Guardeon. by VANELOS

DATASHEET

Guardeon.

Unifique monitoramento, vulnerabilidades, risco e inteligência de ameaças em uma plataforma orientada a risco e governança.

As operações de segurança lidam com um volume crescente de alertas e uma superfície de ataque que se expande por nuvem, endpoints e identidades. Na maioria das organizações, a segurança é operada de forma fragmentada múltiplas ferramentas que não conversam entre si, dados dispersos e pouca correlação. Sem uma visão unificada e priorização por risco, os times reagem a eventos isolados, o tempo de resposta cresce e fica difícil comprovar a postura de segurança para a liderança.

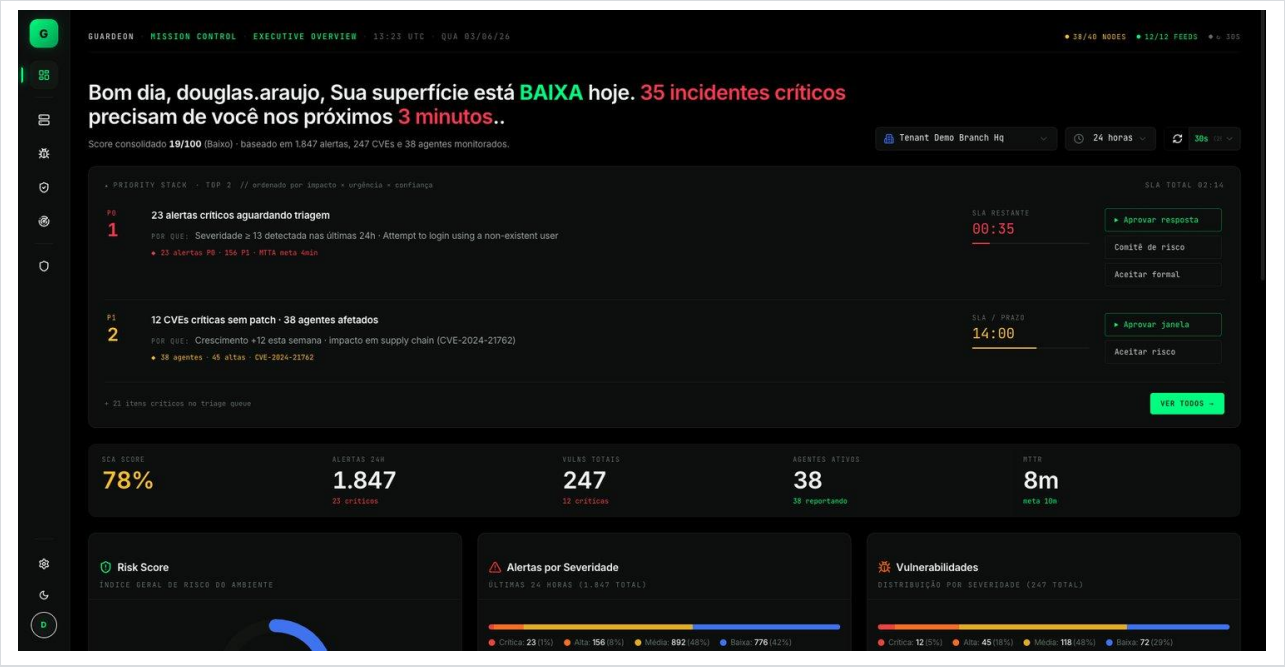

Figura 1. Painel executivo do Guardeon — superfície de ataque, risk score e incidentes críticos priorizados

Para fortalecer a defesa cibernética, as equipes de operações de segurança precisam de:

- **Segurança orientada a risco:** priorizar o que tem maior impacto, antes que vire incidente.
- **Contexto unificado e correlação:** reunir monitoramento, análise de postura, governança, gestão de risco, compliance, vulnerabilidades e CTI em um só lugar.
- **Plataforma única e multi-tenant:** reduzir a complexidade e o custo total de propriedade (TCO).

