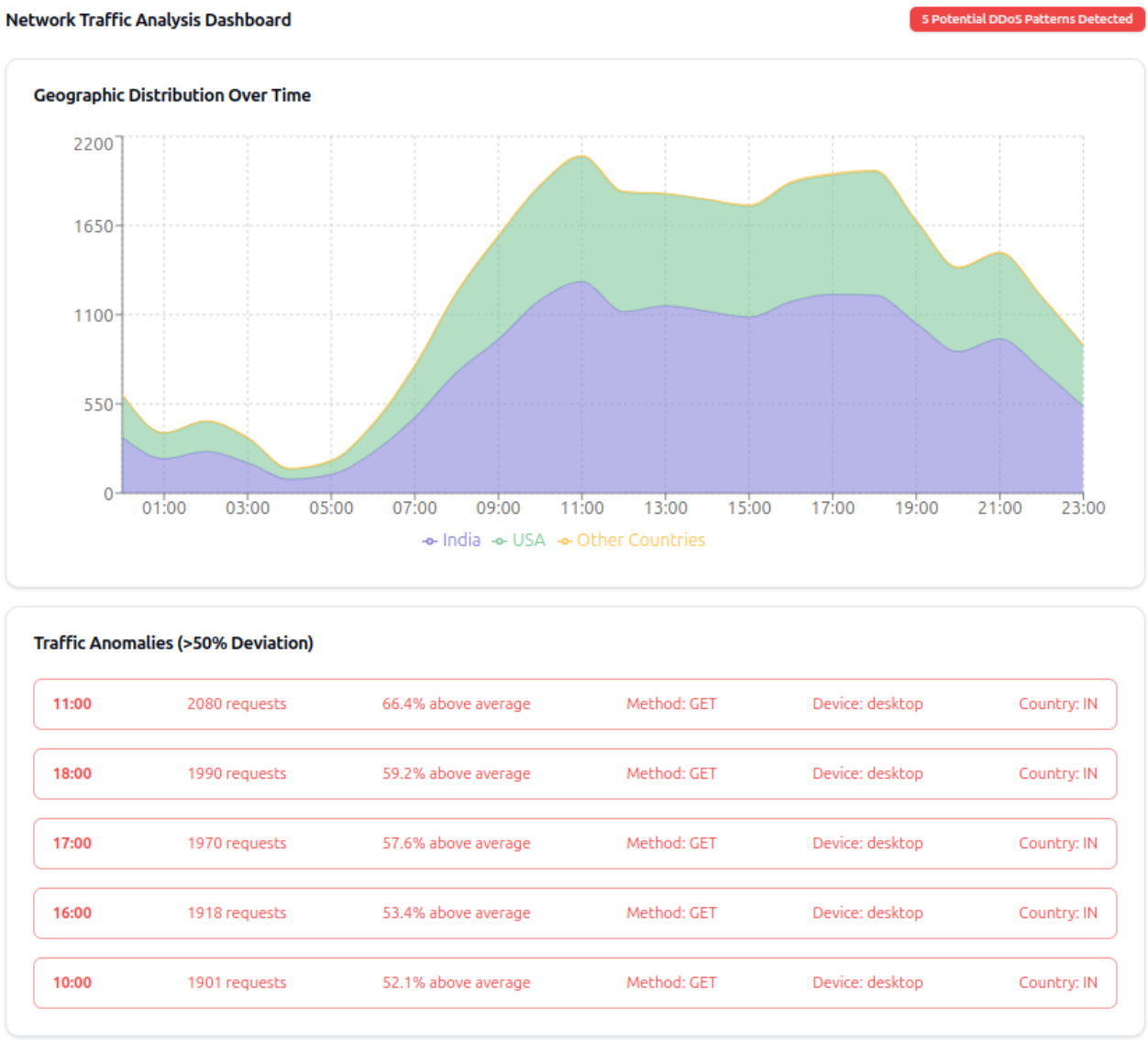

Com base na análise dos dados de tráfego de rede, segue abaixo as principais descobertas:

1. Volume e Distribuição de Tráfego:
    - Total de Requisições: 30.000
    - IPs Únicos: 18.589
    - Agentes de Usuário Únicos: 2.618
2. Distribuição de Métodos de Requisição:
    - GET: 24.967 (83,2%)
    - POST: 4.558 (15,2%)
    - OPTIONS: 385 (1,3%)
    - Outros métodos (PATCH, PUT, DELETE, HEAD): <1%
3. Distribuição por Tipo de Dispositivo:
    - Desktop: 14.720 (49,1%)
    - Tablet: 11.033 (36,8%)
    - Mobile: 4.247 (14,1%)
4. Distribuição Geográfica:

    - Índia: 18.372 requisições (61,2%)
    - EUA: 11.481 requisições (38,3%)
    - Outros países (Brasil, Japão, Reino Unido): <1%
5. Anomalias Detectadas:
    - 187 IPs apresentando comportamento suspeito
    - Critérios de anomalia:
        - Volume de requisições > 2x média
        - Variedade incomum de métodos (>3 métodos)
        - Origens de múltiplos países
6. Preocupações de Segurança:
    - Alta concentração de tráfego de dois países (99,5%)
    - Presença de métodos potencialmente perigosos (DELETE, PUT)
    - Número significativo de IPs anômalos (aproximadamente 1% do total)
7. Padrões Notáveis:
    - Uso predominante de métodos GET/POST (98,4%)
    - Distribuição de tráfego predominante em desktop
    - Alto número de agentes de usuário em relação ao número de IPs

Recomendações:

1. Implementar monitoramento mais rigoroso para os 187 IPs anômalos
2. Revisar e possivelmente restringir métodos HTTP perigosos
3. Investigar o alto número de agentes de usuário para potencial falsificação
4. Configurar controles de acesso baseados em localização devido às fontes de tráfego concentradas
5. Adotar Política sugerida (anexo)