CyberSec
TECH DAY

cisco

Mais que tecnologia

LOGICALIS
Architects of Change

NTT

teletex

Conformidade e Detecção de Ameaças

Potencializando seu investimento em infraestrutura de redes

Fabiano Furlan
Especialista em Cybersegurança - CX

Agenda

Visão geral

Visibilidade contextual em toda a rede

Análise preditiva de ameaças

Detecção e resposta automatizadas

Demonstração

Visão Geral do Secure Network Analytics

Desafios de complexidade à medida que as superfícies de ataque crescem

Necessidade de visibilidade de ponta a ponta

Desafios para os times do NOC / SOC

Como posso garantir que as políticas de segurança de rede estão devidamente aplicadas?

Como posso saber as aplicações / protocolos / portas que estão em uso por cada departamento?

Como faço para monitorar o tráfego dos usuários quando estão fora da rede corporativa / VPN?

Como posso identificar atividades suspeitas de movimentação lateral / *data hoarding* a partir da infraestrutura?

Como posso ter visibilidade de tráfego de equipamentos não gerenciados / IOT?

Os tipos de algoritmos criptográficos em uso estão de acordo com os padrões corporativos?

Secure Network Analytics

Cisco XDR

Extended Detection and Response com Cisco XDR. A análise avançada amplia as detecções locais com inteligência e integrações globais para resposta acelerada

Aprendizado de máquina multicamadas

Combinação de técnicas supervisionadas e não supervisionadas para condenar ameaças avançadas com alta fidelidade

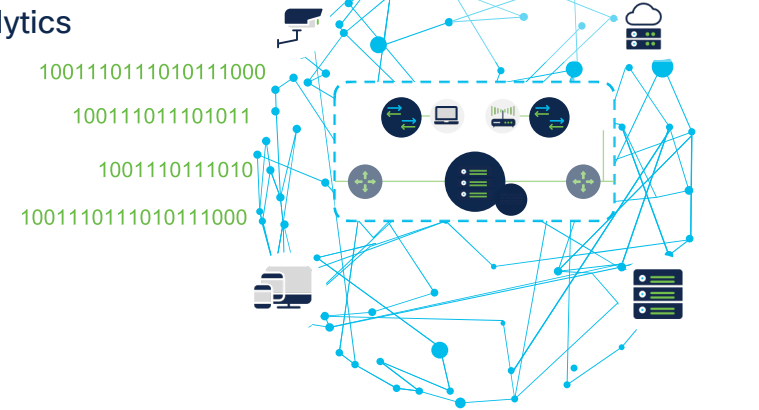
Modelagem comportamental

Análise comportamental de cada atividade dentro da rede para identificar anomalias

Secure Network Analytics

Coleção de dados

Telemetria avançada da infraestrutura de rede existente incluindo telemetria aprimorada para análise de tráfego criptografado



Telemetria dos dispositivos

Insights de dispositivos e processos com telemetria de fluxo do Cisco Secure Client

