minitel NEXT CYBERSECURITY

ThreatDown

Powered by Malwarebytes

BASES DE INTELIGÊNCIA

EP - ENDPOINT PROTECTION

Refere-se a soluções de segurança que protegem dispositivos individuais, como computadores, servidores, laptops e dispositivos móveis, dentro da rede corporativa. Estes dispositivos são pontos vulneráveis a ciberataques. O EP detecta, bloqueia e elimina ameaças diretamente nos dispositivos, como vírus, malware e ransomware. Utiliza tecnologias como análise comportamental, deteção de anomalias e assinaturas de malware para identificar e neutralizar as ameaças antes que se espalhem pela rede.

EDR - ENDPOINT DETECTION AND RESPONSE

A Deteção e Resposta em Pontos Finais (EDR) vai além da simples proteção de dispositivos. Trata-se de uma abordagem mais avançada que não só deteta e responde a ameaças em tempo real, mas também permite a análise forense para entender como o ataque ocorreu e como se espalhou.

MDR - MANAGED DETECTION AND RESPONSE

É um serviço de segurança cibernética avançado que combina monitorização contínua e resposta imediata a ameaças, gerido por uma equipa especializada.

COMO VAI AJUDAR A PROTEGER OS VOSSOS CIENTES:

- **Prevenção de ataques locais:** Impede que malware infecte dispositivos individuais e se propague pela rede.
- **Redução de riscos:** Minimiza a possibilidade de danos e roubo de dados de dispositivos comprometidos.
- **Fácil gestão:** As soluções de EP são muitas vezes fáceis de implementar e gerenciar, mesmo para pequenas e médias empresas.

- **Isolamento de ataque** - A única solução que isola todos os três níveis:
- **Rede** - Limita as comunicações do dispositivo e impede que o malware “comunique com a sua base”.
- **Processo** – Interrompe o malware, o que acaba por manter a produtividade dos colaboradores.
- **Ambiente de trabalho** – Bloqueia acessos por login e mantêm os dispositivos online para análise.

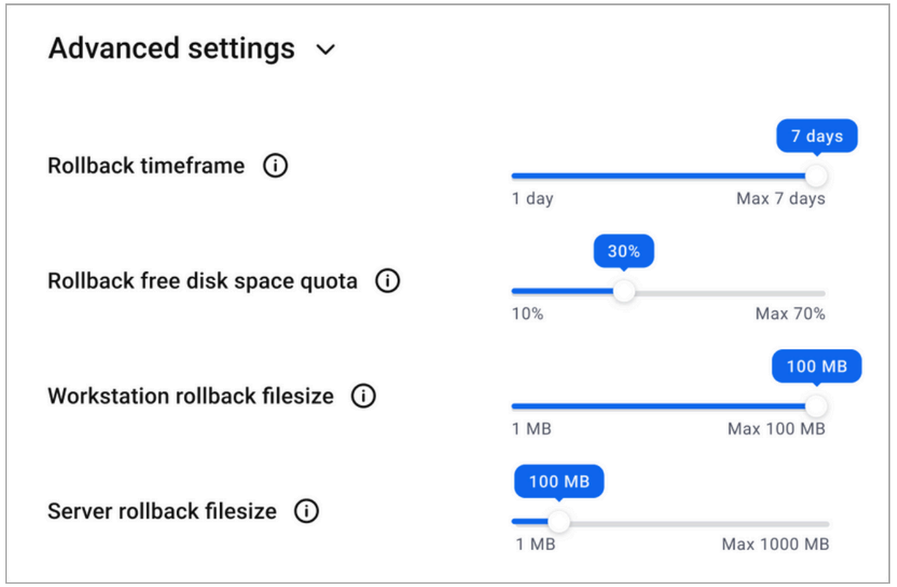
- **Deteção Proativa:** Identificação de ameaças em tempo real com tecnologias avançadas.
- **Resposta Imediata:** Ações rápidas para mitigar riscos e bloquear ataques.
- **Monitorização 24/7:** Garantia de segurança constante, mesmo sem equipa interna.
- **Análise de Incidentes:** Investigação detalhada para entender e prevenir futuros ataques.
- **Relatórios e Conformidade:** Relatórios sobre incidentes, ajudando na conformidade com normas como o RGPD.

