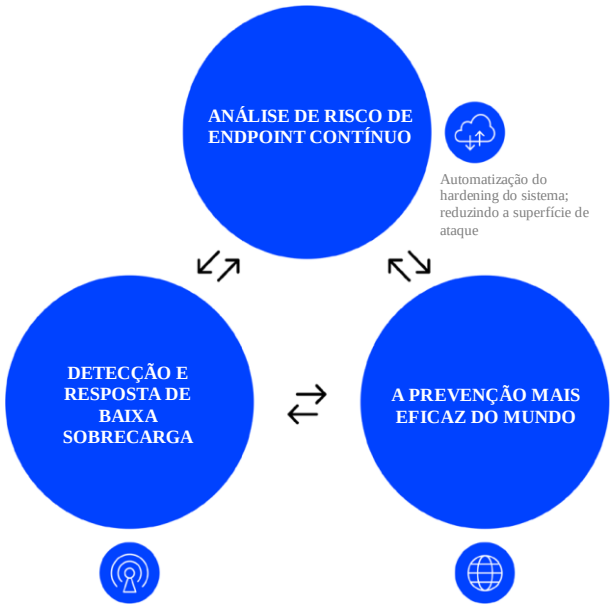
Bitdefender GravityZone Business Security Enterprise

Prevenção unificada, Detecção Estendida, Resposta e Análise de Risco

O **GravityZone Enterprise** combina a proteção mais eficaz do mundo com recursos de detecção e resposta de endpoint estendidos (XEDR) para ajudá-lo a defender sua infraestrutura de endpoints (estações de trabalho e servidores) durante todo o ciclo de vida da ameaça, com alta eficácia e eficiência. A correlação de eventos entre endpoints leva a detecção e a visibilidade de ameaças a um novo nível, combinando a granularidade e o rico contexto de segurança do EDR com a análise de toda a infraestrutura do XDR (eXtended Detection and Response). Ao incorporar o Risk Analytics (para riscos gerados pelo usuário e endpoint) e fortalecer as inovações de forma nativa, ele minimiza a superfície de ataque do endpoint, dificultando a penetração dos invasores. Com o GravityZone Enterprise, você reduzirá o tempo necessário para detectar e responder a ameaças por meio de uma segurança integrada, além de reduzir a necessidade de soluções de vários fornecedores.



Bitdefender GravityZone Enterprise: prevenção, detecção e resposta estendidas em um único agente, gerenciado pela console GravityZone

Como o GravityZone Enterprise ajuda?

A proteção de endpoint mais eficaz do mundo

Unificando as tecnologias EDR, Risk Analytics e Hardening em um único console de agente único, o GravityZone utiliza 30 camadas de técnicas avançadas para interromper com sucesso as violações em todo o ciclo de vida da ameaça, desde o primeiro contato, exploração, persistência e atividade maliciosa.

eXtended Endpoint Detection and Response (XEDR)

O novo recurso de Detecção e Resposta de Endpoint da Bitdefender estende os recursos de análise EDR e correlação de eventos além dos limites de um único endpoint, para ajudá-lo a lidar com mais eficiência com ataques cibernéticos complexos envolvendo vários endpoints. O XEDR fornece visualizações de ameaças exclusivas no nível organizacional para que você possa concentrar as investigações e responder com mais eficiência.

Endpoint e proteção orientada por análise de risco humano

O mecanismo de análise de risco do Bitdefender permite que você avalie, priorize e proteja continuamente as configurações incorretas de segurança de endpoint com uma lista priorizada fácil de entender. Ele também identifica ações e comportamentos do usuário que representam um risco de segurança para sua organização.

Ao simplificar e automatizar as operações de segurança e reduzir continuamente a superfície de ataque, você alcançará os mais altos níveis de proteção com o melhor custo-benefício.

A proteção de endpoint mais eficaz do mundo

Número #1 na maioria dos rankings de 2018 a 2021 nos testes da AV-Comparatives. Mais de 30 tecnologias de proteção desenvolvidas em 20 anos por pesquisadores, matemáticos e cientistas de dados de classe mundial da Bitdefender resultam em proteção superior que atualmente é licenciada para mais de 150 empresas líderes em tecnologia.

Aprendizado de máquina em nuvem e local: A Bitdefender lançou o aprendizado de máquina pela primeira vez em 2009, resultando em maior detecção de ameaças com baixos falsos positivos que podem impedir ameaças desconhecidas na pré-execução e na execução.

