

# Prevenção e Visibilidade com Detecção e Respostas Automatizadas

— GravityZone Business Security Premium — Mais de 30 camadas de Machine Learning

# Ameaças Sem Fronteiras



RANSOMWARE



APT



PHISHING



ENGENHARIA SOCIAL



## Ransomware em Crescimento Constante

Ataques de ransomware continuam a aumentar globalmente, afetando empresas de todos os setores e dimensões.



## Ataques APT Cada Vez Mais Sofisticados

Ameaças Persistentes Avançadas expandiram-se além da espionagem estatal, visando agora empresas privadas.



## Phishing e Engenharia Social como Vetores Principais

O elemento humano é responsável pela maioria das violações de dados através de manipulação e engano.



## Nenhuma Organização Está Imune

Independentemente da dimensão ou setor, todas as empresas enfrentam o mesmo nível de risco e exposição.



**Todas as organizações** — independentemente da dimensão ou setor — enfrentam hoje as mesmas ameaças avançadas que antes visavam apenas grandes corporações.



# GravityZone Business Security Premium

Proteção empresarial avançada com mais de 30 camadas de segurança baseadas em machine learning



## Prevenção Inigualável

Mais de 30 camadas de segurança baseadas em machine learning bloqueiam ameaças avançadas, ransomware e APT antes de causarem danos à organização.

30+ CAMADAS DE PROTEÇÃO



## Análise Forense e Visualização

Visualização detalhada de ataques com rastreamento completo da cadeia de eventos, fornecendo contexto total para investigação e resposta a incidentes.

RASTREAMENTO DE ATAQUES



## Reforço Orientado por Análises

Políticas de segurança orientadas por dados reduzem a superfície de ataque e otimizam continuamente a postura defensiva da organização.

POSTURA DEFENSIVA OTIMIZADA



## Gestão Centralizada

Uma única consola cobre terminais físicos, virtuais, móveis, cloud e email com visibilidade e controlo completos, sem aumentar a complexidade de TI.