O **Guardeon** entrega segurança unificada e orientada a risco. Com o Guardeon, você pode:

- **Antecipar-se com inteligência:** IOCs, campanhas APT e exposição de vazamentos correlacionados ao seu ambiente.
- **Detectar com cobertura MITRE ATT&CK:** mapeie táticas, técnicas e gaps de detecção.
- **Priorizar por risco:** análise de causa raiz e priority stacks acionáveis.
- **Responder no prazo:** SLAs e KPIs monitorados por severidade, do alerta à resolução.

Construído para a operação real

- **Mission Control:** KPIs executivos e insights priorizados.
- **Multi-tenant isolado:** banco e cache dedicados por cliente, com visão consolidada.
- **Offline-first:** sincronização em segundo plano e cache em duas camadas para alta disponibilidade.

Como o Guardeon reduz risco e acelera a resposta

O Guardeon reúne, em um único console, tudo o que as equipes precisam para enxergar, priorizar e responder, transformando dados de segurança em decisões.

1. Visibilidade unificada em tempo real

O **Guardeon Monitor** consolida a operação de segurança a partir da telemetria:

- **Agentes:** estado em tempo real (ativos, desconectados, desatualizados), versão, SO, inventário e último keepalive.
- **Alertas 24h e evolução:** resumo por severidade, detecção de picos, top regras/agentes e tendência de 7 e 30 dias.
- **Performance do SOC:** MTTA, MTTD e MTTR, acurácia e conformidade frente às metas de SLA e compliance.
- **Detalhe do agente:** alertas, vulnerabilidades e técnicas MITRE associadas a cada ativo.

2. Gestão de vulnerabilidades orientada a risco

O **Guardeon Vulnerabilities** análise os resultados e apresenta priorizacão para diminuir a exposição do negócio:

- **Distribuição CVSS e Top CVEs:** priorize por severidade e por número de ativos afetados.
- **Catálogo KEV (CISA):** destaque de vulnerabilidades exploradas ativamente no mundo real.
- **Cobertura de patches e burndown:** acompanhe a redução do risco frente às metas de remediação.
- **SLA de remediação:** metas por severidade e priorização automática das violações.

3. Governança de risco e resposta a incidents

O **Guardeon Risk** análise o compliance do ambiente para tomada de decsiões e adequação a frameworks de segurança:

- **Matriz de risco:** probabilidade × impacto, com os incidentes de maior risco em destaque.
- **Análise de causa raiz:** agrupamento por causa e recomendações de ações preventivas.
- **SLA e MTTR por categoria:** tempo de resposta monitorado por tipo de incidente e severidade.

