
# Kaspersky – Melhores práticas

1T(RM2-T) EDUARDO dos Santos Silva
Encarregado da Divisão de Segurança de Dispositivos da RECIM
Graduado em Ciência da Computação
Pós graduado em Gestão de TI

# TÓPICOS

- **Por que proteger o endpoint?**
- **AV (antivírus) ou NGAV (*next generation antivírus*)?**
  - O que esperar de um NGAV?
  - Diferencial dos NGAV
- **Processo de migração McAfee - Kaspersky**
  - Estratégia de migração
  - Evolução da migração
  - Diferenças observadas

# TÓPICOS

- **Problemas enfrentados**
  - Desinstalação do McAfee
  - Incompatibilidade com Linux MB / erros de instalação
  - Falta de padronização
- **Kaspersky na MB**
  - Quantidade de políticas
  - Quantidade de tarefas
  - Quantidade de grupos
  - Estrutura de atualização
- **Ganhos observados e alguns números**

# Por que proteger o endpoint?

- Vazamento de informações
- Contaminação da rede
- Endpoints são alvos comuns dos *hackers*
- Mineração de dados
- Uso para *botnets*

# Por que proteger o endpoint?


**23 JAN 2018**

# Por que proteger o endpoint?

Brasil é o segundo país no mund

https://tecnologia.uol.com.br/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm

## Brasil é o segundo país no mundo com maior número de crimes cibernéticos

Do UOL, em São Paulo 15/02/2018 | 15h20

Ouvir texto Imprimir Comunicar erro

Reprodução

Pesquisa indica que Brasil pulou de quarto para segundo país mais afetado por golpes e crimes online

**15 FEV 2018**

Dinheiro seria ilegal, diz petista

Haddad quer investigação sobre 'usina' de fake news

76

**FEV 2018**

https://www.cbsi.net.br/2018/02/62-milhoes-de-pessoas-foram-vitimas-de.html

Home › Brasil › Hacker › Notícias › Segurança da Informação › 62 milhões de pessoas foram vítimas de crimes virtuais no Brasil em 2017

## 62 milhões de pessoas foram vítimas de crimes virtuais no Brasil em 2017

Cláudio Florenzano 8 meses atrás Brasil, Hacker, Notícias, Segurança da Informação


62 milhões de pessoas foram vítimas de crimes virtuais no Brasil em 2017

# Por que proteger o endpoint?

Governo do DF confirma ataque

https://g1.globo.com/distrito-federal/noticia/governo-do-df-confirma-ataque-de-virus-wannacry-mas-oculta-extensao-do-dano.ghtml

## Governo do DF confirma ataque de vírus WannaCry, mas oculta extensão do dano

Secretaria de Planejamento contabiliza 23 máquinas infectadas; Saúde e Cidades têm gestão própria. Exames de raio X foram afetados em três hospitais; G1 aguarda retorno da secretaria.

**Por Mateus Rodrigues, G1 DF**

28/07/2017 18h33 · Atualizado há 1 ano




**28 JUL 2017**

# Por que proteger o endpoint?

**28 JUN 2017**

Ciberataque mundial: Vírus Petya

https://brasil.elpais.com/brasil/2017/06/28/tecnologia/1498639459_556568.html

ATAQUES CIBERNÉTICOS ›

## Vírus Petya é mais perigoso e mais sofisticado que WannaCry

Especialistas manifestam surpresa com últimos ataques, que não tentam roubar e vender informação

FÉLIX PALAZUELOS

28 JUN 2017 - 20:26 CEST

NEWSLETTERS
Receba a newsletter do Brasil

PODE TE INTERESSAR

Identificada uma sofisticada técnica para roubar iPhones

Facebook avisará usuários para que monitorem mensagens suspeitas depois da invasão por 'hackers'

**29 JUN 2017**

'Novo Petya' é praga destrutiva e

Não seguro | g1.globo.com/tecnologia/blog/seguranca-digital/post/novo-petya-e-praga-destrutiva-e-nao-virus-de-resgate-dizem-especialistas.html

globo.com | g1 | globoesporte | gshow | videos

EDUARDO SILVA

MENU | G1 | SEGURANÇA DIGITAL | BUSCAR

## 'Novo Petya' é praga destrutiva e não vírus de resgate, dizem especialistas

O especialista em segurança Matthieu Suiche e a fabricante de antivírus Kaspersky Lab concluíram que o ataque que atingiu empresas na Europa - especialmente na Ucrânia - na terça-feira (27) não se trata de um vírus de resgate, mas sim de um "wiper". Um Wiper é um vírus destrutivo cujo único objetivo é causar danos ao computador atacado, inutilizando o sistema operacional, e não ganhar dinheiro cobrando "resgates".