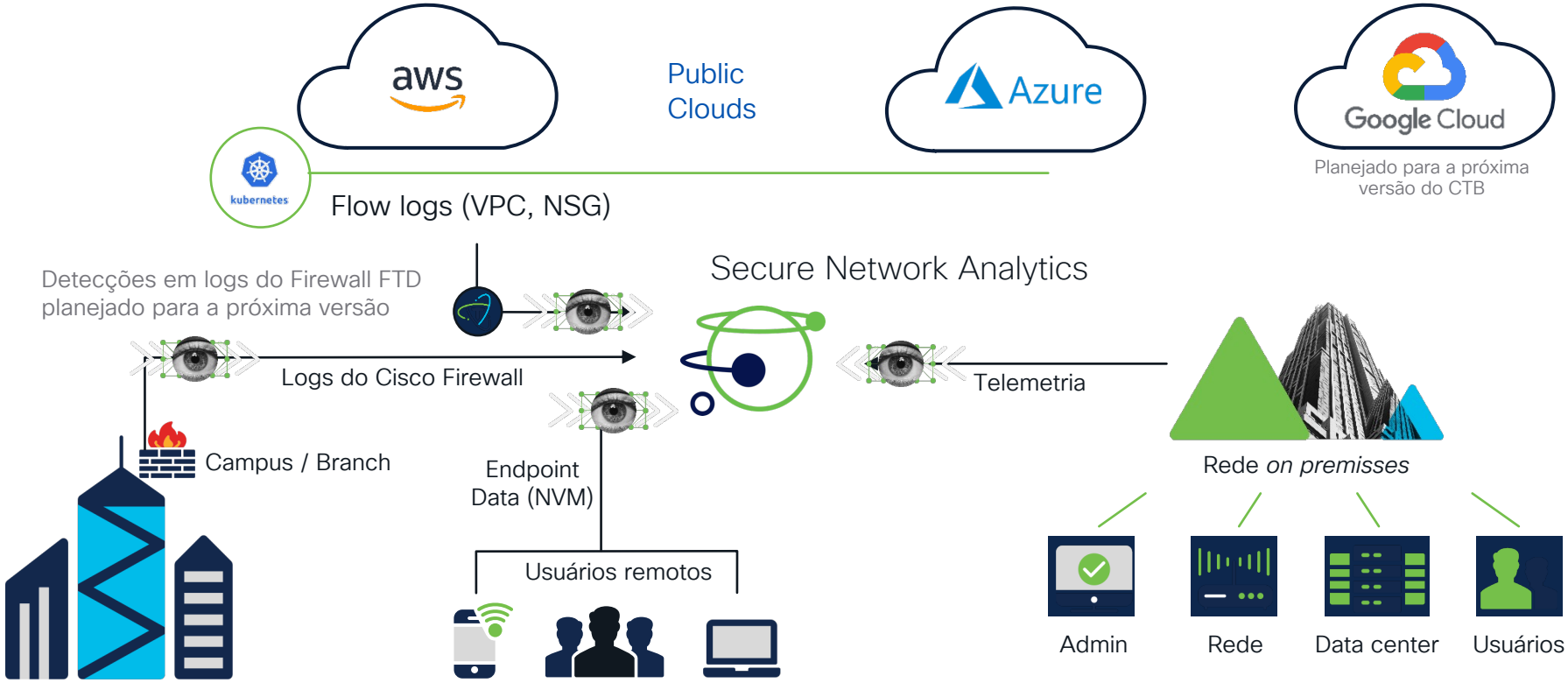
Visibilidade contextual em toda a rede

Sem agentes
Visibilidade sem agentes em toda a empresa, *on premises* e multicloud

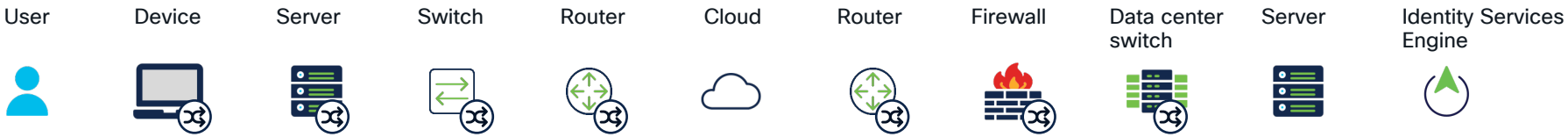
Inteligência acionável
enriquecida com contexto do usuário, dispositivo, localização, time stamp, aplicação e etc.

Segmentação mais inteligente
com conhecimento de quem está na rede e o que está fazendo

Ingestão de multi-telemetria e visibilidade



Visibilidade de infraestrutura fim a fim



NetFlow Export está disponível em todo o portfólio da Cisco

Switch
Catalyst 2960-X (v9/IPFIX)
Catalyst 3650/3850 (v9/IPFIX)
Catalyst 4500E (v9/IPFIX)
Catalyst 6500E (v9/IPFIX)
Catalyst 6800 (v9/IPFIX)
Catalyst 9200 (v9/IPFIX)
Catalyst 9300 (v9/IPFIX ETA)
Catalyst 9400 (v9/IPFIX ETA)
Catalyst 9500 (v9/IPFIX)
Catalyst 9600 (v9/IPFIX)
IE3000 (v9/IPFIX)
IE4000 (v9/IPFIX)
IE5000 (v9/IPFIX)

Router
Cisco ISR 4431 (v9/IPFIX ETA)
Cisco CSR 1000v (v9/IPFIX ETA)
Cisco ASR 1000/1001/1002 (v9/IPFIX ETA)
Cisco ASR 9000 (v9/IPFIX)
Cisco WLC 5520, 8510, 8540 (v9 Enhanced)
Catalyst 8000 (v9/IPFIX ETA)
Catalyst 9800 (v9/IPFIX ETA)

