



1. Visão Geral da UPX

Fundada em 2007, a UPX é referência em cibersegurança, operando scrubbing centers globais com capacidade superior a 98 Tbps e um SOC 24x7 certificado pela ISO 27001. A rede de mitigação da UPX cobre as Américas, Europa e Ásia-Pacífico, utilizando rotas anycast que proporcionam latência média inferior a 25 ms para 95% da internet brasileira. Entre os clientes atendidos pela empresa estão as operadoras Tier-1, bancos e órgãos governamentais.

2. Objetivo

Fornecer à **Telecomunicações Brasília, CNPJ 18.843.645/00001-51** uma solução gerenciada de detecção e mitigação de ataques DDoS com capacidade de tráfego limpo garantido de 3 Gbps, com burst até 30 Gbps. A proposta visa assegurar a disponibilidade, integridade e desempenho dos serviços oferecidos aos clientes finais da operadora.

3. Escopo e Cobertura Técnica

3.1 Proteção por Camada

A plataforma da UPX oferece cobertura completa das camadas L3 (Rede), L4 (Transporte) e L7 (Aplicação).

3.2 Matriz de Cobertura de Ataques

A solução cobre uma ampla gama de vetores de ataque, categorizados conforme abaixo:

- **Volumétricos:** UDP Flood, Fragmented UDP, TCP SYN/ACK/FIN/RST Flood, ICMP Flood, GRE Flood, entre outros, com técnicas como rate-limit, proxy, SYN Cookies, geo ACL e validações de header.
- **Amplificação/Reflection:** DNS, NTP, SNMP, CLDAP, LDAP, Memcached, com uso de filtros como EDNS clamp, suppression, payload signature.
- **Exaustão de Estado de Protocolo:** Proxy TCP Stateless, scrub de opções TCP, MSS clamp.
- **Aplicação:** HTTP GET/POST Flood, HTTP/2 Rapid Reset, Slowloris, GraphQL Abuse, SIP, WebSocket, com ML comportamental, WAF, proxy e limites de conexão.



- **Emergentes:** Carpet-bombing, ataques multi-vetores simultâneos com orquestração adaptativa.

A matriz contempla mais de 40 vetores de ataque, sendo a lista completa disponibilizada mediante solicitação.

4. Componentes

- **Edge Sensor (virtual):** Coleta de NetFlow, S-Flow e jFlow.
- **Sistema de Detecção:** Baseado em heurísticas e modelos de Machine Learning como Isolation Forest e LSTM, com acervo de 10 anos de dados.
- **Orquestrador:** Responsável pela decisão de desvio via BGP Flowspec ou comunidade RTBH.
- **Scrubbing Center:** Emprega filtros baseados em ASIC, eBPF e proxies L7.
- **Portal UPX Vision:** Fornece dashboards em tempo real, APIs REST e Webhooks.
- **Threat-Intel Feed:** Mais de 9 milhões de IPs maliciosos atualizados a cada hora.

5. Capacidade & Performance

Métrica	Garantia	Observação
Capacidade dedicada	3 Gbps	Burst on demand até 30 Gbps
Capacidade agregada rede	> 4 Tbps	Anycast global
IDS/IPS Throughput	Wire-speed	100 GbE sem packet-loss



Latência adicional	≤ 5 ms	Fora de ataque
Deteção	< 3 s	Mais de 95% de acurácia
Início de mitigação	≤ 10 s	Média de 7 s (referência Q4/2024)
SLA de disponibilidade	99,99%	Arquitetura multisite active-active



Thaís Fukasawa

Chief Revenue Officer

UPX