EDR - ENDPOINT DETECTION & RESPONSE

DETETAR COM PRECISÃO
Identificar ameaças maliciosas e suspeitas

RESPONDE IMEDIATAMENTE
Isolar utilizadores, pontos finais e redes para impedir ataques.

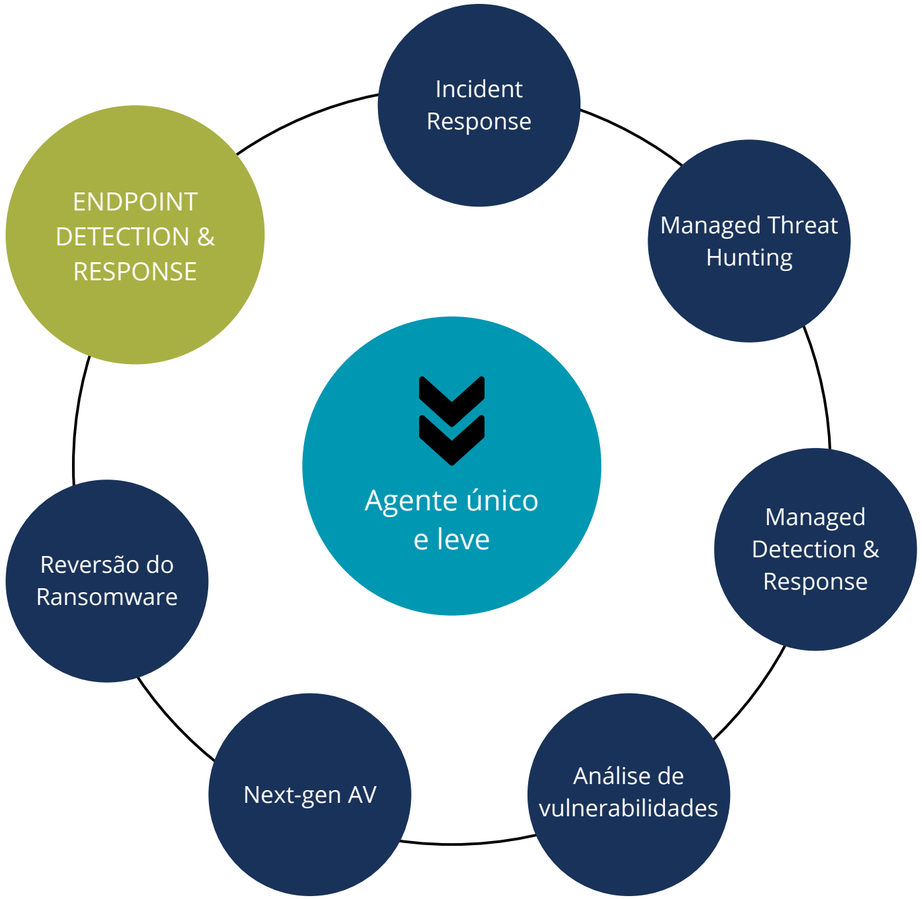
REMEDIAR TOTALMENTE
Retorne os endpoints ao estado íntegro e evite a reinfecção