Como o vírus chegou às empresas atacadas por meio de uma brecha no software de contabilidade e impostos ucraniano M.E. Doc, especula-se que o código malicioso tenha relação com outros ataques cibernéticos destrutivos contra a Ucrânia. O país já sofreu dois apagões elétricos, em dezembro de 2015 e dezembro de 2016, causados por pragas digitais. Autoridades ucranianas, que culpam a Rússia pelos dois incidentes, já sinalizaram crer que o novo ataque também teria ligação com o governo russo.

O responsável pelo ataque na terça-feira foi inicialmente identificado como uma variação do vírus de resgate "Petya", uma praga que existe desde o início de 2016. O novo ataque, que vem sendo chamado de "ExPetr", "NotPetya" e outros nomes, tem uma única grande semelhança com o vírus de resgate: ele reescreve o setor de inicialização (MBR) do disco

Altieres Rohr

OCULTAR PERFIL

Altieres Rohr é fundador e editor do site de segurança Linha Defensiva, especializado na defesa contra ataques cibernéticos. Foi vencedor dos prêmios Internet Segura 2010 – categoria Tecnologia e Eset de Jornalismo 2012 – Categoria Digital.

MAIS FALADOS

segurança

Internet

# Por que proteger o endpoint?


## Sistema da Justiça eleitoral em MT já sofreu 146 mil ataques cibernéticos neste domingo, diz TRE

O TRE alerta que a urna não pode ser atacada porque não é ligada à rede de internet, sistema Wi-fi ou bluetooth.

**Por Tiago Terciotty, TV Centro América**

28/10/2018 12h46 · Atualizado há 22 horas

**28 OUT 2018**

# AV (antivírus) ou NGAV (next generation antivírus)?

Os antivírus tradicionais precisam de um “Paciente Zero” para a elaboração de uma vacina, por isso o chamado “antivírus da nova geração” tem foco na prevenção.

São soluções mais proativas e adaptáveis à detecção e mitigação de riscos.

# O que esperar de um NGAV?

- No primeiro estágio, a ferramenta deve conseguir interromper o funcionamento da ameaça antes que seja executada
- No segundo estágio, a ferramenta deve agir no tratamento rápido da ameaça, caso seja executada
- No terceiro estágio, a ferramenta precisa agir imediatamente nos possíveis impactos causados

# Diferencial dos NGAV

- Controle de aplicativos – *whitelist e blacklist de* aplicativos, seja instalação ou  simples execução
- Controle de dispositivos – Permite bloquear ou restringir o uso de mídias removíveis como pendrives
- Controle da web - Permite criar políticas de navegação com base em categorias predefinidas ou personalizáveis

# Diferencial dos NGAV

- Detecção de comportamento - Detectar e bloquear comportamento malicioso das aplicações logo nos primeiros estágios de execução
- Prevenção de exploração - Se existe um *software* vulnerável instalado, todas suas ações serão monitoradas (principalmente programas descendentes)
- Proteção contra ataque de rede - Detecta e protege o *endpoint* contra ataques de rede
- Firewall - Filtra atividade de rede de acordo com as regras criadas