Meraki
MX/Z (v9 Enhanced v14.5)
MS390 (IPFIX Enhanced/ETA v15.1)

Data center switch
Nexus 1000v (v9/IPFIX)
Nexus 3000 (sFlow)
Nexus 7000 (M Series – v9/IPFIX)
Nexus 7000 (F Series– v9/IPFIX sampled)
Nexus 9000 Series (sFlow)
Nexus 9000 Series EX/FX (v9)

Firewall
ASA 5500-X (NSEL,Syslog)
FTD (NSEL,Syslog)

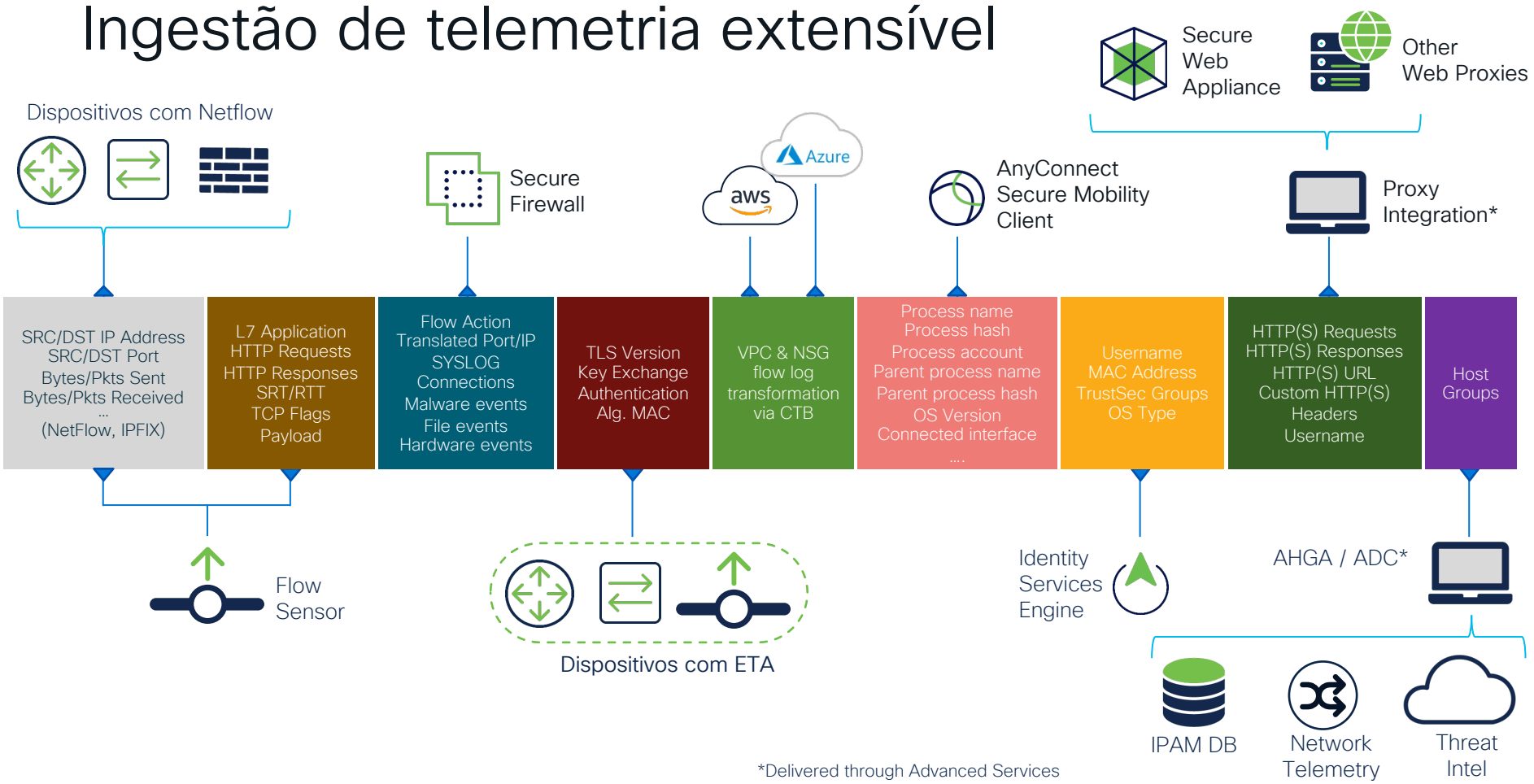
Endpoint
Cisco Secure Client (IPFIX)
AnyConnect (IPFIX)