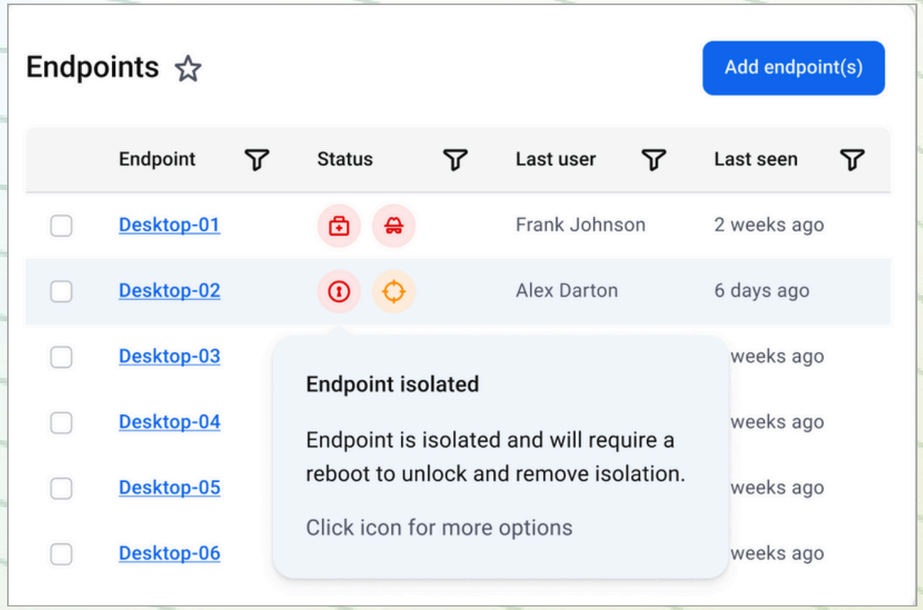


RANSOMWARE ROLLBACK

Restaure ficheiros que foram encriptados, eliminados ou modificados até 7 dias após um ataque. O seu Linking Engine patenteado elimina todos os vestígios de malware, artefactos e alterações de configuração, devolvendo os dispositivos dos clientes a um estado íntegro e prevenindo a reinfeção por ransomware.

EDR - ENDPOINT DETECTION & RESPONSE



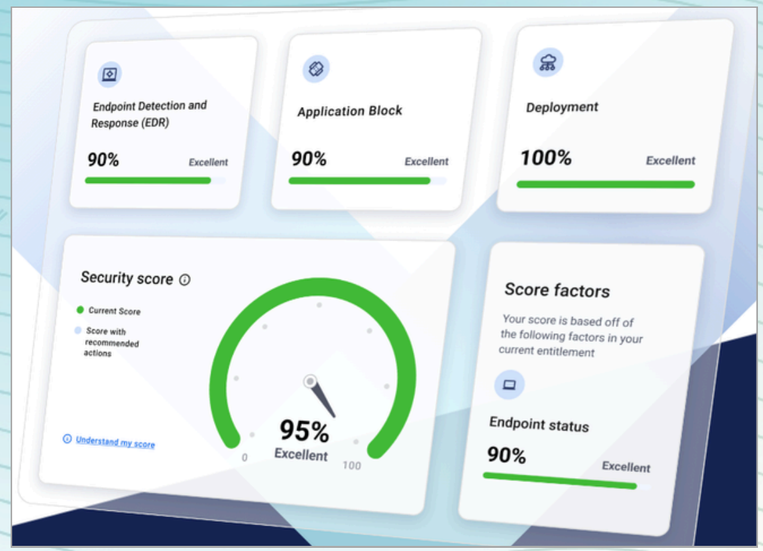


AGENTE ÚNICO E LEVE

O nosso agente simplifica a sua segurança, reduz custos, é implementado facilmente em minutos sem necessidade de reiniciar e não torna o seu sistema mais lento.

MDR: MANAGED DETECTION & RESPONSE

Implemente monitorização, investigação e correção de ameaças geridas 24x7x365 pela equipa de analistas da Threatdown, especializados em MDR para proteger a sua organização. É um serviço extra que vai remediar todos os sinais dados pelo EDR.