# Processo de migração McAfee - Kaspersky

**Estratégia de migração**

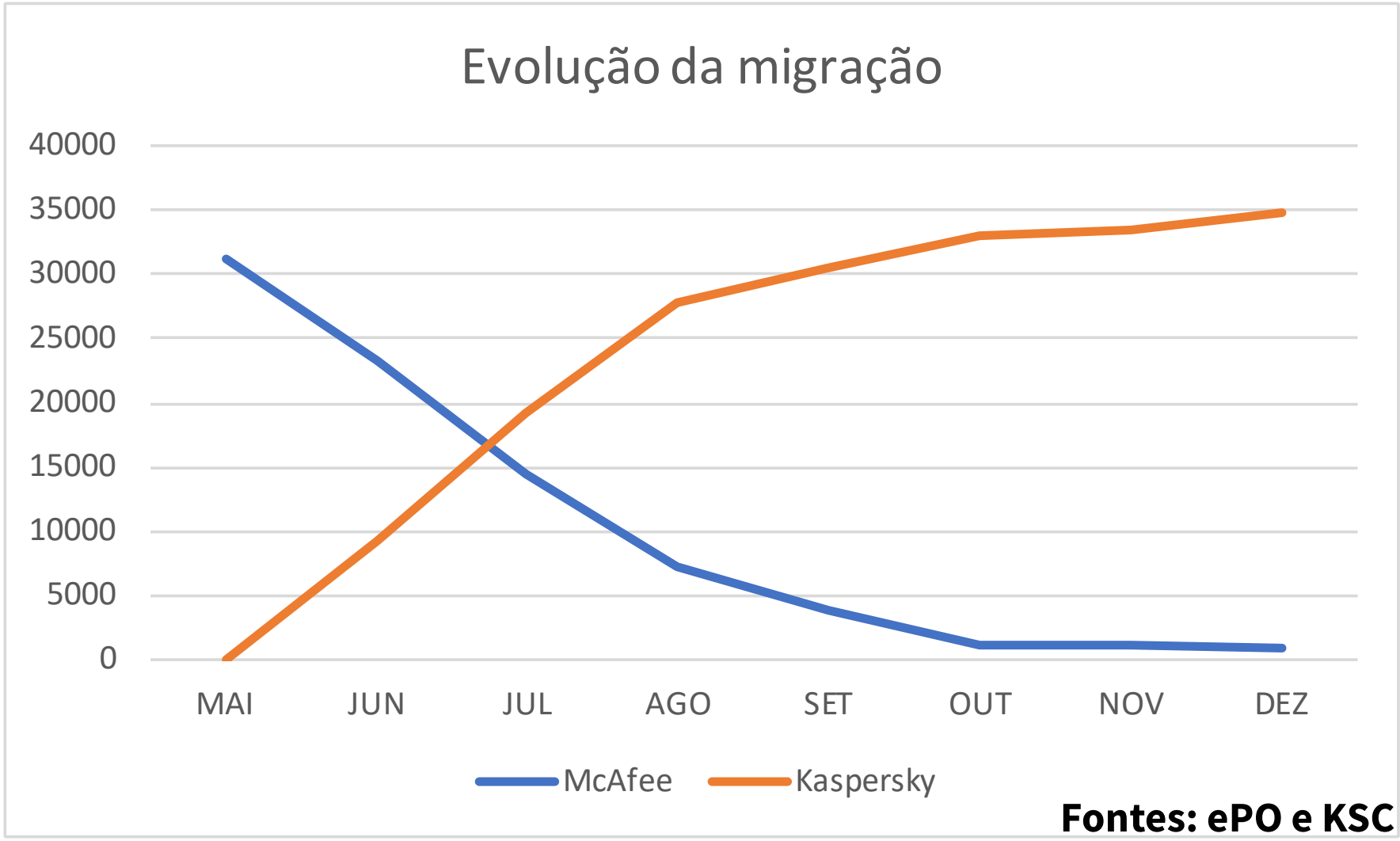
- Remoção do McAfee localmente pelos ADMIN

  → Remoção remota não funciona em todos os casos

- Instalação do Kaspersky localmente pelos ADMIN

  → MB não possui domínio único para as OM

# Processo de migração McAfee - Kaspersky




**Fontes: ePO e KSC**

# Processo de migração McAfee - Kaspersky

## Diferenças observadas

| INÍCIO 05/2017 | |
|---|---|
| Máquinas com McAfee (ePO) | 31231 |
| Máquinas desprotegidas conhecidas (ePO) | 1842 |
| **Total RECIM** | **33073** |

| ATUALMENTE 10/2018 | |
|---|---|
| Máquinas com McAfee (KSC) | 3435 |
| Máquinas com Kaspersky (KSC) | 37646 |
| Máquinas desprotegidas conhecidas (KSC) | 1111 |
| **Total RECIM** | **38757** |

