# CROWDSTRIKE & MDR 24X7

## CROWDSTRIKE FALCON

### SOLUÇÃO DE SEGURANÇA PARA ENDPOINTS NOMEADA LÍDER NO QUADRANTE MÁGICO DO GARTNER DE 2022 PARA PLATAFORMAS DE PROTEÇÃO (EPP/ EDR).

Para organizações que enfrentam desafios com a ineficiência e complexidade das soluções antivírus tradicionais, a solução Falcon Prevent™ da CrowdStrike® está pronta para te ajudar.

A solução Falcon Prevent proporciona uma proteção de excelência através de um único agente leve, uma arquitetura que opera sem a necessidade de atualizações de assinaturas constantes, infraestrutura de gerenciamento local ou integrações complicadas. Além disso, o Falcon não requer reinicializações para instalação ou para ajustes nas configurações de segurança.

## PREVENÇÃO DE ÚLTIMA GERAÇÃO

O Falcon Prevent oferece proteção para endpoints contra uma ampla gama de ataques, desde malwares comuns até ameaças sofisticadas, mesmo quando você estiver offline.

Ele incorpora a inteligência de ameaças líder do setor da CrowdStrike, integrada à CrowdStrike Security Cloud, para bloquear proativamente atividades maliciosas.

## PROTEÇÃO A PROVA DE MANIPULAÇÃO

A proteção contra adulteração impede o usuário ou o processo de tentar manipular ou desativar o agente CrowdStrike Falcon.

## LÍDER EM SEGURANÇA CIBERNÉTICA, INOVADORA E VISIONÁRIA

**Figure 1: Magic Quadrant for Endpoint Protection Platforms**


Source: Gartner (December 2022)

# PRINCIPAIS FUNCIONALIDADES

Construa uma defesa cibernética abrangente com nossa suíte de segurança, incorporando Next Gen AV, resposta em tempo real, análise de dados de ameaça estendida e threat hunters especializados.

Adote o gerenciamento de vulnerabilidades inteligente e aproveite a retenção estendida da Telemetria na nuvem para uma proteção completa sob a asa da CrowdStrike.

## PREVENT

**NEXT GEN AV (NGAV)**

É o módulo responsável por realizar as detecções e bloqueios (Machine Learning, Exploits, Behaviors/IoAs, Remediação)

## INSIGHT

**MÓDULO DE EDR**

Responsável coletar e armazenar toda a telemetria gerada pelos agentes. Traz também a capacidade de gerar um Zero Trust Assessment (ZTA) score, para uso em Workflows e integrações com terceiros. Habilita o app de Investigate e uma série de dashboards e visualizações para acelerar o trabalho do Analista/Responder.

## OVERWATCH

**TIME DE THREAT HUNTERS DA CROWDSTRIKE**

Têm suas próprias ferramentas de hunting na Telemetria Global da Crowdstrike + conexão direta com Threat Intel. É o time que identifica os ataques mais furtivos (low and slow).

## CONTROL & RESPONSE

**REAL TIME RESPONSE (RTR)**

É o módulo responsável por realizar o confinamento do computador (isolar da rede, com comunicação restrita), bem como por proporcionar ao analista um shell na máquina para execução de comandos diversos e scripts. Fundamental para uma Resposta a Incidentes.

## SPOTLIGHT

**RESPONSÁVEL POR VULNERABILITY MANAGEMENT, IDENTIFICANDO VULNERABILIDADES NO S.O. E APLICAÇÕES**

Possui o diferencial chamado Expr.ai, que correlaciona as vulnerabilidades com informações de Threat Intel, repriorizando-as de acordo com esse resultado (ex: um CVE médio altamente explorado acaba sendo mais importante que um CVE alto sem exploits disponíveis).

## THREAT GRAPH EXTENDED PLUS

**TECNOLOGIA QUE SUPORTA O INSIGHT (EDR)**

Essa licença terá 30 dias de retenção online da Telemetria em nossa nuvem.

# Solução MDR

## MELHORE SUA CAPACIDADE DE MONITORAR, IDENTIFICAR E RESPONDER A AMEAÇAS DE SEGURANÇA DE FORMA EFICAZ E OPORTUNA.

O serviço de MDR (Managed Detection and Response) da inov.TI é uma estratégia proativa para aprimorar a segurança cibernética da sua empresa, fornecendo monitoramento, detecção, análise e respostas avançadas a ameaças cibernéticas, com o apoio do nosso time de especialistas em segurança, aliviando assim a carga de segurança da sua empresa e permitindo que ela se concentre no seu principal negócio.

## COMPONENTES DO SERVIÇO DE MDR

### MONITORAMENTO DE AMBIENTE EM TEMPO REAL

- Sincronia dos endpoints com a plataforma de gerenciamento;
- Notificações proativas pelos analistas do SOC 24x7.

### DETECÇÃO PROATIVA DE AMEAÇAS

- Alertas gerados automaticamente;
- Categorização de alertas por criticidade

### SUPORTE / REMEDIAÇÃO / SOLUÇÃO

- Sugestão de implementações de patches e soluções de segurança;
- Acompanhamento de atividades de remediação / solução.

### RESPOSTA (*)

- Análise e Investigação de ameaças detectadas;
- Geração de relatório forense (ataque, remediação e solução final).

**Elemento integrante da solução MDR Enterprise.*