vertip secure mail

Gateway de E-mail com Inteligência Artificial

REF: VSM-DS-2026 · v1.0 · ENTERPRISE

Gateway inteligente que analisa cada e-mail antes de chegar à caixa de entrada. Machine Learning, sandboxing de anexos e análise de reputação em tempo real bloqueiam phishing, spoofing e malware avançado antes de tocar o ambiente interno.

99.9%	<500 ms	IA + Sandbox	24/7
DISPONIBILIDADE	LATÊNCIA DE ANÁLISE	DUPLA CAMADA	MONITORAMENTO

VETOR #1 DE ATAQUE

E-mail corporativo é o principal vetor de ataque cibernético.

01 – Phishing com IA cria mensagens indistinguíveis de comunicações legítimas

02 – Malware polimórfico evade antivírus e filtros baseados em assinaturas

03 – Spoofing falsifica remetentes internos para autorizar fraudes e backdoors

04 – Um único e-mail comprometido gera exfiltração de dados e paralisa operações

FUNCIONALIDADES

Proteção Completa em Cada Camada

Do cabeçalho ao anexo. Da reputação do remetente à URL no corpo. Cada funcionalidade projetada para ameaças avançadas.

01

Machine Learning Anti-Phishing

Classificação probabilística de phishing por análise de linguagem, estrutura, contexto e comportamento do remetente.

02

Sandboxing de Anexos

Detonação de anexos suspeitos em ambiente isolado. Detecta malware polimórfico, droppers e técnicas de evasão.

03

Análise de URLs

Reescrita e verificação de URLs em tempo real. Detecta redirecionamentos, domínios recém-criados e páginas de credential harvesting.

04

Quarentena Inteligente

Retenção de mensagens suspeitas com classificação por severidade. Políticas de liberação por grupo, domínio ou tipo.

05

SPF/DKIM/DMARC Nativo

Validação completa de autenticação de e-mail. Rejeição ou marcação automática de mensagens que falham nas verificações.

06

Dashboard de Ameaças

Visão consolidada de ameaças detectadas, classificação por tipo, volume de bloqueios e tendências em tempo real.

07

Relatórios de Compliance

Relatórios periódicos com evidências de proteção, volumes processados e incidentes bloqueados para auditoria.

08

Políticas Granulares

Regras por domínio, grupo de usuários, tipo de anexo ou nível de risco. Controle fino sem complexidade operacional.

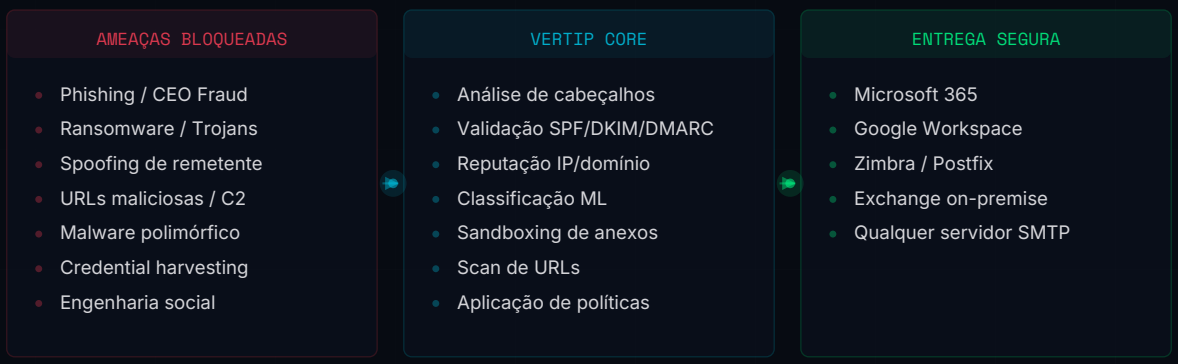
ENGINES DE ANÁLISE

ML Engine | Sandbox | SPF/DKIM/DMARC | Reputation | URL Scan | Heuristics

ARQUITETURA

Fluxo de Processamento

O Vertip opera como gateway MX, interceptando e analisando cada mensagem antes da entrega.



BENEFÍCIOS

O que muda com proteção inteligente

01 Bloqueio antes da caixa de entrada

Ameaças neutralizadas no gateway, antes de chegarem ao usuário. Reduz drasticamente a superfície de ataque.