**5.684** máquinas "desconhecidas" em 05/2017

**7.526** máquinas desprotegidas em 05/2017 (5.684 + 1.842) – **19,41% da RECIM**
**1.111** máquinas desprotegidas atualmente – **2,87% da RECIM**

- **McAfee** incompatível com Linux MB (aproximadamente 3.000 máquinas)
- **Kaspersky** em fase final de adaptação ao Linux MB (2.735 já instaladas)
- **Kaspersky** permite visão das máquinas sem agente instalado

# Problemas enfrentados

- Desinstalação do McAfee
  - → Problemas para remover HIPS e VSE
- Incompatibilidade com Linux MB / erros de instalação
  - → Adaptação do pacote de instalação
  - → Criação de script de instalação
  - → Kaspersky → Linux MB lento
- Falta de padronização
  - → Impacto → empreender ações remotas
  - → Impacto → gerar relatórios

# Kaspersky na MB

- **Quantidade de políticas**
  - → 34 políticas de bloqueio
  - → 7 políticas de segurança para MB
    - → 2 políticas personalizadas
- **Quantidade de tarefas**
  - → 7 tarefas de atualização para MB
    - → 1 tarefa personalizada
  - → 7 tarefas de  varredura para MB
    - → 2 tarefas personalizadas
  - → 40 outras tarefas (backup, envio de mensagem, remoção de SW, versionamento, etc)

