GUARDIAN AI

Guia do Guardian Antivirus

Análise local de arquivos, assinaturas e comportamento estático

Como o motor detecta tipos reais, hashes conhecidos, regras YARA, conteúdo suspeito e ameaças em arquivos compactados.

Versão 1.0 | Julho de 2026

Motor local integrado ao Guardian AI

fraudguardian.com.br

0. Comece aqui

Uma visão rápida para entender o Guardian Antivirus sem precisar conhecer análise de malware.

> **Uso em quatro passos**
> Envie ou anexe o arquivo ao Guardian, aguarde a identificação e a análise local, leia o veredito e consulte as evidências. O sistema não precisa executar o arquivo para produzir o diagnóstico.

Fluxo rápido

- 1. O arquivo é recebido pelo fluxo público ou como anexo de um e-mail.
- 2. O Guardian identifica o tipo real do conteúdo e calcula hashes criptográficos.
- 3. Hashes, regras YARA, análise estática e, quando aplicável, conteúdo compactado são avaliados.
- 4. As evidências são combinadas em score de 0 a 10, confiança e veredito explicável.

Leitura em 20 segundos

0-10	35-98%	4
NOTA DE RISCO	CONFIANÇA DO SCAN	FAIXAS DE VEREDITO

Nota de risco responde: “quão preocupantes são as evidências encontradas neste arquivo?” Confiança responde: “quanto material consistente o motor reuniu para sustentar esse diagnóstico?”

> **Regra de segurança**
> “Nenhuma ameaça forte identificada” não significa que o arquivo é comprovadamente seguro. Malware novo, conteúdo criptografado, regras incompletas e técnicas de evasão podem não produzir detecção.

O que diferencia este motor

O Guardian Antivirus é um componente local do Guardian AI. Ele combina assinaturas conhecidas com inspeção do conteúdo, detecção do tipo real e análise especializada por formato. A arquitetura foi desenhada para continuar operando mesmo quando um módulo opcional não estiver disponível.

Sumário

Estrutura desta documentação.

> **Escopo desta versão**
> Este documento descreve a implementação atual do Guardian Antivirus em julho de 2026. O motor faz análise estática e por assinaturas; ele não é uma sandbox de execução dinâmica.

1. O que é o Guardian Antivirus

O motor local de análise de arquivos do Guardian AI.

Guardian Antivirus é o subsistema responsável por analisar arquivos enviados diretamente ao site e anexos extraídos de e-mails. Seu objetivo é produzir um diagnóstico explicável sem depender de uma única assinatura ou de um único formato de arquivo.

A análise combina hashes conhecidos, regras YARA, detecção do tipo real, heurísticas estáticas, módulos especializados e inspeção recursiva de arquivos compactados. Cada descoberta é transformada em uma evidência com risco, confiança, severidade, descrição e origem.

O que o Guardian pretende responder

- O conteúdo corresponde exatamente a uma assinatura de malware conhecida?
- Há padrões YARA associados a famílias, técnicas ou comportamentos suspeitos?
- A extensão exibida corresponde ao tipo binário real do arquivo?
- O arquivo possui características estáticas relevantes, como macros, conteúdo ativo ou APIs suspeitas?
- Existe conteúdo perigoso escondido em ZIP, 7Z, RAR, TAR ou outros formatos compactados?
- As evidências, quando combinadas, justificam risco baixo, elevado, suspeito ou alto?

> **Importante**
>
> O Guardian Antivirus estima risco. Ele não executa o arquivo e não substitui análise dinâmica, engenharia reversa ou investigação pericial quando essas etapas forem necessárias.

2. Como o sistema funciona

Do upload ao veredito final.

1	2	3	4	5	6
Entrada	**Identificação**	**Assinaturas**	**Estática**	**Recursão**	**Score**
Arquivo ou anexo	Tipo real + hashes	Hash + YARA	Formato e heurísticas	Compactados internos	Risco e confiança

O engine central coordena as etapas. Se um componente falhar, o erro é registrado e as demais camadas continuam sempre que possível. Essa abordagem evita transformar uma dependência opcional em ponto único de falha.

3. O que é analisado

As principais camadas de evidência do Guardian Antivirus.