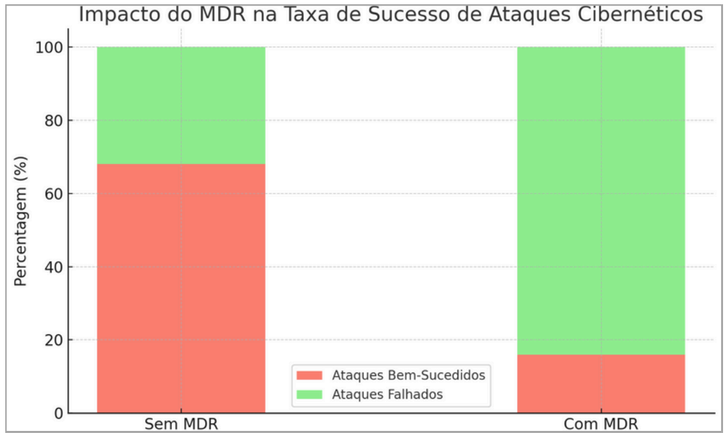


Redução de ataques bem-sucedidos:

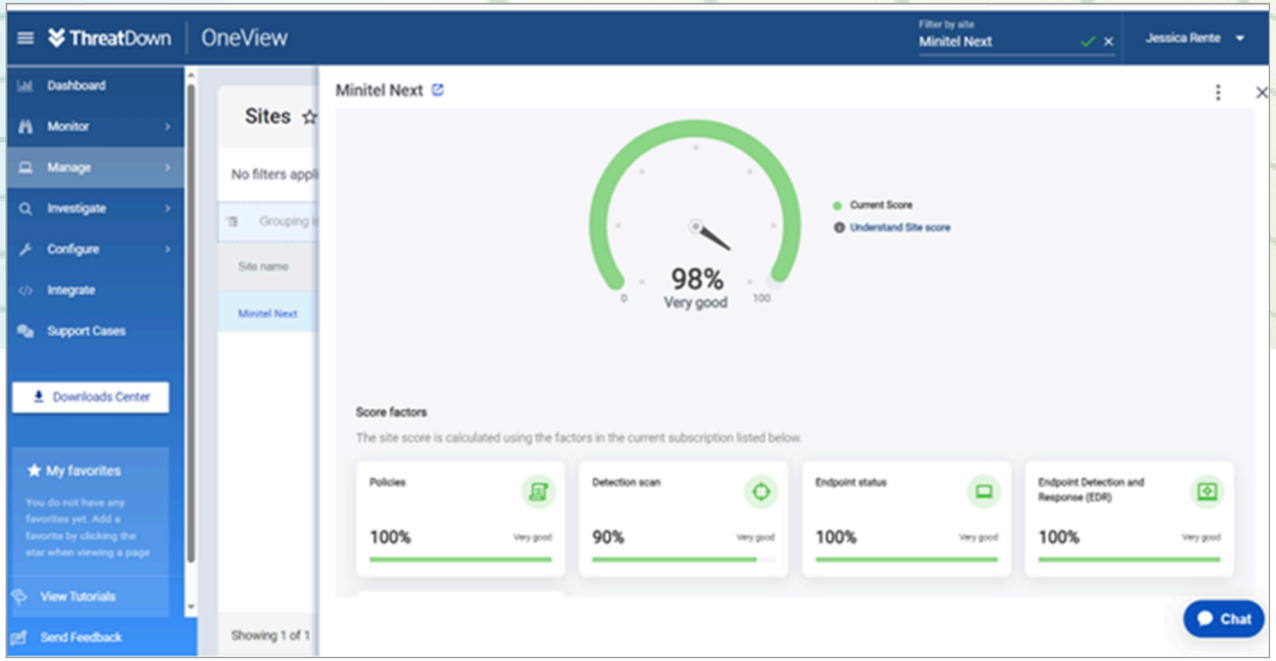
- **Sem MDR:** Cerca de 68% dos ataques são bem-sucedidos devido a detecção tardia ou resposta inadequada.
- **Com MDR:** Apenas 16% dos ataques conseguem atingir o alvo, com os outros 84% sendo neutralizados.

Melhoria no tempo de detecção e resposta:

- **Sem MDR:** O tempo médio para identificar uma ameaça é superior a 200 dias.
- **Com MDR:** As ameaças são detectadas e respondidas em menos de 24 horas, em média.