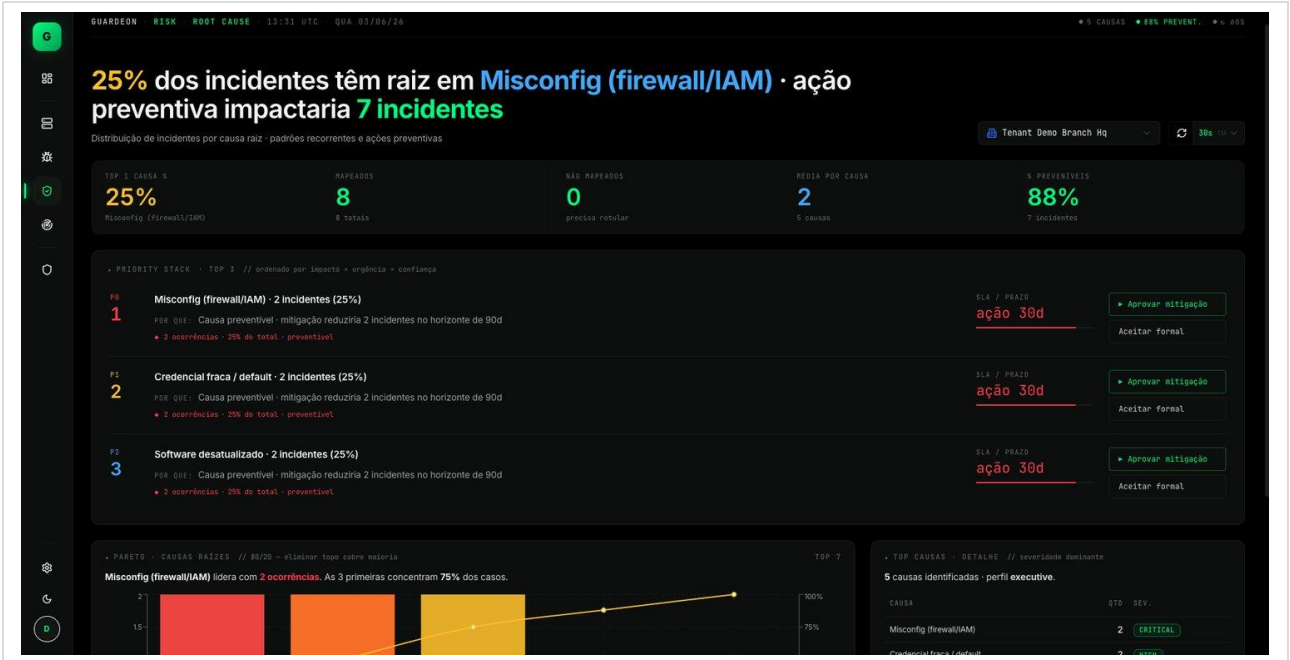

Figura 2. Guardeon Risk — análise de causa raiz e ação preventiva priorizada

4. Inteligência de ameaças (CTI) acionável

O **Guardeon CTI** monitora o ambiente externo, apresentando informações estratégicas para defesa cibernética:

- **IOCs e campanhas APT:** indicadores (IPs, domínios, hashes, URLs) correlacionados com campanhas ativas e com as detecções internas.
- **Monitoramento de domínios e exposição:** reputação, typosquatting/C2 e busca de e-mails corporativos em vazamentos.
- **Threat hunting e atribuição:** hipóteses associadas a táticas MITRE e catálogo de atores de ameaça com nível de confiança.

