Global Secure Datacenter Network

Outra forma como o Webroot corta os custos operacionais para os seus clientes é através da arquitetura de bases de dados globais (principalmente a Amazon Web Services), extremamente escalável e resiliente, com que trabalha e, através do qual, funcionam o serviço de segurança web Webroot SecureAnywhere®. Estas bases de dados trabalham numa base totalmente redundante por isso, mesmo na eventualidade de uma falha total do data center, o Webroot SecureAnywhere® Web Security Service continua a funcionar através de todas as outras bases de dados secundárias. Este nível de redundância e arquitetura IT escalável permite fornecer um tempo de atividade ao nível de uma operadora.

Para além de operar em data centers altamente seguros, o Webroot faz o controlo rigoroso dos acessos, realiza regularmente testes de penetração e ainda credenciou e auditou o serviço de segurança web para SAS70 Type II.

Dashboard personalizado de segurança web

Ter a capacidade de visualizar instantaneamente o que está a ocorrer a nível da utilização web é uma forma extremamente útil de reduzir os custos operacionais associados à segurança web. O Webroot SecureAnywhere® Web Security Service disponibiliza aos administradores um painel de controlo personalizável que lhes permite ver rapidamente o estado da utilização da internet na empresa e o impacto que esta utilização esta a ter a nível da banda larga e outras métricas chave.

COMO É QUE A SEGURANÇA BASEADA EM CLOUD COMPLEMENTA A SEGURANÇA ENDPOINT?

Uma questão frequentemente colocada é: 'Se já tenho segurança endpoint, porque é que preciso de uma gateway de segurança web?'

Esta questão é compreensível, no entanto, assume que a segurança endpoint deveria ser a primeira e última linha de defesa. Enquanto a segurança endpoint possibilita vários níveis de proteção contra ameaças e, em alguns casos, alguns controlos de acesso, as defesas são básicas e nunca destinadas a oferecer o nível ou camadas de segurança encontrada numa gateway de segurança web dedicada.

De facto, confiar apenas na segurança endpoint está a agravar os problemas de segurança. Está a aceitar que o malware entre na sua rede antes de o eliminar.

Ameaças da internet

Desde 2015, o Webroot tem publicado relatórios intitulados Threat Brief-Insights from Collective Threat Intelligence. Referia que o Webroot verificou um aumento contínuo no número de URLs maliciosos, endereços IP, malware e apps móveis utilizadas pelos cibercriminosos para roubar dados sensíveis, interromper serviços, ou causar outros tipos de prejuízo. O número de ataques a retalhistas, instituições financeiras e empresas de tecnologia tem crescido nos últimos anos e esta tendência não mostra sinais de diminuição.

Seguem-se alguns infográficos dos resultados:

1/3
dos IPs maliciosos são **dos Estados Unidos**

1/2
do total de IPs maliciosos têm **base na Ásia**

Atacantes em países de alto risco escolhem países de confiança para hospedar os seus sites maliciosos

Os 10 países com mais URLs maliciosos

5 categorias mais utilizadas para URLs de alto risco

01	02	03	04	05
Negócios e economia	Sociedade	Compras	Viagens	Saúde e medicina

16,8% São suspeitos
Sites com cartões de boas vindas têm maior risco de serem suspeitos

No que toca malware na internet, a maioria das estatísticas e dados obtidos através de fornecedores de segurança como parte de updates genéricos de segurança e pesquisa específica relacionada com a oferta da tecnologia de gateway web secure.

Não se pode negar, após toda esta pesquisa, que o uso diário da internet é um alto risco.

10 principais categorias de URLs suspeitos e de alto risco

1. URLs com SPAM
2. Sites de malware
3. Negócios e economia
4. Prevenção de proxy e anonimizadores
5. Phishing e outras fraudes
6. Sociedade
7. Compras
8. Viagens
9. Saúde e medicina
10. Entretenimento e artes

Algumas estatísticas do Threat Brief

- 85.000 Novos endereços IP maliciosos são surgem todos os dias.
- Menos de 55% de todos os URLs são de confiança.
- Do top 10 das categorias de sites mais visitados pelos clientes Webroot, 6 apareceram também no top 10 dos URLs suspeitos e de alto risco.
- 30% Dos utilizadores da internet acedem a sites de phishing.
- 15% Dos novos ficheiros são executáveis maliciosos.

CONCLUSÃO

Ainda existem muitas organizações sem uma gateway web segura, que confiam apenas na segurança endpoint para parar malware, ou utilizam soluções on-premise mais antiquadas, que apenas respondem parcialmente às necessidades atuais de controlo da utilização web e de segurança.

Considerando que uma empresa se depara com cerca de 5.00 ameaças de malware em apenas um mês e que muitas delas não são detetadas por antivírus endpoint convencionais, é claro o porquê da internet ser o risco de segurança número um e a relevância do serviço de segurança web Webroot SecureAnywhere®, cuja segurança preventiva protege empresas de todas as dimensões e setores.

A segurança de gateway web possibilita diferentes verificações, controlos e análises, oferecendo uma camada de segurança adicional e complementar, essencial para a postura de segurança que as empresas devem ter atualmente.

SOBRE O WEBROOT

O Webroot disponibiliza soluções Smarter Cybersecurity™. Oferece soluções de segurança endpoint e serviços de inteligência de ameaças para garantir a segurança da Internet of Everything.

Aproveitando a plataforma de inteligência de ameaças, tanto computadores, como tablets, smartphones e outros estão protegidos contra malware e outros ciberataques.

A solução premiada SecureAnywhere™ e os serviços BrightCloud® threat intelligence protegem dezenas de milhões de consumidores, empresas e dispositivos empresariais.

A tecnologia Webroot é escolhida por inúmeras empresas líderes de mercado, incluindo a CISCO, F5 Networks, Microsoft, Palo Alto Networks, RSA, Arruba e muitas outras.

O Webroot esá sediado nos Estados Unidos mas tem subsidiárias na Europa, América do Norte e região Ásia-Pacífico.