CONSOLA UNIFICADA

# Dashboard em Tempo Real

● MONITORIZAÇÃO ATIVA



ENDPOINTS GERIDOS

45 licenças

Inventário total: 44 dispositivos registados



ENDPOINTS ATIVOS

28 dispositivos

Workstations: 100% das ameaças detetadas



AMEAÇAS BLOQUEADAS

209 ↓ 25

Redução vs. período anterior



RISCO EMPRESARIAL

73% ↑ 1

Score de risco global da empresa



TOP 5 TIPOS DE AMEAÇAS

Lateral Movement

Web Malware

Phishing

Virus

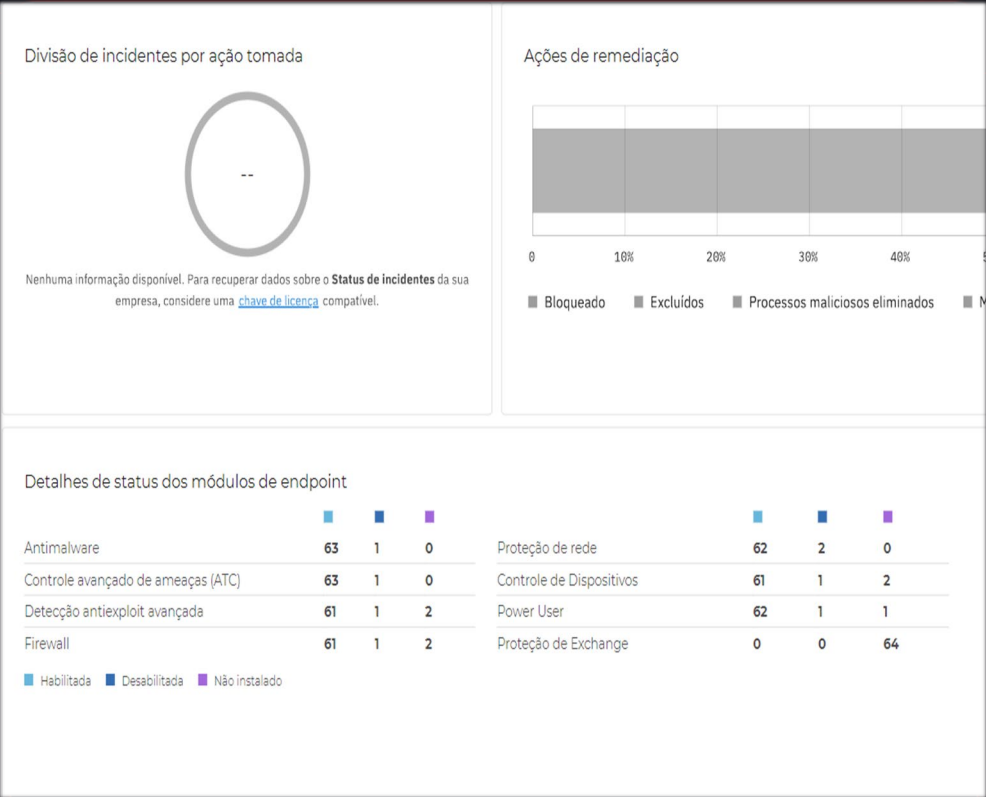
Harmful App



INVENTÁRIO DE REDE

44 dispositivos

Visibilidade completa de todos os endpoints



INTERFACE REAL DO CLIENTE

Bitdefender GravityZone Dashboard

RESUMO EXECUTIVO

209

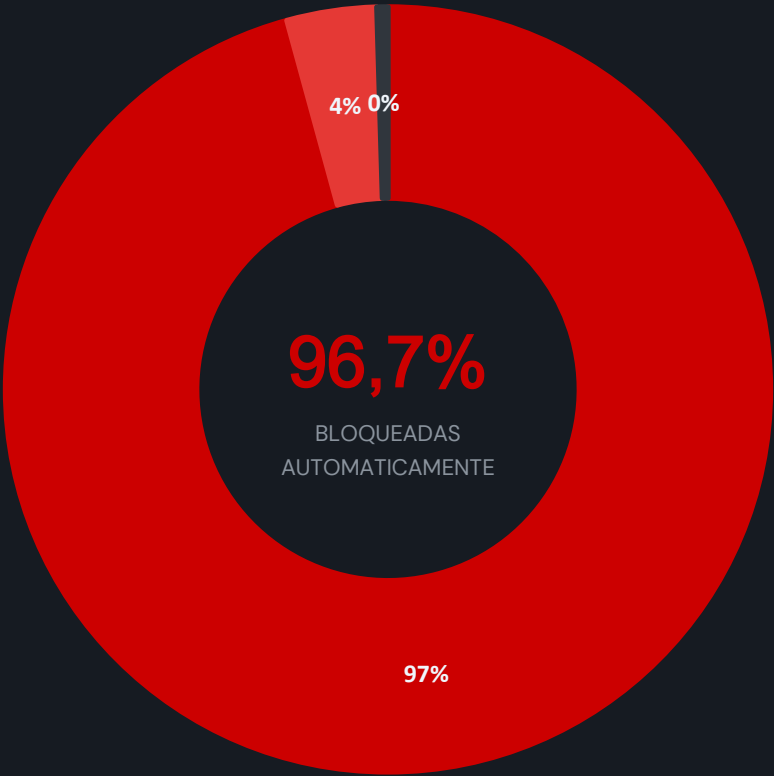
Ameaças bloqueadas no período

73%

Score de risco empresarial atual

# Ações de Remediação Automatizadas

## Ações de Remediação



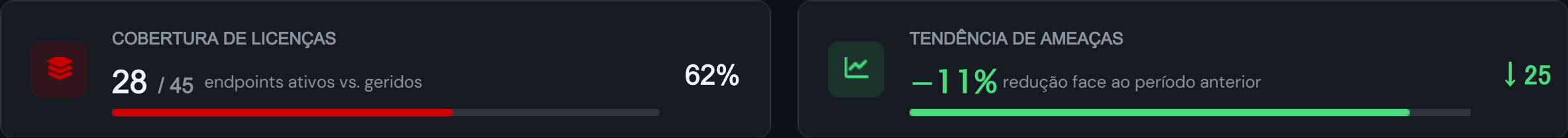
- Bloqueadas automaticamente 96,7%
- Eliminadas (deleted) 3,83%
- Quarentena / Desinfetadas 0%

## Módulos de Proteção — Estado Operacional

|                                                                     |                                                                      |
|---------------------------------------------------------------------|----------------------------------------------------------------------|
| <div></div> <div>Antimalware</div> <div>100% Ativo</div>            | <div></div> <div>Advanced Threat Control</div> <div>100% Ativo</div> |
| <div></div> <div>Advanced Anti -Exploit</div> <div>100% Ativo</div> | <div></div> <div>Firewall</div> <div>100% Ativo</div>                |
| <div></div> <div>Network Protection</div> <div>100% Ativo</div>     | <div></div> <div>Device Control</div> <div>100% Ativo</div>          |

**Zero intervenção manual necessária** — 96,7% das ameaças bloqueadas e 3,83% eliminadas de forma totalmente automática. Processos maliciosos terminados sem ação humana.

