BLUE COAT®

A segurança fortalece os negócios

APPLIANCE PARA ANÁLISE DE MALWARE

FOLHA DE DADOS

SANDBOXING HÍBRIDO PARA DETECÇÃO E ANÁLISE DE MALWARE AVANÇADO E DESCONHECIDO

Appliance para análise de malware

O Appliance para análise de malware da Blue Coat é um componente essencial do Security & Policy Enforcement Center (Centro de aplicação de políticas e segurança) da Blue Coat. Integrado ao Sistema de análise de conteúdo da Blue Coat, ele fecha a lacuna entre o bloqueio de malware conhecido e a detecção e análise de malware desconhecido e avançado.

O appliance personalizável oferece análise abrangente e detonação de malware com uma abordagem de detecção dupla que permite analisar arquivos suspeitos e reduzir o impacto de ameaças de dia zero e malware desconhecido.

Abordagem de detecção dupla: A melhor maneira para detectar mais comportamentos maliciosos

O Appliance para análise de malware utiliza uma abordagem poderosa de detecção dupla que combina os benefícios de emulação de código com introspecção de máquina virtual. Essa abordagem captura mais comportamentos maliciosos em uma gama maior de ambientes personalizados do que outras soluções que tipicamente dependem de uma única metodologia. A abordagem de detecção dupla inclui:

- Sandbox® – Um ambiente bare-metal que emula um sistema real para detectar malware que, de outra maneira, não detonará em um ambiente virtualizado.
- IntelliVM – Perfis de máquinas virtuais que replicam ambientes reais de produção, incluindo aplicações personalizadas, para identificar rapidamente anomalias e diferenças em comportamento que revela antianálise e outras técnicas de evasão de malware avançado.

Sistemas simulados: Detonação para malware evasivo

A tecnologia exclusiva de sandboxing simula ambientes de bare-metal para detectar malware evasivo. O Appliance de análise de malware utiliza detonação de malware para executar arquivos dentro do simulador como se estivessem em um sistema real, sem código de execução na CPU direcionada, carregando em memória real ou comunicando com outros componentes de sistema físico.

Trabalhando no nível de kernel, o emulador coloca o malware em ação, interceptando o comportamento e convertendo-o em informações de perícia de passo a passo. Sem nunca colocar os sistemas reais em risco, a tecnologia de sandboxing proporciona um mapa do dano que a ameaça causaria se tivesse permissão para executar em uma máquina real.

Ambientes virtuais personalizados para detecção mais rápida de anomalia

Com a tecnologia IntelliVM, o Appliance para análise de malware usa perfis de máquinas virtuais para espelhar diferentes tipos de ambientes personalizados. Desse modo, é possível detectar rapidamente anomalias e diferenças em comportamento que revelam técnicas de evasão de malware avançado. O Appliance para análise de malware monitora uma ampla gama de eventos de sistema para verificar sinais de comportamento malicioso em um ambiente virtualizado seguro e instrumentado.

Os perfis do IntelliVM podem ser personalizados para adicionar flexibilidade quando malwares não tradicionais são analisados e para espelhar com precisão os ambientes de produção a fim de detectar malware avançado e ataques direcionados. Os analistas de segurança podem analisar todos os tipos de ameaças, em qualquer versão de qualquer aplicação que escolherem. Eles são capazes de combinar com precisão os ambientes de computadores desktop de suas organizações, reunindo informações sobre malwares que visam essas organizações específicas e que podem estar em busca de explorar certas vulnerabilidades de aplicações.

Informações de ameaças compartilhadas: Operacionalize conhecimentos aprendidos para fortificar a infraestrutura de segurança

Depois que um malware avançado ou desconhecido e ameaças de dia zero são detonados, as novas informações de ameaças são compartilhadas localmente por toda a infraestrutura de segurança bem como com todos os 15 mil clientes da Blue Coat e os 75 milhões de usuários em todo o mundo por meio de uma Rede de informações globais. Transformar ameaças desconhecidas em ameaças conhecidas e compartilhar essas informações por toda a infraestrutura de segurança aumenta a escalabilidade e a eficácia da defesa ao mover a proteção para gateways de Web segura do Blue Coat ProxySG.