Tipo real	Magic bytes, subtipo ZIP e comparação entre conteúdo real, extensão declarada e MIME sugerido.
Hashes	MD5, SHA-1 e SHA-256 usados como identificadores para consulta na base local de malware conhecido.
YARA	Regras próprias e comunitárias para padrões binários, strings, famílias e comportamentos suspeitos.
Estática genérica	Entropia, dupla extensão e incompatibilidade entre extensão apresentada e conteúdo executável.
PE / ELF	Análise especializada de executáveis Windows e Linux quando o formato é reconhecido.
PDF	Procura características estruturais e conteúdo ativo relevante sem executar o documento.
Office	Inspeção de documentos OpenXML e OLE para sinais como macros, automação ou relacionamentos suspeitos.
Scripts	Indicadores em PowerShell, JavaScript, VBS, BAT/CMD, shell, Python e outros formatos textuais suportados.
APK / JAR	Análise inicial de pacotes Android e arquivos Java compactados.
Compactados	ZIP, TAR, GZIP, BZIP2, XZ e, com dependências opcionais, 7Z e RAR; filhos são analisados recursivamente.

Princípio de correlação

Nenhuma heurística genérica deve ser lida como prova isolada de malware. Uma extensão dupla ou entropia alta, por exemplo, ganha valor quando aparece junto de outras evidências.

4. Hash Engine e banco de assinaturas

Detecção exata de conteúdo conhecido.

O primeiro nível de reputação é baseado em hashes criptográficos. O arquivo recebe identificadores e o Guardian consulta uma base SQLite local de assinaturas. Quando há correspondência exata, o motor consegue reconhecer conteúdo conhecido sem executar o arquivo.

4.1 Hashes utilizados

MD5	Identificador legado ainda comum em bases de malware e feeds de assinaturas.
SHA-1	Hash intermediário mantido para compatibilidade com bases existentes.
SHA-256	Identificador principal e mais forte para rastreamento de conteúdo no Guardian.

4.2 Base local

A tabela malware_hashes guarda hash, tipo, tamanho, nome da assinatura, família quando conhecida, fonte, confiança e metadados. Registros são atualizados por hash, permitindo importar novas fontes sem duplicar a mesma assinatura.

4.3 Assinaturas ClamAV

O Guardian aceita a importação de arquivos de assinaturas de hash em formato compatível com ClamAV e também bases genéricas TXT, CSV e JSON. O objetivo é reutilizar inteligência existente em uma base local controlada pelo projeto.

> **Privacidade**
> A consulta de hash do Guardian Antivirus é local. O arquivo não precisa ser enviado a um serviço externo para que a base local seja consultada.

Evidência dominante

Uma correspondência forte no Hash Engine não deve ser diluída por sinais fracos de baixa relevância. Na implementação atual, uma assinatura de hash com risco muito alto força o score do arquivo a pelo menos 9,8/10.

5. YARA Engine e regras

Detecção baseada em padrões, contexto e metadados.

YARA permite descrever características que podem existir em arquivos maliciosos ou suspeitos: strings, sequências binárias, combinações lógicas e condições dependentes do próprio arquivo. O Guardian converte cada match em uma evidência explicável.

5.1 Como o Guardian carrega regras

- Procura arquivos .yar e .yara no diretório de regras, inclusive subdiretórios.
- Valida cada arquivo individualmente; uma regra quebrada não derruba todo o YARA.
- Recompila automaticamente quando nome, tamanho ou data de modificação das regras muda.
- Aplica timeout para impedir que uma regra excessivamente cara bloqueie o scan.
- Registra arquivos ignorados e erros de compilação para diagnóstico no Admin.

5.2 Metadados usados pelo Guardian

severity	critical, high, medium, low ou info.
confidence	Confiança da regra; aceita valor em escala 0-1 ou percentual interpretável pelo engine.
risk	Peso de risco de 0 a 10. Quando ausente, o Guardian usa um padrão baseado na severidade.
description	Explicação humana exibida no resultado.
family / category	Família de malware ou categoria técnica, quando disponível.
source	Origem ou autor da regra.