# Executive Summary — Visão Executiva



💡

**Visão Executiva:** O sistema bloqueou **209 ameaças** automaticamente, com uma redução de 25 incidentes face ao período anterior. O score de risco de **73%** requer atenção — 17 endpoints geridos permanecem sem agente ativo.



GRAVITYZONE NETWORK

PROTEÇÃO DE REDE

# Controlo de Tráfego de Rede

O Firewall e Network Protection do GravityZone permitem criar regras granulares de acesso, bloqueando comunicações não autorizadas e protegendo a infraestrutura contra ameaças externas e internas.



## Firewall com Regras Configuráveis

Defina quais tráfegos podem passar pela rede com políticas granulares e personalizáveis por grupo.



## Bloqueio de Tráfego Não Autorizado

Network Protection bloqueia comunicações maliciosas antes de atingirem os endpoints da organização.



## Proteção Contra Movimento Lateral

Impede que atacantes se movam entre sistemas internos após uma intrusão inicial na rede.



## Visibilidade Total do Tráfego de Rede

Monitorização contínua de todas as comunicações para deteção e resposta rápida a anomalias.



**Dado Real:** O Lateral Movement foi o tipo de ameaça mais bloqueado no dashboard GravityZone — demonstrando a eficácia crítica do controlo de tráfego de rede.

# Controlo de Dispositivos



## USB & Armazenamento

Controlo total de pendrives e discos internos/externos, bloqueando transferências não autorizadas de dados sensíveis da organização.

BLOQUEIO GRANULAR

## Impressoras & Bluetooth

Gestão de impressoras e ligações Bluetooth para evitar fugas de informação por canais periféricos frequentemente

ignorados

CANIS PERIFÉRICOS

## Prevenção de Exfiltração

Impede a saída não autorizada de dados sensíveis e a introdução de malware via dispositivos físicos conectados aos endpoints.

PROTEÇÃO DE DADOS

## Políticas por Grupo

Regras configuráveis por grupo de utilizadores, adaptando o nível de acesso a hardware conforme o perfil e função na organização.

CONTROLO CENTRALIZADO



# Análise de Riscos Humanos e de Endpoint

*Reduza proativamente a superfície de ataque da sua organização*



## Configurações Incorretas

Avaliação contínua de configurações incorretas de endpoints e vulnerabilidades de patches não aplicados.



## Vulnerabilidades de Aplicações

Identificação e priorização de vulnerabilidades de aplicações por nível de severidade e impacto.



## Comportamento de Utilizadores

Análise de comportamento dos utilizadores mais expostos e identificação de padrões de risco.



## Snapshot de Risco

Visão consolidada do risco para servidores e dispositivos de utilizador final em tempo real.



**Foco estratégico:** Concentre-se nos dispositivos e utilizadores mais expostos para reduzir eficazmente a superfície de ataque da organização.

# Prevenção de Ataques Inigualável



+30 Camadas de Machine Learning



## PREVENÇÃO

### Bloqueio Pré-Execução

Machine learning bloqueia ameaças antes de qualquer execução no sistema.



## DETEÇÃO

### Advanced Threat Control

Anti-Exploit identifica comportamentos suspeitos em tempo real.



## RESPOSTA

### Remediação Automática

**96,7% de bloqueio** com resposta e contenção automáticas.



## ANÁLISE FORENSE

### Visualização de Kill Chains

Mapeamento completo da cadeia de ataque para investigação.



## REFORÇO

### Avaliação Contínua

Monitorização e reforço contínuo da postura de segurança.



### PROTEÇÃO ABRANGENTE

**+30 camadas de ML** garantem cobertura em cada fase do ciclo de vida da ameaça

**96,7%**

Taxa de Bloqueio

**5**

Fases de Proteção

**+30**

Camadas de ML

OBRIGADO PELA SUA ATENÇÃO

# NXTPRESENT



PARCEIRO OFICIAL BITDEFENDER · ANGOLA



EMAIL

**geral@nxtpresent.ao**



TELEFONE

**933 870 778**



NIF

**5001437313**



SERVIÇOS

**Implementação & Suporte**



**AGENDE UMA DEMONSTRAÇÃO**