BLUE COAT®

A segurança fortalece os negócios

Benefícios do Appliance para análise de malware

- **Análise superior e precisão –** Abordagem exclusiva de detecção dupla combina sandboxing com o IntelliVM para oferecer detecção inigualável de malware e ameaça. A classificação automática de amostra e a pontuação de risco por maior padrão correspondente juntamente com suporte para fluxos de trabalho de análise de malware existentes permitem trabalhar nos eventos de sistema detectados com base em atividade maliciosa potencial.
- **Facilidade de uso e alertas –** A comunicação de incidentes em tempo real com análise detalhada do evento proporciona notificação imediata para analistas de segurança, enquanto uma interface de usuário aprimorada baseada na Web permite a interação com o malware e a capacidade de clicar em instaladores. O painel baseado na Web permite a realização de buscas simples das informações de malware e banco de dados de coleta, armazenamento de amostras, relatórios e eventos.
- **Arquitetura e desempenho dimensionáveis** Processamento de centenas de milhares de arquivos por dia com processamento paralelo de amostras em até 55 máquinas virtuais por cada Appliance para análise de malware. Múltiplas VMs com SOs Windows XP e Windows 7 e configurações ilimitadas de software são compatíveis.

SÉRIE DE APPLIANCE PARA ANÁLISE DE MALWARE	MAA S400-10	MAA S500-10
DESEMPENHO		
Amostras de malware	12.000 amostras por dia	50.000 amostras por dia
SISTEMA		
Unidades de disco	2 x 500GB	6 x 1TB
RAM	32GB	96GB
Portas on-board	(2) portas 1000Base-T de cobre (1) porta 1000Base-T de cobre, para gerenciamento de sistema (1) porta 1000Base-T de cobre, para gerenciamento de BMC	(2) portas 10 Gb Base-T de cobre (1) porta 1000Base-T de cobre, para gerenciamento de sistema (1) porta 1000Base-T de cobre, para gerenciamento de BMC
NICs opcionais	2 x 10 GB Base-T de cobre	
Fontes de alimentação	2	2

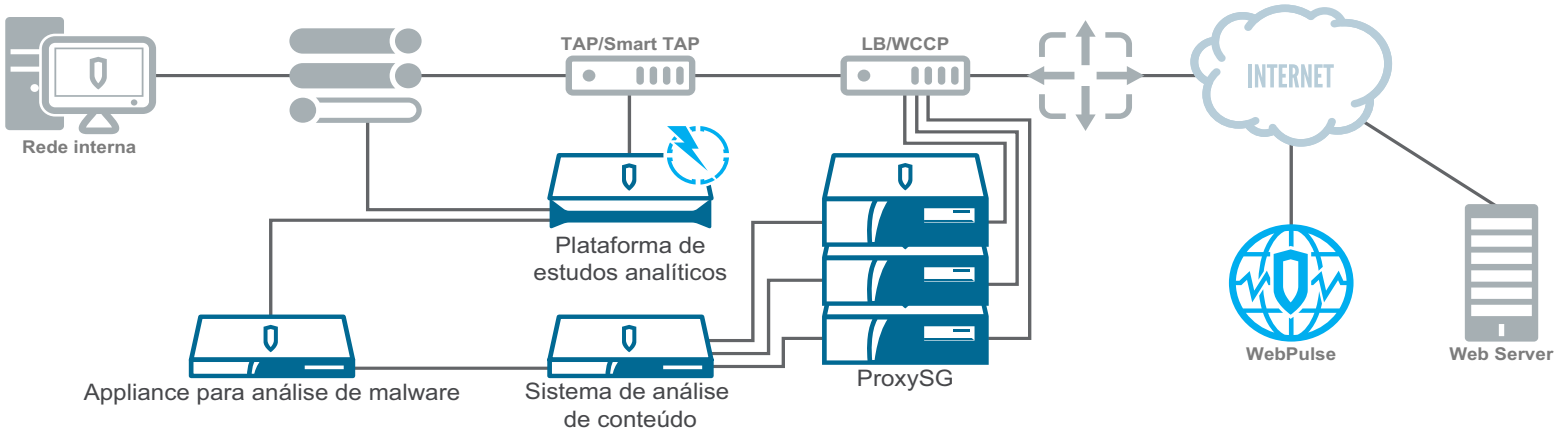
PROPRIEDADES FÍSICAS	MAA S400-10	MAA S500-10
DIMENSÕES E PESO		
Dimensões	572 mm x 432,5 mm x 42,9 mm (22,5 pol. x 17,03 pol. x 1,69 pol.) (somente o chassi) 643 mm x 485,4 mm x 42,9 mm (25,3 pol. x 19,11 pol. x 1,69 pol.) (chassi c/ extensões) Altura 1 RU	710 mm x 433,3 mm x 87,2 mm (27,95 pol. x 17,05 pol. x 3,43 pol.) (somente o chassi) 812,8 mm x 433,4 mm x 87,2 mm (32 pol. x 17,06 pol. x 3,43 pol.) (chassi c/ extensões) Altura 2 RU
Peso (máximo)	Aprox. 12,8 kg (28 lb) +/- 5 %	Aprox. 30 kg (66,12 lb) +/- 5 %
AMBIENTE OPERACIONAL		
Alimentação	Fontes de alimentação duplas redundantes com hot-swap, alimentação CA 100 - 127 V a 8 A, 200 - 240 V a 4 A, 47 - 63 Hz (alimentação CC disponível)	Fontes de alimentação duplas redundantes com hot-swap, alimentação CA 100 - 240 V, 50 - 60 Hz, 12 - 5 A (alimentação CC disponível)
Potência máxima	450 Watts	1100 Watts
Classificação térmica	Típico 1086 BTU/Hr, Máx. 1381 BTU/Hr.	Típico 2598,42 BTU/Hr, Máx. 3751 BTU/Hr.
Temperatura	5 °C a 40 °C (41 °F a 104 °F) no nível do mar	
Umidade	20% a 80% de umidade relativa, sem condensação	
Altitude	Até 3.048 m (10.000 pés)	