Cloud
AWS
Azure
(Flow Logs via CTB)

Servers, software
SNA Flow Sensor (v9/IPFIX ETA)
Cisco UCS VIC (v9/IPFIX)

A lista acima é uma lista não exaustiva. Para recursos individuais de cada produto, consulte o Cisco feature navigator: https://cfnng.cisco.com/

Ingestão de telemetria extensível

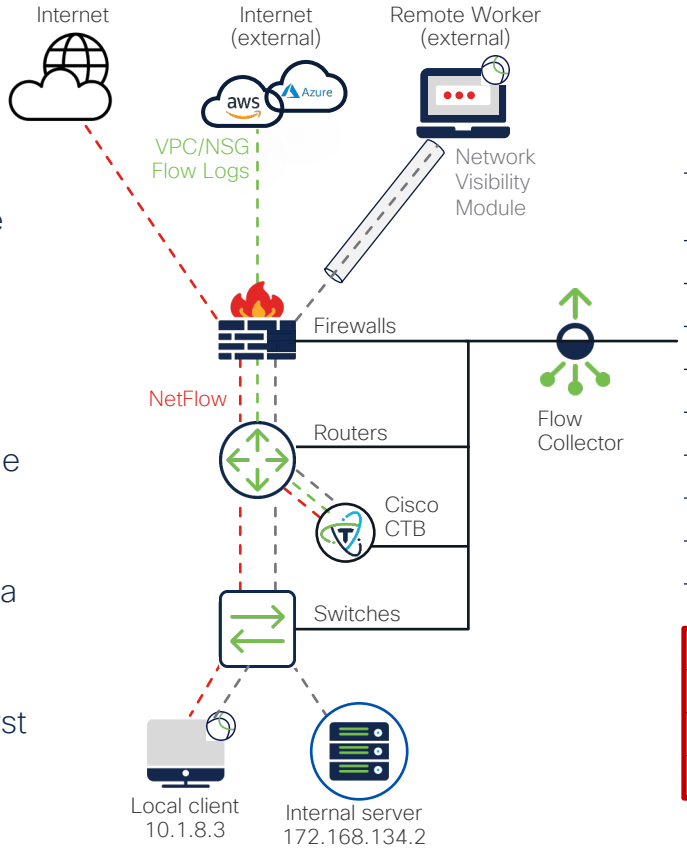


*Delivered through Advanced Services

A rede é a fonte da verdade

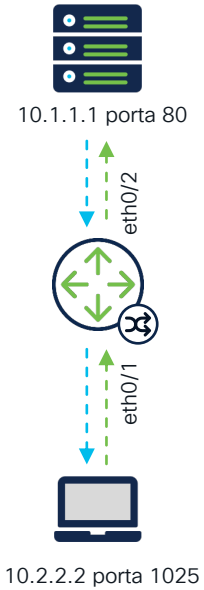
Veja TUDO!

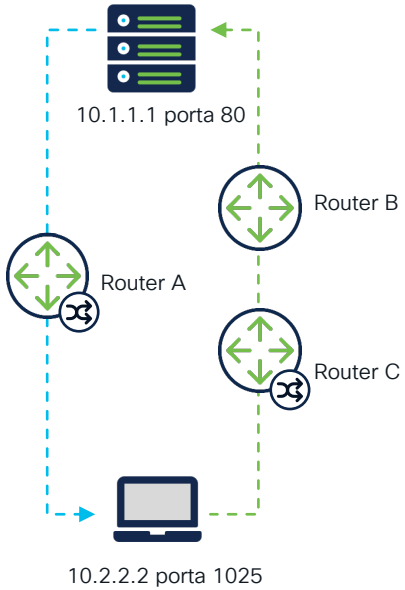
- Um traço de cada conversa
- Coleta de informações sem agente
- Coleta de dados do dispositivo do trabalhador remoto (NVM)
- Ingestão de telemetria em nuvem (registros dos fluxos)
- Visibilidade de tráfego leste-oeste e norte-sul (registros Cisco FTD e NSEL)
- Coleta leve de metadados usando a infraestrutura existente
- Capture NetFlow aprimorado nas plataformas Cisco ASR, ISR, Catalyst 9000 e Meraki (GTA)



