Bitdefender GravityZone Ultra Suite

DESCUBRA E PARE AS AMEAÇAS EVASIVAS COM PRECISÃO E AGILIDADE

GravityZone Ultra, com Endpoint Security XDR, destaca-se sobre os produtos EDR especializados, que são muito complexos e barulhentos, prevenindo, detectando e respondendo a ataques sofisticados que ultrapassam o antimalware tradicional. O GravityZone Ultra oferece em um único pacote de segurança:

- Redução da superfície de ataque (através de firewall, controle de aplicativos, controle de conteúdo e gerenciamento de patches).
- Proteção de dados (através da criptografia de disco completo).
- Detecção e eliminação de malware antes da sua execução (através do Machine Learning ajustável, a inspeção de processos em tempo real e a análise no Sandbox).
- Detecção automatizada, fácil investigação e reparo local graças ao novo log de eventos do endpoint e à análise de ameaças do Endpoint Security XDR.

O resultado é uma ótima prevenção de ameaças, uma detecção precisa de incidentes e uma resposta inteligente que minimiza a exposição a infecções e interrompe violações.

Como um conjunto integrado de proteção de terminais, o GravityZone Ultra garante um nível constante de segurança para todo o ambiente de TI, para que os invasores não encontrem endpoints mal protegidos para usar como pontos de partida para ações mal-intencionadas contra a organização. O GravityZone Ultra é baseado em uma arquitetura simples e integrada, com gerenciamento centralizado para terminais e data center. Ele permite que as empresas implementem rapidamente a solução de proteção de endpoint e exige menos esforço de gerenciamento após a implementação.

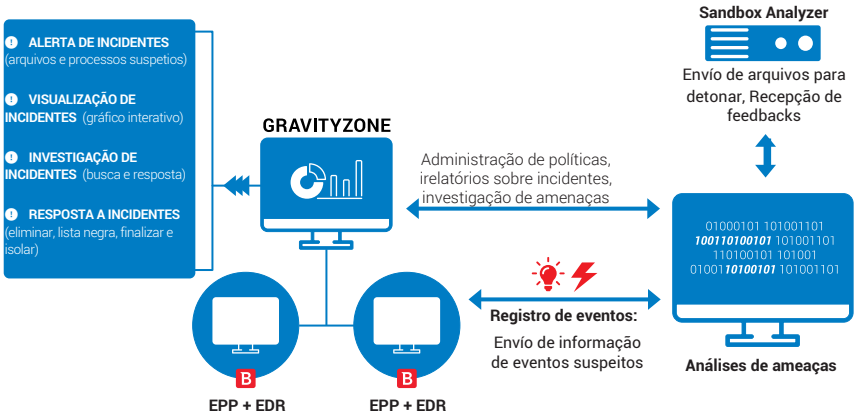


Figura 1. Bitdefender XDR: prevenção, detecção e resposta em um único agente, gerenciado pelo console GravityZone

EDR fácil

Graças à visibilidade clara dos indicadores de comprometimento (IOCs) e fluxos de trabalho de pesquisa e resposta a incidentes de ameaças em um único clique, o GravityZone Ultra reduz os recursos e as habilidades necessárias para as equipes de segurança. O novo registro de dados do endpoint é um complemento perfeito para a matriz existente de ferramentas de proteção contra ameaças e captura um amplo registro de atividades do sistema (criação de arquivos e processos, instalação de programas, carregamento de módulos, modificação de registros, conexões rede, etc.) contribuindo para uma visão de toda a cadeia de eventos envolvidos no ataque na empresa.

O módulo de análise de ameaças funciona na nuvem e filtra continuamente os eventos de comportamento nas atividades do sistema para criar uma lista priorizada de incidentes dignos de investigação e resposta adicionais.