Exemplo simplificado

```
rule Guardian_Example
{
  meta:
    severity = "high"
    confidence = 85
    risk = 7
  strings:
    $a = "powershell" nocase
    $b = "EncodedCommand" nocase
  condition:
    $a and $b
}
```

> **Pacotes externos**
> O Admin pode receber conjuntos maiores, como pacotes comunitários. Regras incompatíveis continuam visíveis como erro e são ignoradas, enquanto os arquivos válidos permanecem ativos.

6. Detecção de tipo e análise estática

O nome do arquivo não é considerado verdade absoluta.

Antes de aplicar analisadores especializados, o Guardian examina bytes iniciais e estruturas internas para determinar o tipo real. ZIPs podem ser reclassificados como DOCX, XLSX, PPTX, APK ou JAR conforme os arquivos encontrados dentro do container.

6.1 Sinais genéricos

- Dupla extensão potencialmente enganosa, como documento.pdf.exe.
- Executável PE ou ELF apresentado com extensão de documento ou imagem.
- Entropia global elevada em executáveis, usada apenas como sinal auxiliar.
- Tipo MIME sugerido e extensão declarada registrados como contexto do relatório.

6.2 Analisadores especializados

PE	Executáveis Windows; estrutura e indicadores estáticos próprios do formato.
ELF	Executáveis Linux/Unix e metadados relevantes.
PDF	Estrutura do documento e sinais de conteúdo ativo ou ações potencialmente perigosas.
Office	OpenXML e OLE, com inspeção de macros, automação e relações internas.
Scripts	Padrões de download, execução, ofuscação e comandos sensíveis em linguagens suportadas.
APK / JAR	Inspeção inicial de pacotes Android e Java sem executar código.

> **Análise estática**
> O Guardian lê estrutura, bytes e conteúdo textual. Ele não executa macros, scripts, executáveis ou APKs durante o scan.

7. Arquivos compactados e análise recursiva

A ameaça pode estar dentro de outro arquivo.

Quando o arquivo é um container compactado, o Guardian tenta inspecionar seus membros e reaplica o mesmo pipeline a cada filho. Assim, um executável malicioso dentro de um ZIP pode elevar o risco do ZIP mesmo que o container externo não corresponda a nenhuma assinatura.

7.1 Formatos

ZIP, TAR, GZIP, BZIP2 e XZ são tratados diretamente. 7Z usa py7zr quando disponível; RAR usa rarfile e pode depender de backend de extração no sistema.

7.2 Proteções contra abuso

Arquivo principal	128 MB por padrão.
Membro compactado	64 MB por arquivo interno.
Expansão total	256 MB durante o scan.
Quantidade	Até 1000 arquivos internos.
Profundidade	Até 4 níveis de arquivos compactados aninhados.
Taxa de compressão	Limite padrão de 150x para reduzir risco de decompression bomb.

7.3 Situações especiais

- Path traversal: nomes que tentam escapar do diretório temporário são bloqueados.
- Arquivos protegidos por senha: o Guardian informa que parte do conteúdo ficou sem inspeção.
- Limites atingidos: o scan interrompe a expansão necessária para proteger o servidor.
- Risco do filho: o container herda o maior risco relevante encontrado no conteúdo interno.

> **Por que o pior filho importa?**
>
> Usar média seria perigoso: um ZIP com 99 arquivos inofensivos e 1 malware não deveria parecer seguro. O score do container considera o filho de maior risco.

8. Como o score é calculado

Risco, severidade e confiança são conceitos relacionados, mas diferentes.

8.1 Fórmula simplificada

> **Score de risco**
> O motor soma risco x confiança das evidências, desconta sinais protetivos quando existirem, aplica regras para evidências dominantes e limita o resultado entre 0 e 10.

Nota	Veredito	Interpretação prática
0,0 a 2,49	Nenhuma ameaça forte identificada	Poucos sinais relevantes foram encontrados. Isso não é uma certificação de segurança.
2,5 a 4,99	Risco elevado	Existem características que merecem atenção ou investigação adicional.
5,0 a 7,49	Arquivo suspeito	A combinação de evidências indica possibilidade relevante de conteúdo perigoso.
7,5 a 10,0	Alto risco de malware	Há sinais fortes; evite abrir ou executar até investigar a origem.