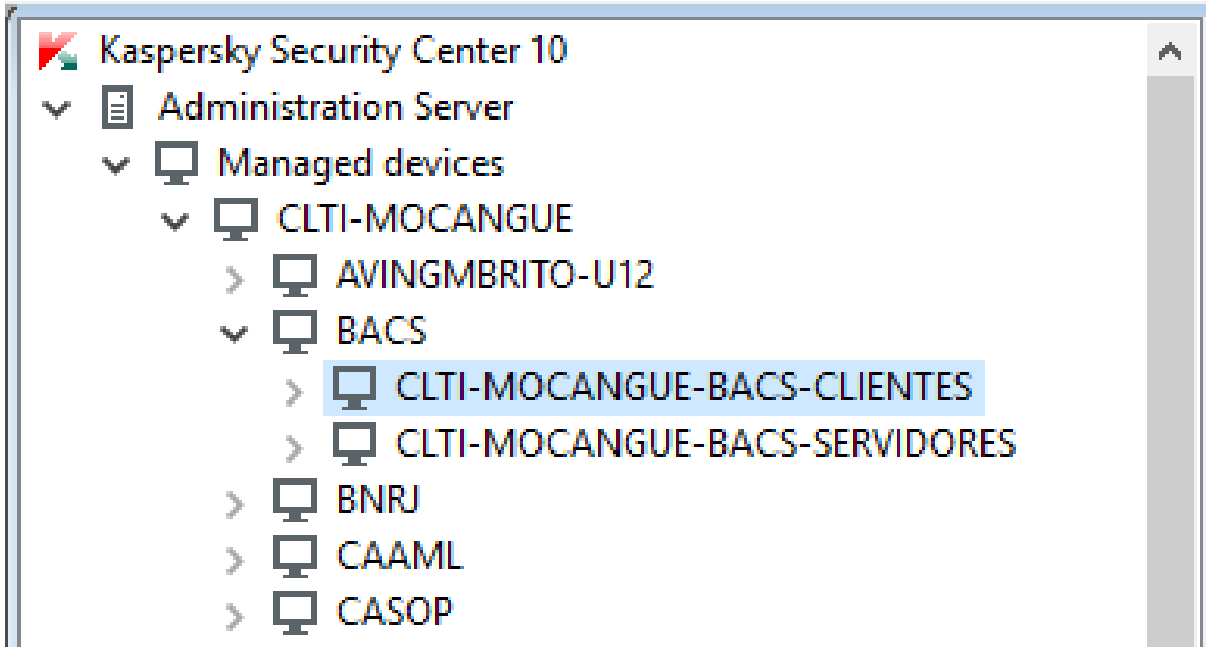
# Kaspersky na MB

## Quantidade de grupos

- **1 grupo principal**

  → 33 subgrupos de CLTI

  → 439 subgrupos de OM



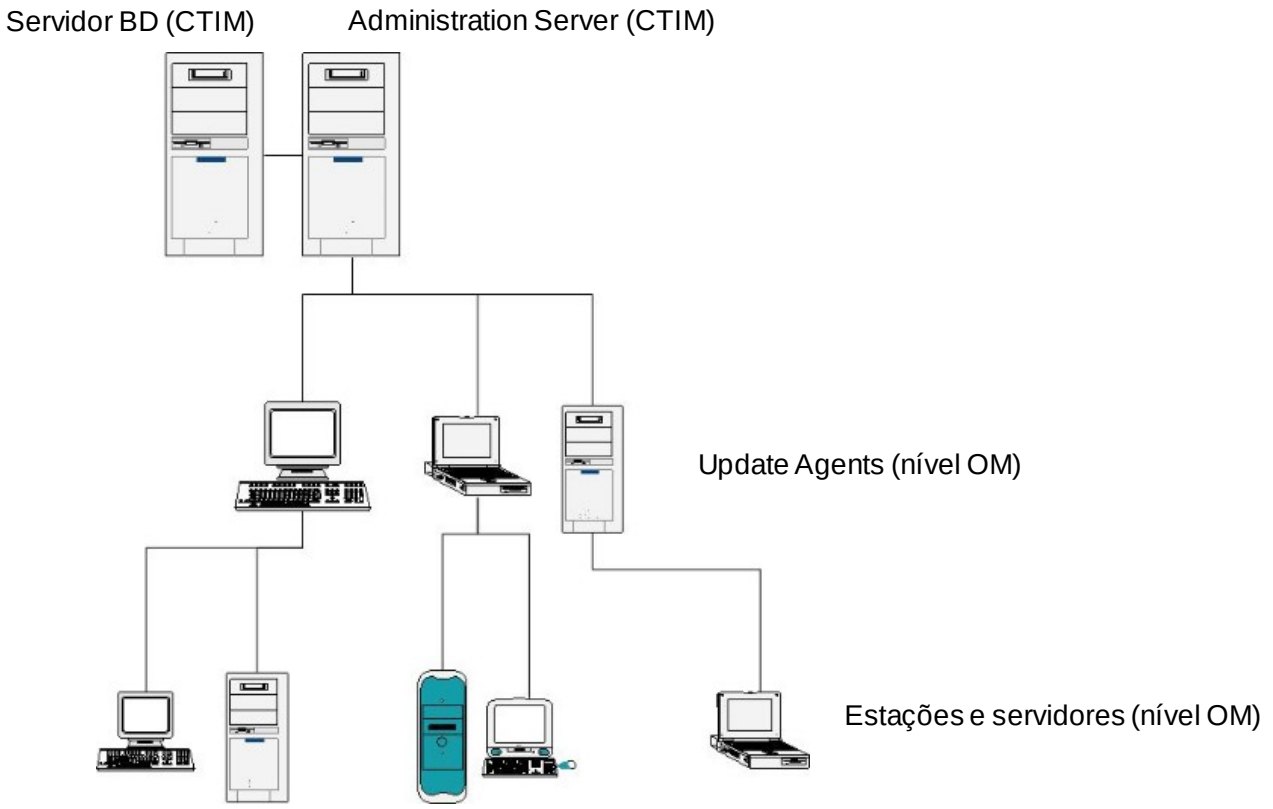
# Kaspersky na MB

- **Estrutura de atualização**

  → 1.479 Update Agents

  → 38.757 máquinas

  → 26,20 máquinas por UA



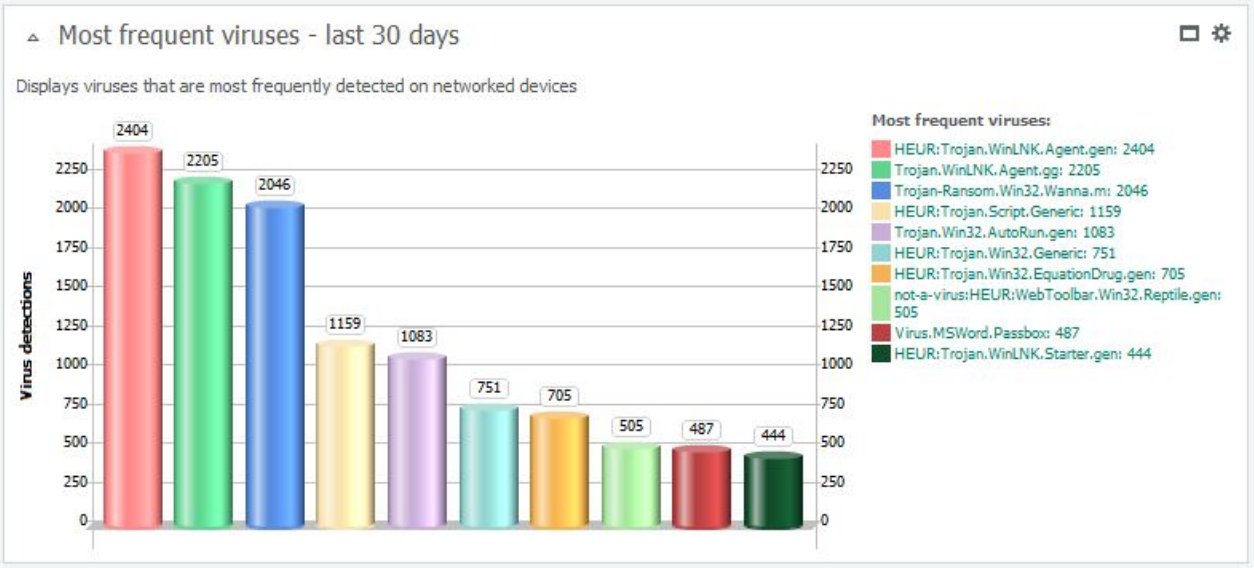