Beneficios Principais

O Endpoint Security XDR, além das funções tradicionais de EPP, fornece aos analistas de segurança e às equipes de resposta a incidentes as ferramentas necessárias para analisar atividades suspeitas, investigar e responder adequadamente às ameaças avançadas:

- Visibilidade do endpoint em tempo real
- Destaca as atividades suspeitas
- Investigação com um único clique
- Protocolo de intervenção antes de alertas e visualização de análise de incidentes
- Rastreamento de ataques ativos e movimentos laterais
- Resposta rápida
- Reduz o tempo de ocupação com resolução, contenção e reparo rápidos

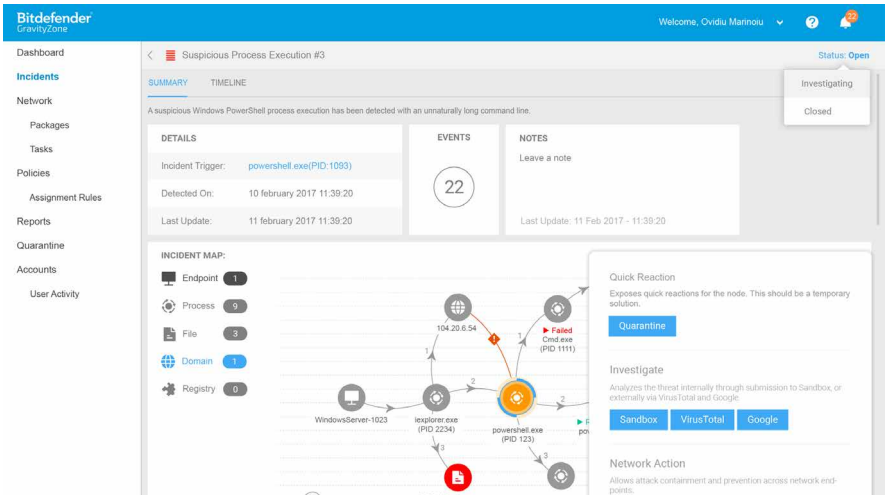


Figura 2. A página de detalhes do incidente fornece uma descrição clara do escopo dos incidentes. O profissional pode facilmente obter testes e responder adequadamente.

Melhora a visualização de segurança. Evite a fadiga causada por alertas

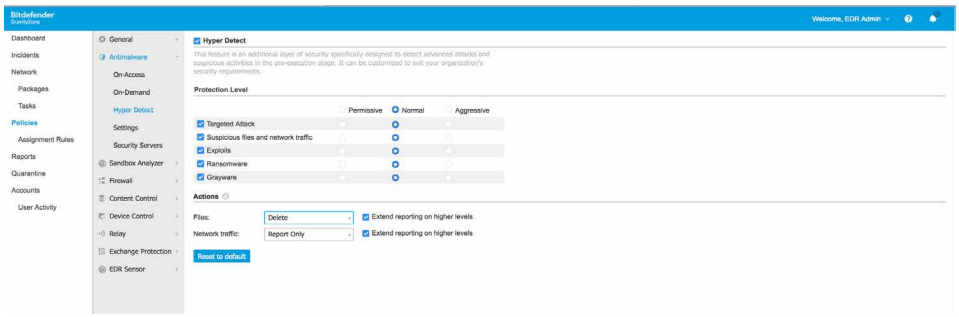
Apenas eventos relevantes, relacionados e classificados por gravidade são apresentados para análise e resolução manual. Minimiza o ruído e as informações redundantes, já que a grande maioria dos ataques normais e avançados são bloqueados na fase de pré-execução ou no início da execução. Ameaças evasivas, incluindo malware sem arquivos, exploits, ransomware e malware oculto, são neutralizadas graças a tecnologias altamente eficazes de prevenção em camadas e de última geração para endpoints e ao inspetor de processos com base no comportamento durante a execução. A resposta e o reparo automáticos eliminam a necessidade de intervenção humana em ataques bloqueados.

A detecção altamente confiável permite que o pessoal de segurança se concentre apenas em incidentes e ameaças reais:

- Minimize o ruído e a distração de alarmes falsos
- Reduzir o volume de incidentes com prevenção eficaz de ameaças
- Esqueça o reparo manual de ataques bloqueados graças ao reparo automático

Uma resposta inteligente significa prevenção avançada

Como o GravityZone Ultra é uma solução que cobre todo o ciclo de prevenção-detecção-resposta, permite uma resposta rápida e uma efetiva restauração em um estágio seguro. Aproveitando a inteligência sobre ameaças coletadas dos endpoints durante o processo de pesquisa, uma única interface fornece as ferramentas para ajustar imediatamente a política e corrigir as vulnerabilidades para evitar incidentes futuros e melhorar a segurança do seu ambiente.