8.2 Evidências dominantes

- Hash conhecido de alto risco: score mínimo de 9,8/10.
- Regra YARA crítica: score mínimo de 8,8/10.
- Arquivo compactado: o score nunca fica abaixo do maior score de seus filhos.

8.3 Confiança

A confiança começa em uma base conservadora e aumenta conforme crescem a força e a quantidade das evidências. Na implementação atual ela fica entre 35% e 98%, podendo também herdar a confiança de um filho relevante em arquivos compactados.

> **Não é probabilidade de infecção**
> Confiança alta significa que o diagnóstico está apoiado por evidências mais fortes ou numerosas. Não significa uma probabilidade matemática de o arquivo ser malware.

9. Integração com e-mail e arquivos .eml

O antivírus é uma camada do Guardian, não um substituto do analisador de e-mail.

O motor central separa explicitamente os perfis EMAIL, FILE, TEXT e LINK. Isso impede que evidências específicas de e-mail sejam aplicadas por engano a um arquivo isolado.

9.1 Arquivo .eml

> **Regra de roteamento**
> Um .eml é interpretado como mensagem RFC822. O próprio contêiner .eml não é tratado como malware genérico; somente os anexos internos são enviados ao Guardian Antivirus.

1	2	3	4	5
.eml	**Headers**	**Conteúdo**	**Anexos**	**Antivírus**
Parser de e-mail	SPF/DKIM/DMARC	Texto + links	Extração segura	Scan dos anexos

9.2 Anexos dentro de e-mail

PDFs, imagens e demais arquivos são analisados no contexto do e-mail e o resultado técnico completo do antivírus permanece disponível no relatório. Para o score de fraude do e-mail, o resultado do anexo é transformado em uma evidência limitada, evitando que uma única dimensão apague sinais de remetente, conteúdo, links ou autenticação.

Score do arquivo	Evidência no e-mail	Uso
AV >= 9,0	Anexo identificado como malware	Evidência muito forte no e-mail.
AV >= 7,5	Anexo com alto risco de malware	Evidência forte.
AV >= 5,0	Anexo considerado suspeito	Evidência relevante.
AV >= 2,5	Anexo com sinais de risco	Evidência moderada.

Essa separação é importante: “alto risco de malware” descreve um arquivo; “grande chance de golpe” descreve a análise global de um e-mail.

10. Administração, dependências e configuração

Como manter o motor operacional e atualizar sua inteligência.

10.1 Painel administrativo

- Status do YARA Engine e das dependências opcionais.
- Upload e validação de regras .yar/.yara.
- Importação de bases de hashes e histórico de fontes.
- Scanner de teste para validar arquivos sem executar o conteúdo.
- Métricas da base: assinaturas, tipos de hash, fontes e tamanho do banco.

10.2 Dependências principais

yara-python	Compilação e execução das regras YARA.
pefile	Apoio à inspeção de executáveis PE do Windows.
py7zr	Leitura e extração controlada de arquivos 7Z.
rarfile	Leitura de RAR; determinados ambientes exigem um backend externo.

10.3 Configuração padrão

GUARDIAN_AV_MAX_FILE_BYTES	128 MB
GUARDIAN_AV_MAX_EXPANDED_BYTES	256 MB
GUARDIAN_AV_MAX_ARCHIVE_MEMBER_BYTES	64 MB
GUARDIAN_AV_MAX_ARCHIVE_FILES	1000
GUARDIAN_AV_MAX_ARCHIVE_DEPTH	4
GUARDIAN_AV_MAX_COMPRESSION_RATIO	150
GUARDIAN_AV_YARA_TIMEOUT	10 segundos

Fail-safe

Hash DB, YARA, análise estática e arquivos compactados podem ser habilitados ou desabilitados por configuração. Uma falha de um módulo é registrada em errors e não deve apagar resultados produzidos pelas outras camadas.

11. Limitações, privacidade e boas práticas

Como interpretar o resultado de forma responsável.