Hyperdetect - aprendizado de máquina ajustável: permite que as equipes de TI ajustem a proteção em serviços de negócios confidenciais com maior risco.

Defesa de Anomalia: Tecnologia avançada de aprendizado de máquina que faz a linha de base dos serviços do sistema e monitora as técnicas de ataque furtivo. Capaz de proteger aplicativos personalizados de ataques maliciosos.

Sandbox baseado em nuvem: fornece detecção em pré-execução de ataques avançados enviando automaticamente arquivos que exigem análise adicional para a sandbox em nuvem e tomando ações de correção com base no veredicto.

Defesa contra ataques de rede: detecte e bloqueie novos tipos de ameaças no início da cadeia de ataque, como ataques de força bruta, ladrões de senha, movimentação lateral, dentro outros.

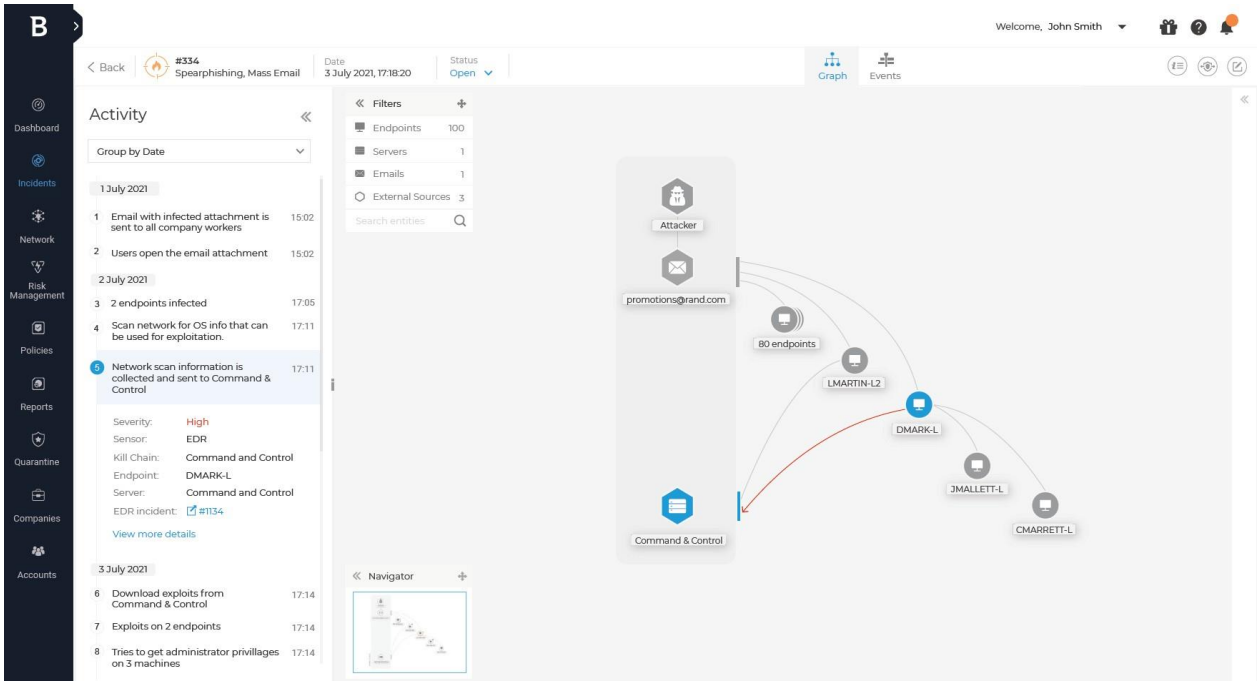
Anti-Exploit: Vários mecanismos de prevenção contra exploração protegem a memória e bloqueiam ataques antes que eles explorem os sistemas, reduzindo os esforços de triagem.

Proteção para ataque sem arquivo: detecte e bloqueie malware baseado em script, sem arquivo, ofuscado e personalizado com correção automática.