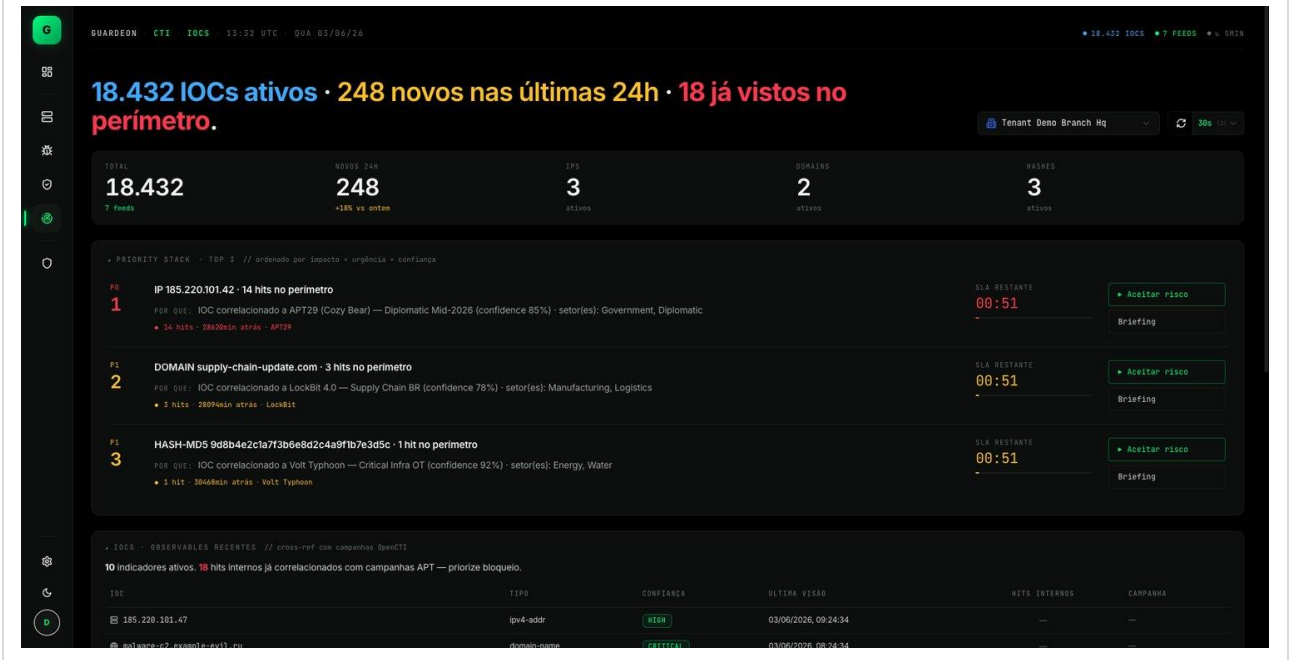

Figura 3. Guardeon CTI — IOCs ativos, novos indicadores e correlação com campanhas APT

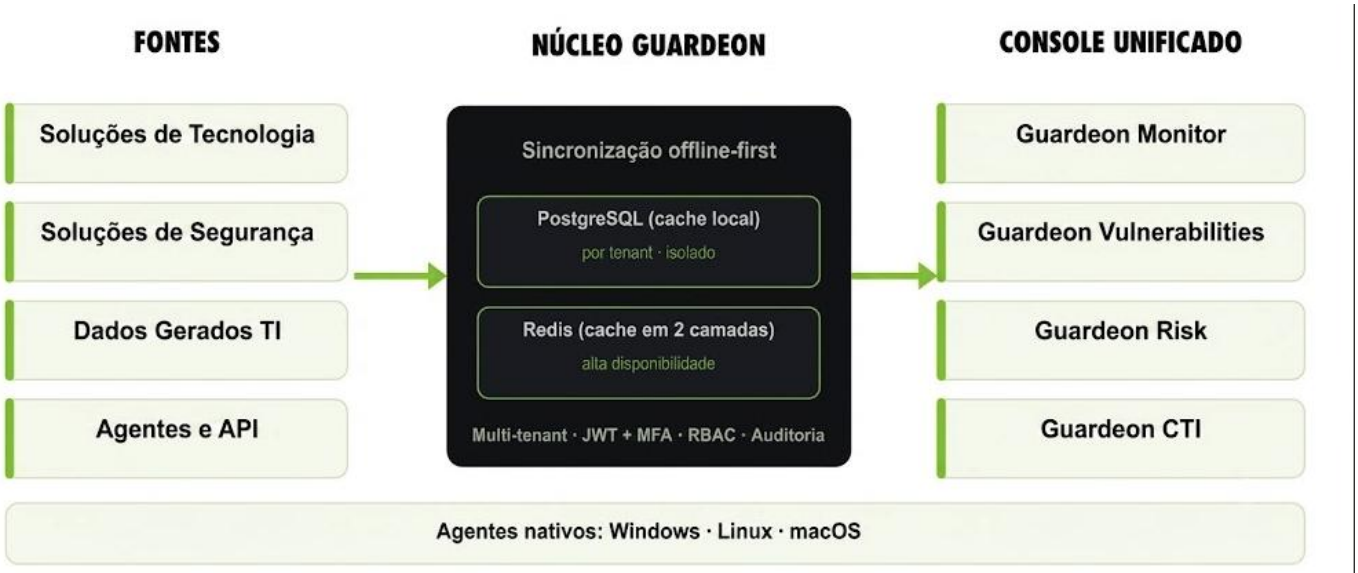

Figura 4. Arquitetura multi-tenant e offline-first do Guardeon

Cobertura completa de endpoints e ambientes

A partir de um único console e de agentes, o Guardeon monitora e protege todo o parque:

- **Agentes multiplataforma:** coleta nativa em Windows, Linux e macOS, para detecção em endpoints e servidores.
- **SIEM e Governança unificada:** alertas, regras e técnicas MITRE centralizados, com retenção e sincronização automatizadas.
- **Infraestrutura:** métricas de disponibilidade e capacidade via integração e convergência para ações priroizadas em infraestrutura e segurança.