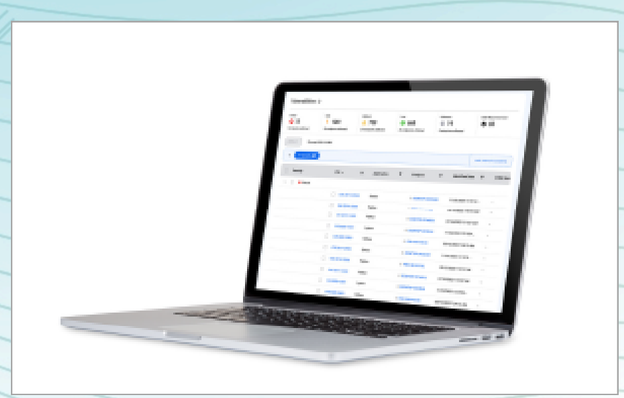
SECURITY ADVISOR

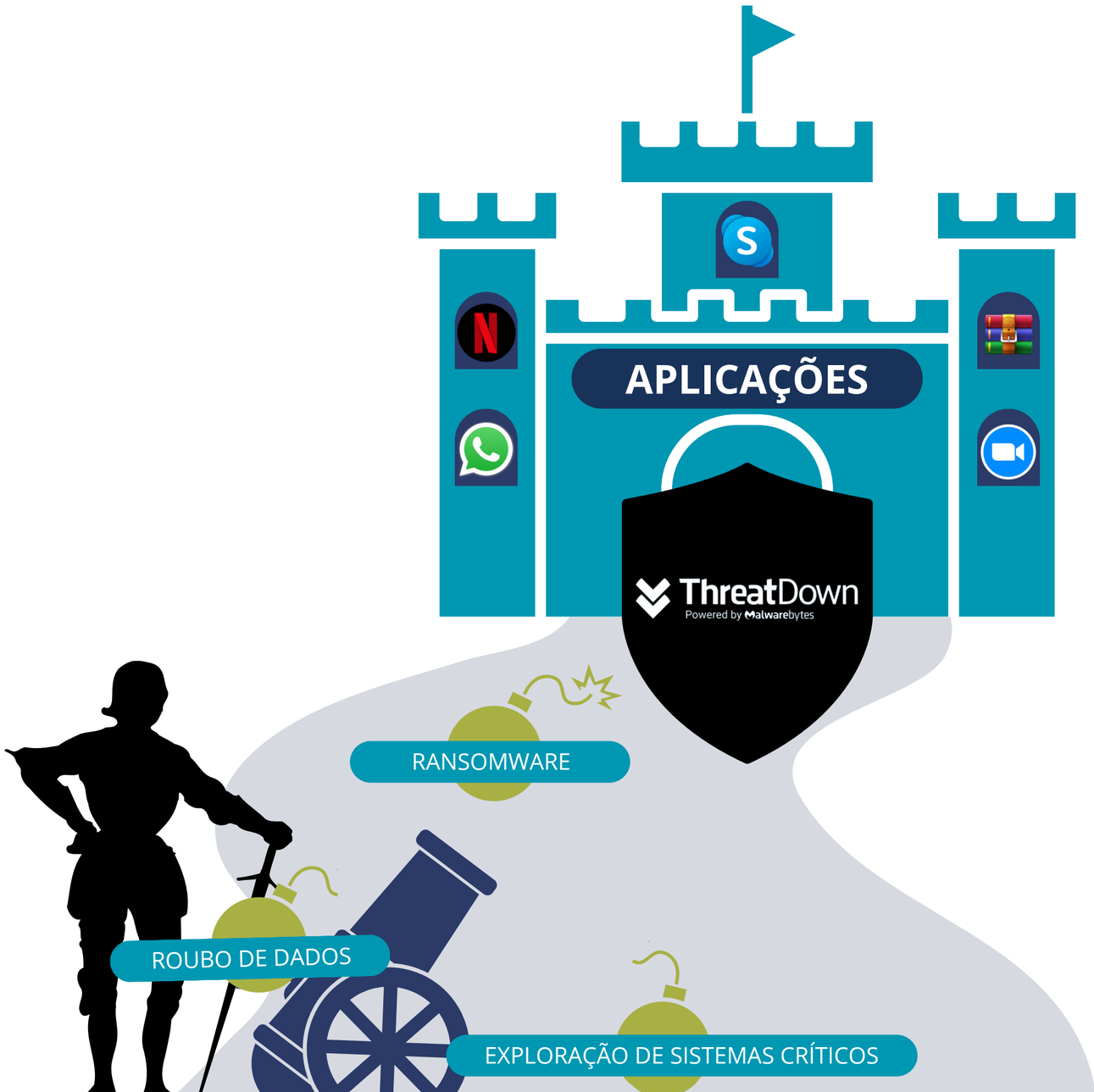


- Classificação de segurança rápida
- Foco nos problemas
- Sugestão instantânea com implementação

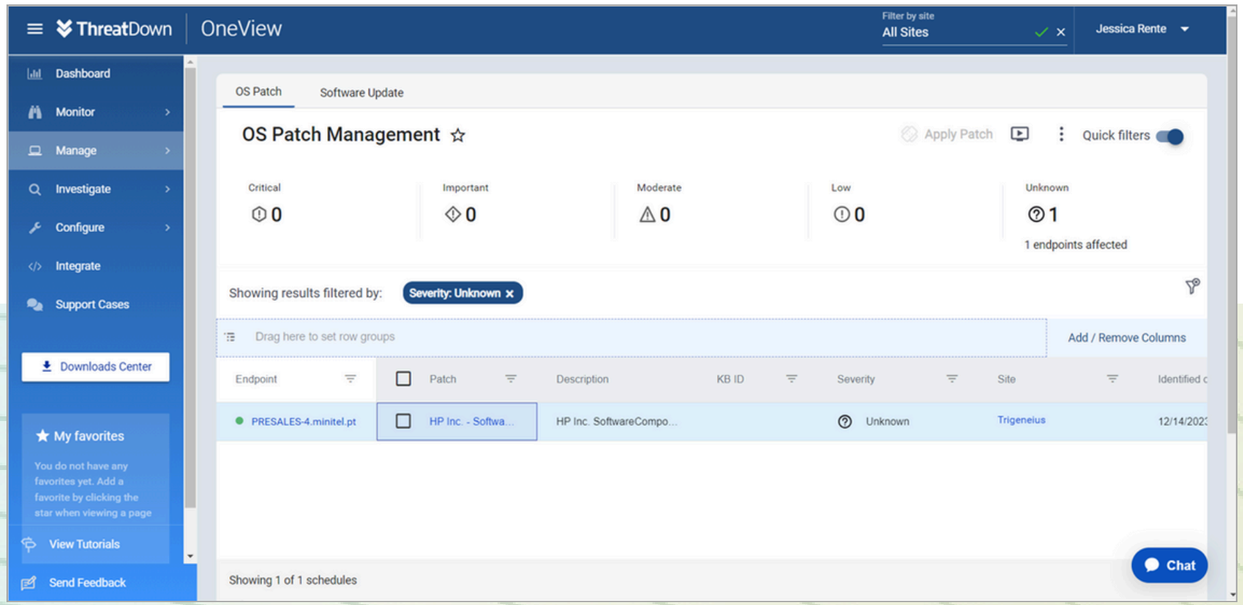
ANÁLISE DE VULNERABILIDADES

- Identifique vulnerabilidades críticas
- Avalie aplicações legadas e modernas
- Compreenda a prioridade no seu ecossistema
- Conhecimento para agir
- Atualizamos a sua aplicação