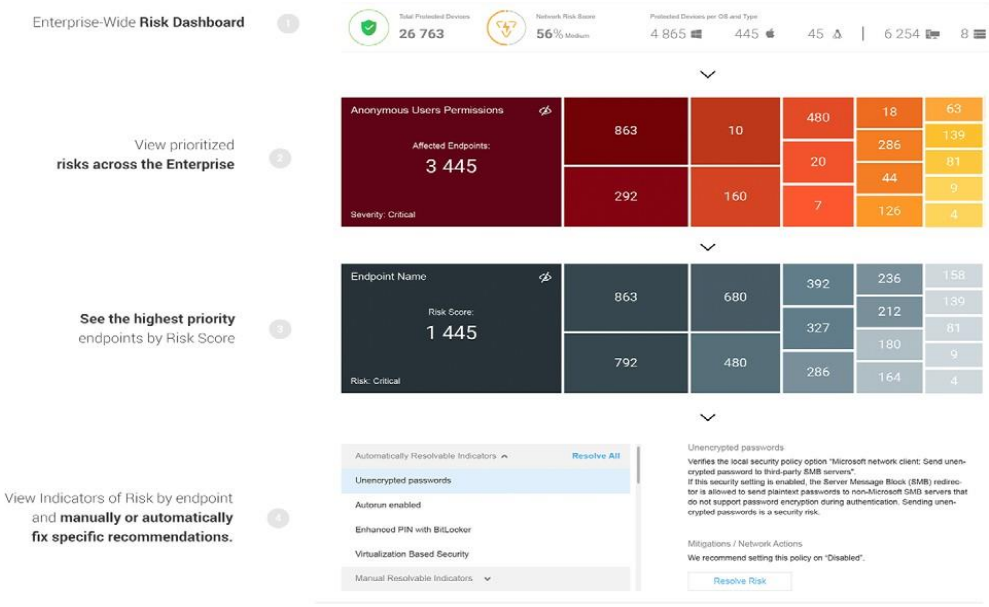
Firewall de cliente integrado, controle de dispositivos, filtragem de conteúdo da Web, controle de aplicativos e muito mais.

Investigação de incidentes estendida e resposta inteligente com proteção evoluída

O GravityZone Enterprise permite uma investigação eficaz de incidentes e uma resposta rápida para restaurar os endpoints a um estágio "melhor do que antes". Ferramentas de investigação de incidentes, como o Extended Incident View, fornecem visibilidade em nível organizacional sobre incidentes de segurança e ajudam as equipes de segurança a validar atividades suspeitas e responder adequadamente a ameaças cibernéticas. A pesquisa avançada de dados atuais e históricos com base em IOCs, MITRE e outros artefatos relevantes permite a identificação rápida de ameaças que podem se esconder na infraestrutura do endpoint. Ao usar a inteligência coletada dos endpoints durante a investigação, a interface única de gerenciamento fornece as ferramentas para ajustar imediatamente a política e/ou corrigir as vulnerabilidades identificadas para evitar incidentes futuros, melhorando a segurança do seu ambiente.



O Extended Incident View fornece visibilidade em nível organizacional sobre o incidente. O analista de segurança pode facilmente adquirir evidências e responder de forma eficaz. Análise de Risco de endpoint para gerenciamento contínuo de superfície de ataque.



Permite processos de proteção de sistema ativo em toda a empresa. O mecanismo de Endpoint Risk Analytics (ERA) da Bitdefender permite que as organizações avaliem, priorizem e protejam continuamente configurações incorretas de segurança de endpoint e configuração com uma lista priorizada fácil de entender. Com análises de risco exclusivas, há redução contínua da superfície de ataque.

PRINCIPAIS CARACTERÍSTICAS

Detecção e resposta de endpoint estendidas
Essa tecnologia de correlação entre endpoints, conhecida como XEDR, leva a detecção e a visibilidade de ameaças a um novo nível, aplicando recursos de XDR para detectar ataques avançados em vários endpoints em infraestruturas híbridas (estações de trabalho ou servidores, executando vários sistemas operacionais).

Análise Integrada de Risco Humano e de Endpoint
Analise continuamente os riscos usando centenas de fatores para descobrir e priorizar os riscos de configuração para todos os seus endpoints, permitindo ações automáticas de proteção. Ele identifica ações e comportamentos do usuário que representam um risco de segurança para a organização, como o uso de páginas da Web não criptografadas para fazer login em sites, gerenciamento de senhas inadequado, uso de USBs comprometidos, infecções recorrentes, etc.

Defesa em camadas
Tecnologias sem assinatura, incluindo aprendizado de máquina local e em nuvem avançado, tecnologias de análise de comportamento, sandbox integrado e proteção de dispositivos funcionam como uma proteção em camadas altamente eficaz contra ameaças sofisticadas.