11.1 Limitações

- Assinaturas por hash só reconhecem conteúdo idêntico ao que já existe na base.
- Regras YARA podem gerar falsos positivos ou deixar de detectar variantes novas e ofuscadas.
- Análise estática não observa o comportamento real do programa em execução.
- Arquivos criptografados ou protegidos por senha podem esconder conteúdo que o motor não consegue inspecionar.
- Limites de tamanho, profundidade e expansão podem impedir a inspeção integral de pacotes extremos.
- Malware direcionado ou recém-criado pode não possuir assinatura ou padrão conhecido.

11.2 Privacidade

O motor foi desenhado para análise local. Hashes, YARA, heurísticas e descompactação são processados no ambiente Guardian. Essa arquitetura reduz a necessidade de enviar arquivos desconhecidos para serviços externos.

11.3 Boas práticas

- Não execute um arquivo apenas porque o score foi baixo.
- Considere origem, contexto, assinatura digital e expectativa do recebimento.
- Para incidentes importantes, preserve o arquivo e os hashes para investigação adicional.
- Atualize regularmente as bases de hashes e regras YARA utilizadas pelo ambiente.

> **Princípio de uso**
>
> O relatório reduz incerteza e organiza evidências. Em casos críticos, ele deve apoiar - e não substituir - investigação adicional.

12. Perguntas frequentes

Respostas rápidas para situações comuns.

O Guardian disse “nenhuma ameaça forte identificada”. Posso abrir?

Não é uma garantia. O resultado significa que as camadas disponíveis não reuniram evidências fortes naquele scan. Avalie também a origem e o contexto.

YARA encontrou uma regra. Isso prova que é malware?

Não necessariamente. A qualidade depende da regra. O Guardian usa severidade, risco, confiança e outras evidências para evitar tratar todo match como prova absoluta.

Por que o arquivo aparece como PE se termina em .pdf?

O Type Detector usa o conteúdo real. Um início MZ típico de executável Windows pode revelar um arquivo disfarçado com extensão de documento.

O Guardian abre ZIP, 7Z e RAR?

Sim, dentro dos limites de segurança. ZIP/TAR e formatos de stream são nativos; 7Z e RAR dependem das bibliotecas opcionais instaladas.

Arquivo protegido por senha é seguro?

Não. Significa apenas que o conteúdo interno não pôde ser totalmente inspecionado. O relatório deve indicar essa limitação.

O antivírus executa o malware em sandbox?

Não. A versão documentada é estática e baseada em assinaturas, estrutura e conteúdo. Execução dinâmica não faz parte deste motor.

Por que um .eml não aparece como arquivo comum?

Porque o Input Router reconhece RFC822 e envia o conteúdo para o pipeline de e-mail. Somente anexos internos são analisados como arquivos.

13. Glossário

Termos técnicos usados nesta documentação e nos relatórios.

Hash	Impressão digital calculada a partir do conteúdo de um arquivo.
MD5 / SHA-1 / SHA-256	Algoritmos de hash usados para identificar conteúdo e consultar assinaturas conhecidas.
YARA	Linguagem e mecanismo de regras para encontrar padrões em arquivos e memória.
Magic bytes	Bytes característicos no início ou estrutura de um arquivo usados para reconhecer seu tipo real.
PE	Portable Executable, formato comum de executáveis e bibliotecas no Windows.
ELF	Executable and Linkable Format, formato comum em sistemas Linux/Unix.
Entropia	Medida estatística da distribuição dos bytes; valores altos podem indicar compactação ou criptografia.
Decompression bomb	Arquivo pequeno que expande para volume excessivo de dados e pode consumir recursos do servidor.
Path traversal	Tentativa de usar caminhos como ../ para gravar ou acessar conteúdo fora do diretório permitido.
Análise estática	Inspeção de estrutura e conteúdo sem executar o programa.
Falso positivo	Arquivo legítimo classificado como suspeito ou malicioso.
Falso negativo	Arquivo malicioso que não foi identificado como de alto risco.

GUARDIAN AI

Guardian Antivirus

Análise local de arquivos baseada em assinaturas, YARA, estrutura e correlação de evidências.

fraudguardian.com.br

Versão 1.0 | Julho de 2026

> **Nota de versão**
> Esta documentação descreve a implementação atual do Guardian AI e pode ser atualizada conforme novas regras, assinaturas, módulos e controles de segurança forem adicionados.