02 IA que aprende e evolui

Modelos de ML treinados continuamente com dados reais. A proteção melhora a cada análise sem atualização manual.

03 Sandboxing sem impacto no fluxo

Anexos suspeitos detonados em paralelo. Entregas legítimas sem atraso perceptível ao usuário.

04 Visibilidade total de ameaças

Dashboard com classificação de ameaças, volume de bloqueios, tendências e detalhamento por tipo de ataque.

05 Relatórios executivos e técnicos

Evidências de proteção para auditorias, compliance e board report. Relatórios periódicos automáticos.

06 Quarentena com controle granular

Políticas por grupo, domínio ou tipo de ameaça. Liberação controlada sem expor o ambiente.

COMPARATIVO

Vertip vs. Gateway Genérico

Comparação detalhada de capacidades entre proteção dedicada com IA e filtros tradicionais.

CAPACIDADE	VERTIP	GATEWAY GENÉRICO
DETECÇÃO DE AMEAÇAS		
Machine Learning anti-phishing	Sim	Não
Sandboxing de anexos em ambiente isolado	Sim	Não
Análise comportamental de remetente	Sim	Não
Detecção de malware polimórfico	Sim	Não
Detecção de ameaças zero-day	Sim	Não
Modelos de IA atualizados continuamente	Sim	Não
AUTENTICAÇÃO E VALIDAÇÃO		
Validação SPF/DKIM/DMARC	Nativo	Parcial
Análise de reputação IP/domínio	Tempo real	Não
Detecção de spoofing/CEO fraud	ML + regras	Básico
Análise de URLs com reescrita	Sim	Não
Verificação de domínios recém-criados	Sim	Não
GESTÃO E CONTROLE		
Quarentena com políticas granulares	Sim	Não
Políticas por grupo/domínio/tipo	Sim	Não
Dashboard de ameaças em tempo real	Sim	Não
Relatórios de compliance automatizados	Sim	Não
Relatórios executivos periódicos	Sim	Não
Liberação controlada de quarentena	Sim	Não
INFRAESTRUTURA E CONFIABILIDADE		
Latência média de análise	<500ms	Variável
Disponibilidade garantida (SLA)	99.9%	Sem SLA
Compatibilidade M365 / Workspace / On-prem	Total	Parcial
Operação como gateway MX transparente	Sim	Parcial
Monitoramento de proteção 24/7	Sim	Não
Escalabilidade para grandes volumes	Sim	Limitado

SEGMENTOS

Para quem é o Vertip Secure Mail

Organizações que dependem do e-mail para operar e não podem ter caixas de entrada comprometidas.

01 Dados Sensíveis

Organizações com dados financeiros, pessoais ou estratégicos que não podem ter caixas de entrada comprometidas.

02 Financeiro e Bancário

Bancos, fintechs e seguradoras com requisitos regulatórios de proteção contra fraude via e-mail.

03 Educação

Ambientes com milhares de contas, alta rotatividade e alvos frequentes de phishing massivo.

04 Saúde e Hospitais

Proteção de dados de pacientes e comunicações médicas. Conformidade com regulações de privacidade.

05 E-commerce e Varejo

Proteção contra phishing de marca, comprometimento de contas e fraude com fornecedores.

06 Indústria e Manufatura

Proteção de supply chain, prevenção de ransomware via e-mail e segurança de ambientes OT.

07 Compliance Rigoroso

Empresas sujeitas a LGPD, ISO 27001, PCI-DSS que exigem proteção documentada.

08 Múltiplos Domínios

Infraestruturas com vários domínios de e-mail que precisam de proteção centralizada.

ESCALA

- **Milhões** de e-mails analisados mensalmente
- **<500ms** latência média de análise por mensagem
- **99,9%** de disponibilidade garantida
- **Monitoramento 24/7** proteção ativa e contínua

Solicitar Avaliação Técnica

Proteja sua operação de e-mail com inteligência artificial.

whatsapp +55 48 99212-2596

e-mail contato@memphisnetwork.com.br

plataforma www.memphisnetwork.com.br/vertip-secure-mail

www.memphisnetwork.com.br