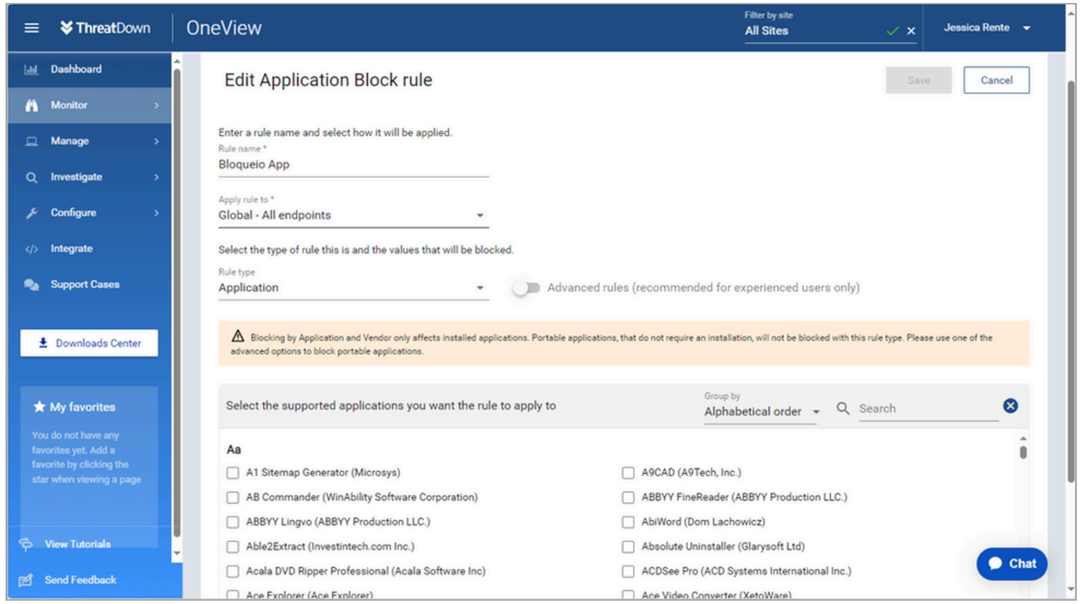
PATCH MANAGEMENT



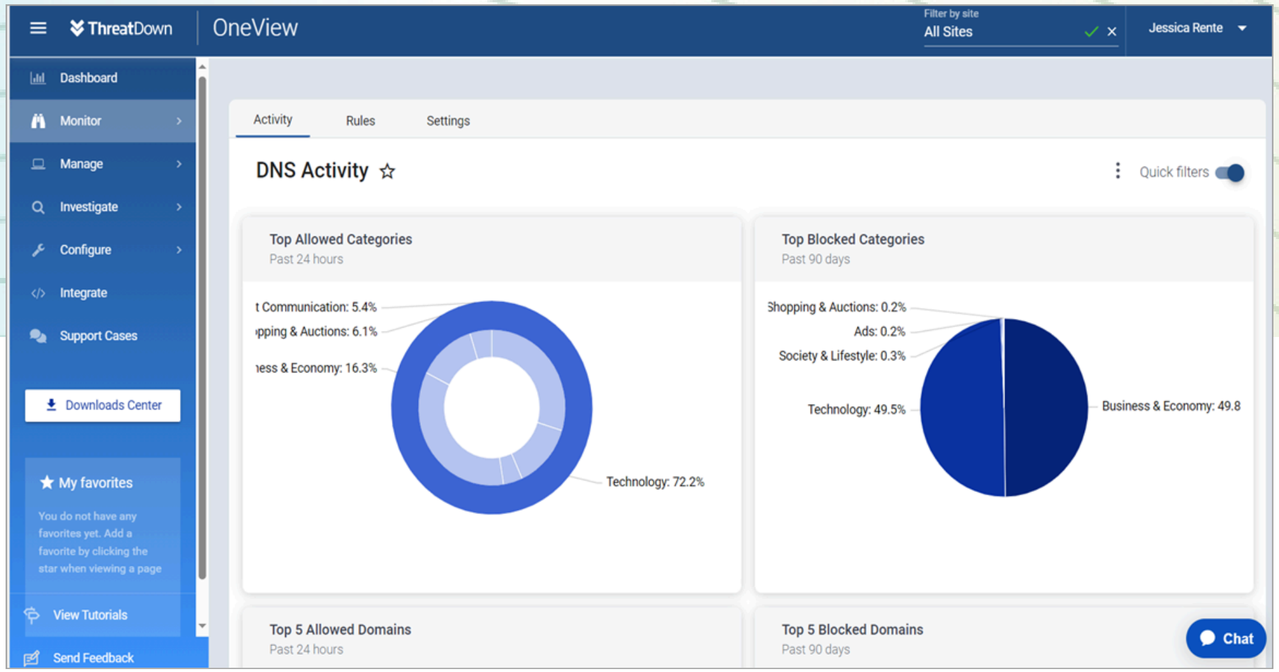
- Simplifique o processo de aplicação de patches
- Definir e priorizar a implantação
- Catálogo aplicações continuamente atualizado
- Patches simultâneos, imediatos e programados