# Ganhos observados e alguns números

- **Facilidade para o ADMIN instalar/desinstalar a ferramenta**

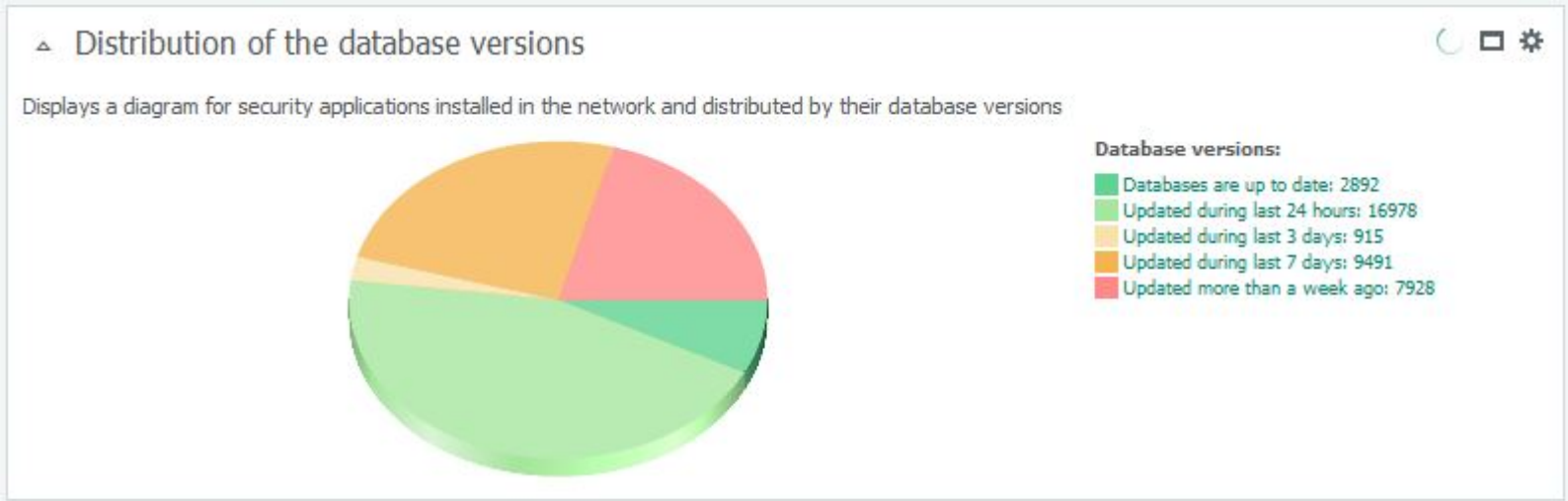
  → Um instalador, vários produtos

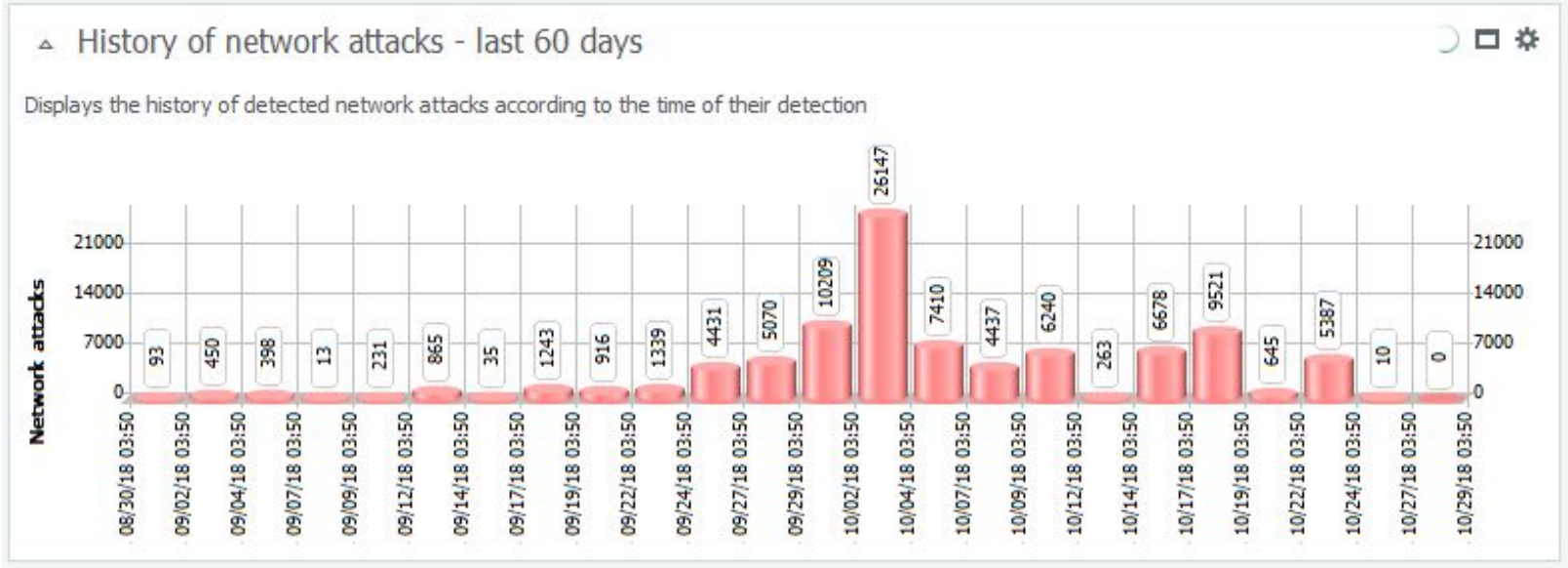
- **Suporte a tomada de decisão**

  → Gráficos e relatórios sobre a saúde das máquinas da MB



# Ganhos observados e alguns números

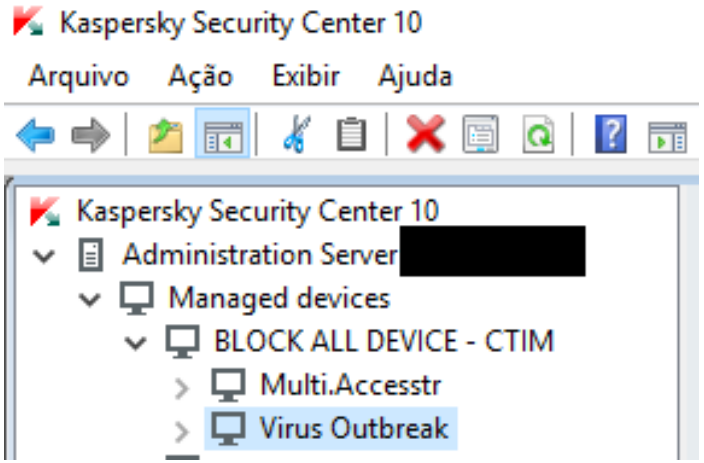