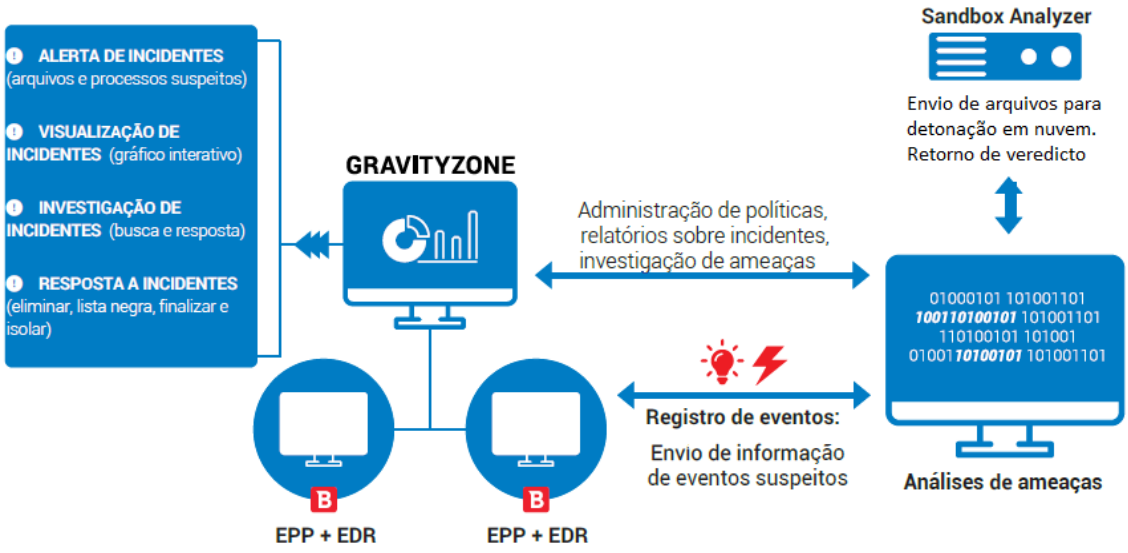
Investigação e Resposta a Incidentes de Baixa Sobrecarga
Triagem rápida de alertas e investigação de incidentes, usando linha do tempo de ataque e sandbox, permitem que as equipes de resposta a incidentes reajam rapidamente e interrompam os ataques em andamento (um clique para responder).

Prevenção e Detecção Modernas e de Última Geração com Correção Automática
A melhor concentração de prevenção do mundo e recursos de detecção baseados em comportamento impedem que ameaças avançadas sejam executadas na infraestrutura corporativa. Com recursos avançados de prevenção, como PowerShell Defense, Exploit Defense e Anomaly Detection, o GravityZone Enterprise bloqueia os ataques modernos no início da cadeia de ataque, na pré-execução, protegendo a postura de segurança da sua organização. Uma vez que uma ameaça ativa é detectada, a resposta automática entra em ação para bloquear mais danos ou movimentos laterais.

Defesa contra Ataques de Rede
O Bitdefender Network Attack Defense, uma nova camada de segurança de rede de endpoint projetada para detectar e impedir tentativas de ataque que estão fazendo uso de vulnerabilidades de rede bloqueando vários ataques, como: Força Bruta, Ladrões de Senhas ou Movimentação Lateral antes mesmo de serem executados. O Network Attack Defense também gera incidentes de EDR e é uma importante fonte de informações para correlações de incidentes de endpoint.

Fluxo de Análise, Detecção e Reposta otimizados

Detecção automatizada, fácil investigação e reparo local graças ao novo log de eventos do endpoint e análise de ameaças do EDR.



Construído para Cyber-resiliência

Bitdefender GravityZone Enterprise: Prevenção unificada, Detecção Estendida, Resposta e Análise de Risco

O Bitdefender GravityZone Enterprise conta com um único agente de console única para fornecer o conjunto completo de recursos de segurança, visibilidade e gerenciamento integrado em todo o ambiente corporativo: estações de trabalho e servidores, físicos e virtuais. O GravityZone é nativo da nuvem, mas também oferece suporte a implantações locais quando os regulamentos ou requisitos de negócios o impõem.

GravityZone: a solução mais premiada do mundo!

AV-TEST
Melhor Proteção 2020

AV-TEST
Melhor Proteção (EDR) 2021

AV-COMPARATIVES
Produto Excepcional 2020

AV-COMPARATIVES
Produto Excepcional 2021

Para saber mais, acesse www.bitdefender.com.br/business/products/enterprise-security.html