Complementos e integrações

- **Threat Intelligence:** CTI para campanhas e intrusion sets; HIBP para exposição de credenciais; catálogo CISA KEV.
- **Busca e indexação:** consultas de alta performance sobre grandes volumes de eventos.
- **Forense e investigação:** linha do tempo por ativo, forense de rede e detalhamento de incidentes.
- **Segurança por padrão:** autenticação JWT com MFA (TOTP), controle de acesso por papel (RBAC) e trilha de auditoria.

Especificações técnicas

Arquitetura	Multi-tenant com isolamento de dados por cliente; tenant virtual para visão agregada; arquitetura offline-first (leitura sempre do cache/banco local).
Fontes & integrações	API, segurança, infraestrutura e catálogo CISA KEV.
Sincronização	Jobs em segundo plano: agentes, alertas, vulnerabilidades, métricas e limpeza/retenção; cache em duas camadas.
Detecção	Correlação por nível de regra e por técnica MITRE ATT&CK; evolução temporal e top agentes/regras.
Segurança & acesso	Autenticação JWT, MFA TOTP obrigatório, RBAC (admin/usuário + acesso global), sessões em Redis, cabeçalhos de segurança e trilha de auditoria.
Agentes	Coletores nativos para Windows, Linux e macOS, com instaladores dedicados.
Implantação	SaaS multi-tenant gerenciado ou on-premises em containers Docker.

Tabela 1. Especificações técnicas do Guardeon

Implantação e gestão flexíveis

- **SaaS multi-tenant gerenciado:** provisionamento automatizado e isolamento total de dados por cliente, sem o overhead de operar a infraestrutura.
- **On-premises / self-hosted:** containers Docker com administração total.

A conclusão: operações de segurança mais maduras

O Guardeon gera valor direto para o negócio, permitindo que seu SOC obtenha:

- **Menos trabalho manual:** correlação, triagem e priorização automatizadas por risco.
- **Resposta mais rápida e precisa:** foco em ameaças validadas e priorizadas, com SLA e MTTR monitorados.
- **Analistas mais capacitados:** tempo liberado para atividades estratégicas, como threat hunting e governança.

Recurso	Guardeon Platform
Monitoramento Frota de agentes, alertas 24h e evolução	✓
Cobertura MITRE ATT&CK Táticas, técnicas e priorização de gaps	✓
Performance do SOC MTTA, MTTD e MTTR com metas de SLA	✓
Multi-tenant & visão consolidada Isolamento por cliente e tenant GERAL	✓
Segurança & governança JWT + MFA, RBAC e auditoria completa	✓
Gestão de vulnerabilidades CVSS, Top CVEs e cobertura de patches	✓
Catálogo KEV (CISA) Vulnerabilidades exploradas ativamente	✓
Governança de risco Matriz e análise de causa raiz	✓
SLA & MTTR por severidade Metas, conformidade e violações	✓
CTI, IOCs e campanhas APT Correlação com detecções internas	✓
Threat hunting e atribuição Hipóteses MITRE e atores de ameaça	✓
Monitoramento de domínios Reputação, C2 e exposição de vazamentos	✓
Integração de infraestrutura Métricas de NOC	✓
Forense e detalhe de agente Linha do tempo e forense de rede	✓

Tabela 2. Módulos e capacidades do Guardeon

Guardeon by Vanelos · Plataforma Unificada de Cibersegurança

Fale com a gente: comercial@vanelos.com.br · www.vanelos.com.br