APPLICATION BLOCK

- Controlo para impedir a utilização de aplicações não autorizadas pelo administrador de rede
- Proteção contra malware incorporada em aplicações descarregadas da Internet
- Registo de aplicações bloqueadas, com filtros por equipamento e/ou data
- É possível extrair a informação para o Excel



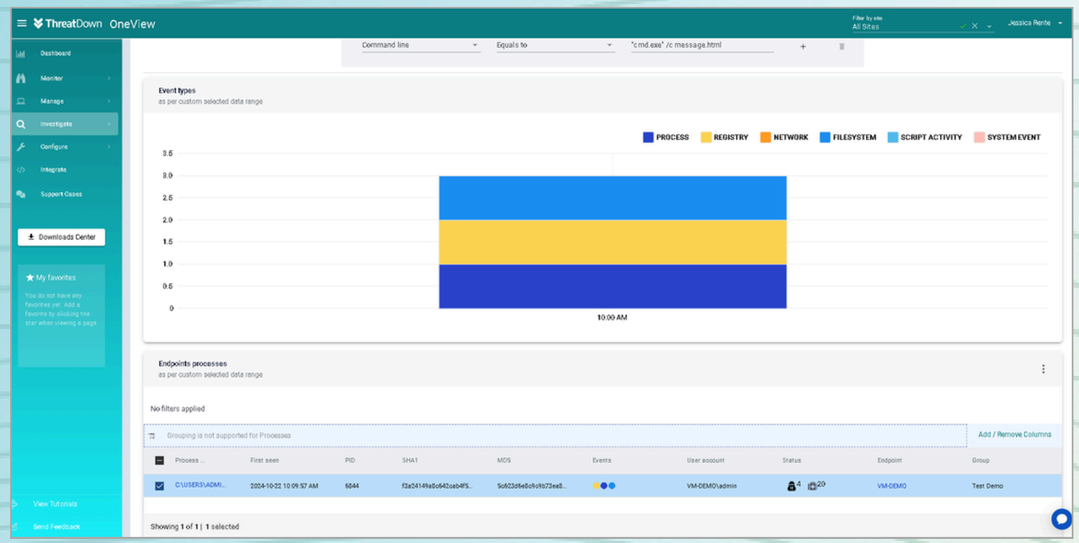
DNS FILTERING



- Encripta a comunicação do DNS através da utilização de DNS sobre HTTPS (DoH)
- Proteção contra agentes de ameaças que criam domínios da web falsos
- Isola as interações do navegador e da aplicação web de potenciais ameaças
- Bloqueios e permissões configuráveis

FLIGHT RECORDER

Funcionalidade concebida para monitorizar e registar a atividade do sistema, ajudando a detetar e analisar ameaças complexas ou incidentes de segurança.



- Monitorização contínua
- Análise de ameaças avançadas

  Compreender como uma ameaça se infiltrou, qual foi o seu comportamento e quais ficheiros e registos foram afetados.

- Rastreamento de eventos passados

  Dá possibilidade à equipa de segurança analisar o vetor de ataque e tomar medidas preventivas.

- Melhor compreensão de incidentes

  Permite investigar incidentes passados e obter insights sobre como melhorar a segurança

minitel NEXT CYBERSECURITY

ThreatDown

Powered by Malwarebytes

next@minitel.pt

www.minitelnext.com

+351 213 810 900