BLUE COAT®

A segurança fortalece os negócios

PARA TODOS OS APPLIANCES PARA ANÁLISE DE MALWARE

REGULAMENTAÇÕES	SEGURANÇA	CONFORMIDADE ELETROMAGNÉTICA (EMC)
Internacional	CB – IEC60950-1, Segunda edição	CISPR22, Classe A; CISPR24
EUA	NRTL – UL60950-1, Segunda edição	FCC parte 15, Classe A
Canadá	SCC – CSA-22.2, Nº 60950-1, Segunda edição	ICES-003, Classe A
União Europeia (CE)	CE – EN60950-1, Segunda edição	EN55022, Classe A; EN55024; EN61000-3-2; EN61000-3-3
Japão	---	VCCI V-3, Classe A
México	NOM-019-SCFI por Declaração NRTL	---
Argentina	S Mark – IEC 60950-1	---
Taiwan	BSMI – CNS-14336-1	BSMI – CNS13438, Classe A
China	CCC – GB4943.1	CCC – GB9254; GB17625
Austrália/Nova Zelândia	AS/NZS 60950-1, Segunda edição	AS/ZNS-CISPR22
Coreia	---	KC – RRA, Classe A
Rússia	CU - IEC 60950-1	GOST-R 51318.22, Classe A; 51318.24; 51317.3.2; 51317.3.3
AMBIENTAL	Diretiva RoHS 2011/65/EU, Regulamento REACH Nº 1907/2006	
GARANTIA DO PRODUTO	Garantia limitada e intransferível de hardware por um período de um (1) ano a contar da data de expedição. Contratos de suporte BlueTouch disponíveis para atendimento 24 horas por dia, 7 dias por semana, para software com opções de suporte para hardware.	
CERTIFICAÇÕES GOV.	Para mais informações sobre certificação governamental, entre em contato com Federal_Certifcations@bluecoat.com.	
MAIS INFORMAÇÕES	Entre em contato com regulatoryinfo@bluecoat.com para esclarecer dúvidas específicas e obter suporte sobre certificação de conformidade regulatória.	



Arquitectura de referencia de protección contra amenazas avanzadas de Blue Coat.

Blue Coat Systems Inc.
latam.sales@bluecoat.com

Sede Corporativa
Sunnyvale, CA USA
+1.408.220.2200

Blue Coat Brasil
São Paulo
+55 11 3443 6879

Blue Coat México
México D.F.
+52 55 3300 5825

Blue Coat Argentina
Buenos Aires
+54 (11) 4850 1215