Plataforma completa de segurança de terminais em um único agente e uma única console

O GravityZone Ultra herda todos os controles de reforço e prevenção de última geração incluídos no Endpoint Security HD e no pacote GravityZone Elite:

- Reduz a exposição com prevenção sólida
- Detecção baseada em Aprendizado de Máquina e comportamento aborda ameaças desconhecidas na fase de pré-execução e no início da execução
- Detecta e bloqueia malware roteirizado, sem arquivos, oculto e personalizado, com reparo automático
- Proteção de memória para evitar exploits
- Reduz a superfície de ataque, permitindo controles de segurança de TI
- Integração de um firewall bidirecional, controle de dispositivos, filtragem de conteúdo da Web, controle de aplicativos, gerenciamento de patches e muitos outros recursos.

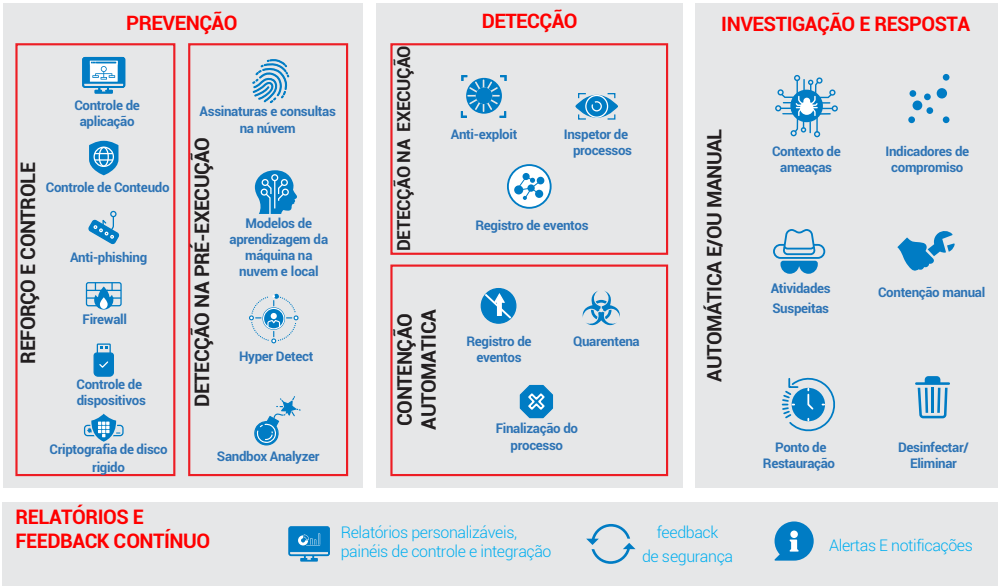
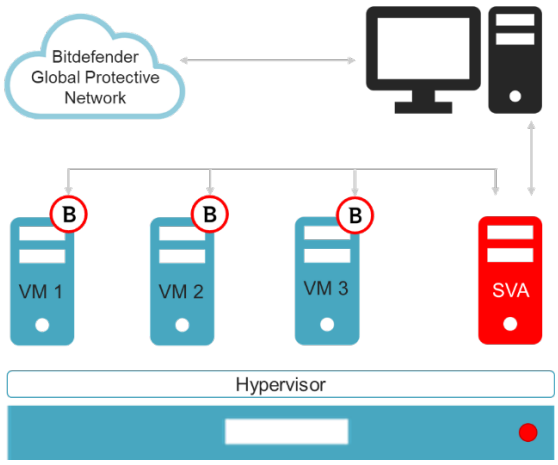


Figura 3. Bitdefender XDR: a plataforma de segurança completa para terminais

Proteção do DataCenter

Totalmente integrado ao Bitdefender Endpoint Security XDR, o componente de proteção do DataCenter do conjunto GravityZone Elite é o Security for Virtualized Environments (SVE). É a solução de segurança mais avançada para data centers no mercado em termos de proteção antimalware para máquinas virtuais, otimizando não apenas as taxas de consolidação, mas também os custos operacionais. O GravityZone SVE é uma solução de negócios compatível, mesmo com os maiores data centers. A integração em um ambiente de produção é simples e ambientes virtuais de qualquer tamanho podem se beneficiar dessa tecnologia.