# Ganhos observados e alguns números

- **Agilidade em ações de proteção à RECIM**

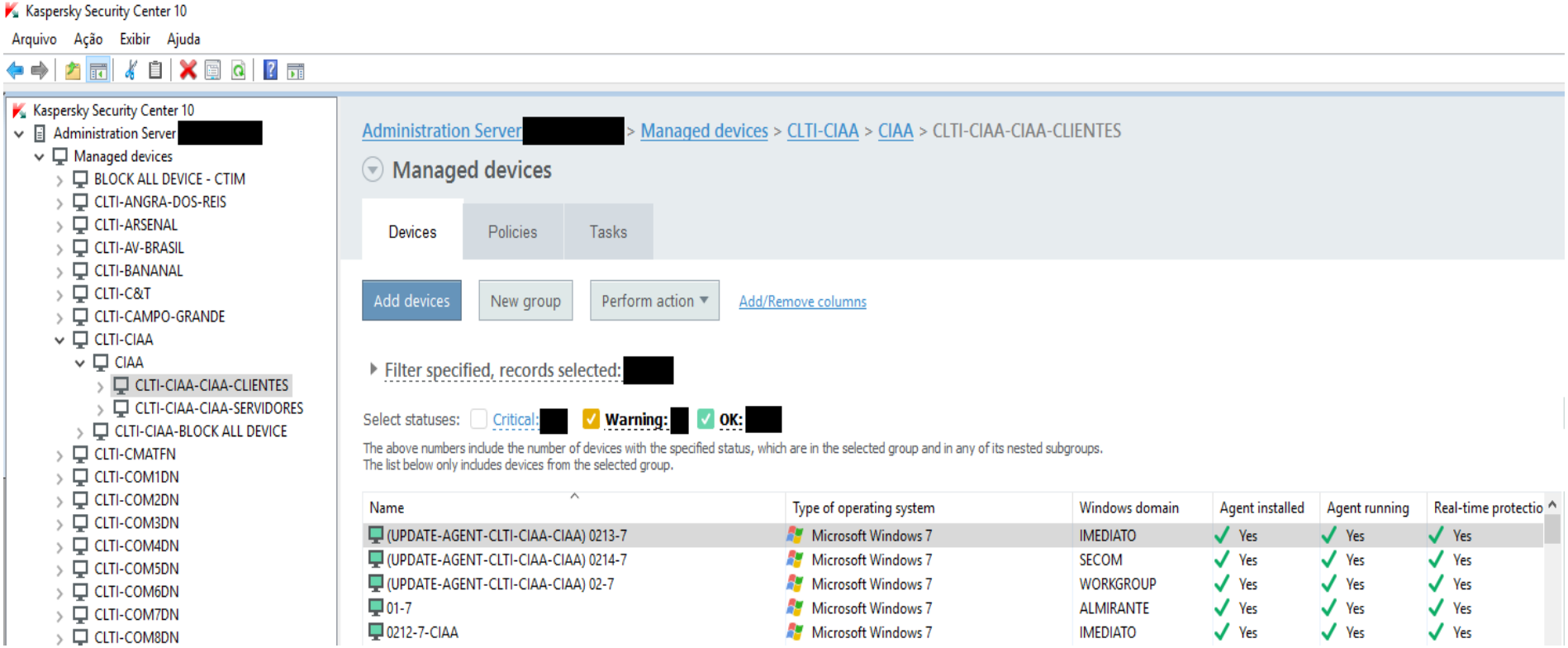
  → Máximo de 60 minutos para bloquear remotamente uma máquina suspeita




- **Visão gerencial simplificada**

# Ganhos observados e alguns números

- Visão gerencial simplificada



# Ganhos observados e alguns números

- **Detecções de ransomware**

  → 120 detecções por mês

- **Detecções de ataques de rede**

  → 70.000 detecções por mês

# Tópicos abordados

- Por que proteger o endpoint?
- AV (antivírus) ou NGAV (*next generation antivírus*)?
- Processo de migração McAfee – Kaspersky
- Problemas enfrentados
- Kaspersky na MB
- Ganhos observados e alguns números

# OBRIGADO!