Beneficios Principals



Agilidade

O SVE permite a automação da segurança durante todo o ciclo de vida do data center durante a implementação, bem como durante as operações diárias de segurança de um ambiente virtual muito dinâmico. Integra-se ao VMware (vCenter, vShield, NSX), ao Citrix XenCenter e ao Nutanix Enterprise Cloud Platform e permite um provisionamento automatizado rápido.

Eficiencia de Operação

O Console de Gerenciamento Unificado do Centro de Controle da GravityZone simplifica a implantação, a manutenção e a atualização de segurança e fornece visibilidade centralizada de todas as estações de trabalho e servidores físicos e virtuais. Ele suporta criação centralizada e gerenciamento automático de políticas de segurança
para ajudar a otimizar as operações de TI e melhorar a conformidade.

Melhor uso da infraestrutura

A análise centralizada e um agente muito leve reduzem bastante o uso

de memória, espaço em disco, CPU e atividade de E / S em servidores host, o que aumenta a densidade de máquinas virtuais e o ROI na infraestrutura de TI.

Compatibilidade universal
Compatível com as principais plataformas de hipervisor (VMware ESXi, Microsoft Hyper-V, Citrix Xen, Red Hat KVM e Nutanix AHV), ambos com o Windows e com o Linux como sistemas operacionais.

Escalabilidade linear ilimitada
Vários SVAs podem ser usados para aumentar a capacidade analítica à medida que o data center cresce e mais máquinas virtuais são criadas. Quando um SVA existente atinge um determinado limite de carga, novos podem ser implementados para responder a esse crescimento. Um benefício adicional da implementação de vários SVAs é a melhoria da capacidade de recuperação e a distribuição da carga: a carga de um SVA com falha ou sobrecarga pode ser assumida por outro SVA ativo ou menos carregado.

Defesas de camada de última geração
GravityZone Security for Virtualized Environments incorpora todas as camadas da chave de segurança Endpoint Security, incluindo HyperDetect, Sandbox Analyzer e métodos de detecção de ataques sem arquivos para fornecer proteção líder de ativos de negócios digitais armazenados ou processados no DataCenter

Características

- Projetado para permitir a transformação do data center: SDDC, hiperconvergência e a nuvem híbrida
- Integração total com VMware, Nutanix, Citrix, AWS e Microsoft para proteger seu investimento, automatizar a implementação e gerenciar inventários e licenças
- Suporta vários ambientes de virtualização e nuvem com uma única implantação
- Visibilidade de painel único e capacidade de gerenciamento centralizado de toda a nuvem híbrida
- Arquitetura eficiente, resiliente e escalável baseada em SVA compatível com todos os hipervisores
- Maximização da densidade de VMs, baixa latência de início e desempenho ideal do aplicativo
- Camada avançada de segurança com cobertura contínua em toda a nuvem híbrida

Centro de Controle GravityZone

O GravityZone Control Center é a console de gerenciamento integrado centralizado que fornece uma única console para todos componentes de gerenciamento de segurança, incluindo segurança de endpoint, segurança de data center, segurança do Exchange e dispositivos móveis. Você pode ficar na nuvem ou ser implantado localmente. O centro de administração GravityZone incorpora várias funções e inclui o servidor de banco de dados, o servidor de comunicações, o servidor de atualizações e o console da web. O Control Center é fornecido como uma imagem de dispositivo virtual e pode ser implementado em menos de trinta minutos. Em empresas maiores, você pode configurar uma arquitetura com vários dispositivos virtuais, com várias instâncias de funções específicas e com o balanceador de carga integrado, para oferecer grande escalabilidade e disponibilidade.

Para obter uma lista mais detalhada dos requisitos do sistema, acesse www.bitdefender.es/business/ultra-security

BD-NGZ-Nov.21.2017-Tk#: crea2183
Bitdefender-NGZ-UltraSuite-Datasheet-creat2199-A4-es_ES