Flow information	Packets
Source address	10.1.8.3
Destination address	172.168.134.2
Source port	47321
Destination port	443
Interface	Gi0/0/1
IP TOS	0x00
IP protocol	6
Next hop	172.168.25.1
TCP flags	0x1A
Source SGT	100
:	:
ETA meta data	IDP | SPLT
Application name	NBAR SECURE-HTTP
Process Name	chrome.exe
Process Account User	Acme/john

Processamento de telemetria: sessões de ponta a ponta





Data Deduplication / Stitching

- Flow stitching: simétrico e assimétrico
- Dos dados às informações da sessão
- Armazenamento eficiente de dados de telemetria
- Necessário para relatórios precisos em nível de host
- Nenhum dado é descartado: elementos de dados únicos são gravados no banco de dados

Registro de telemetria bidirecional

Start time	Client IP	Client port	Server IP	Server port	Proto	Client bytes	Client Pkts	Server bytes	Server Pkts	Interfaces
10:20:12.221	10.2.2.2	1025	10.1.1.1	80	TCP	2027	5	28712	17	eth0/1 eth0/2

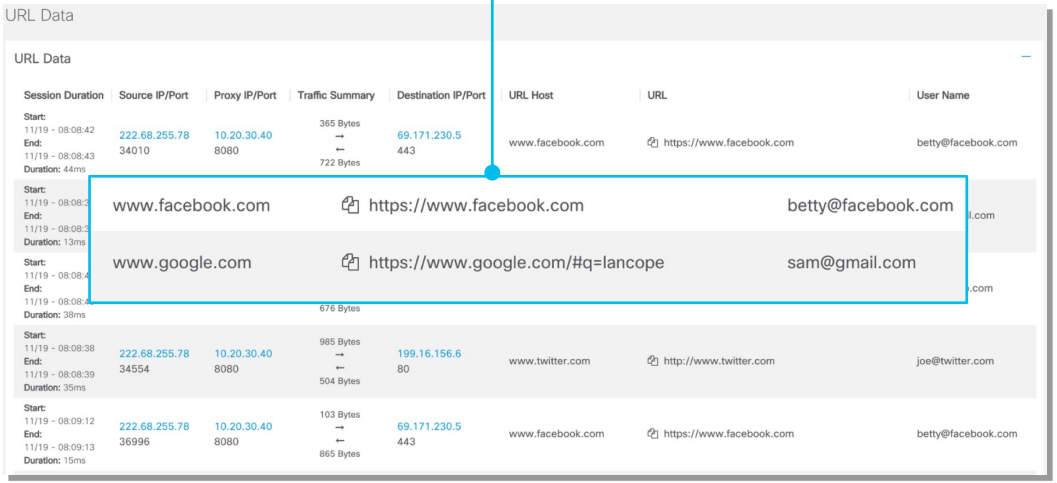
Capacidades forenses avançadas a partir da integração com proxy

Web proxy

Secure Network Analytics

SYSLOG information	Pacotes
Timestamp	1456312345
Elapse time	12523
Source IP	192.168.2.100
Source port	4567
Destination IP	65.12.56.123
Destination port	80
Bytes	400
URL	http://cisco.com
Username	john

Visibilidade de URL da Web



- Cisco Secure Web Appliance
- Bluecoat proxy
- Squid
- McAfee web gateway

Dispositivos de rede: registros de telemetria NVM

Dispositivo do usuário
AnyConnect / Secure Client

Flow Collector

Data Store

Telemetria NVM
- Sessão
- Interface
- Usuário
- SO
- Processo

Start Time*
End Time*
Source IP*
Source Port*
Destination IP*
Destination Port*
Bytes Sent*
Bytes Received*
Packet Count* (derived)
Protocol*

Interface Info UID
Interface Index
Interface Type
Interface Name
Interface Details List
Interface Mac Addr.

UDID
User
User Account Type
Agent Version
Virtual Station Name
OS Name
OS Version
OS Edition
System Manufacturer
System Type

Process Account*
Process Account Type
Process ID
Process Name*
Process Hash*
Process Path
Process Args
Parent Process ID
Parent Process Account
Process Account
Parent Process Name*
Parent Process Hash*
Parent Process Path
Parent Process Args
Host Name
DNS Suffix
Module Name List
Module Hash List
Parent Process Name
Parent Process Hash

* Registros de telemetria NVM disponíveis em implantações sem Data Store

Retenção extendida e visualização de logs de firewall

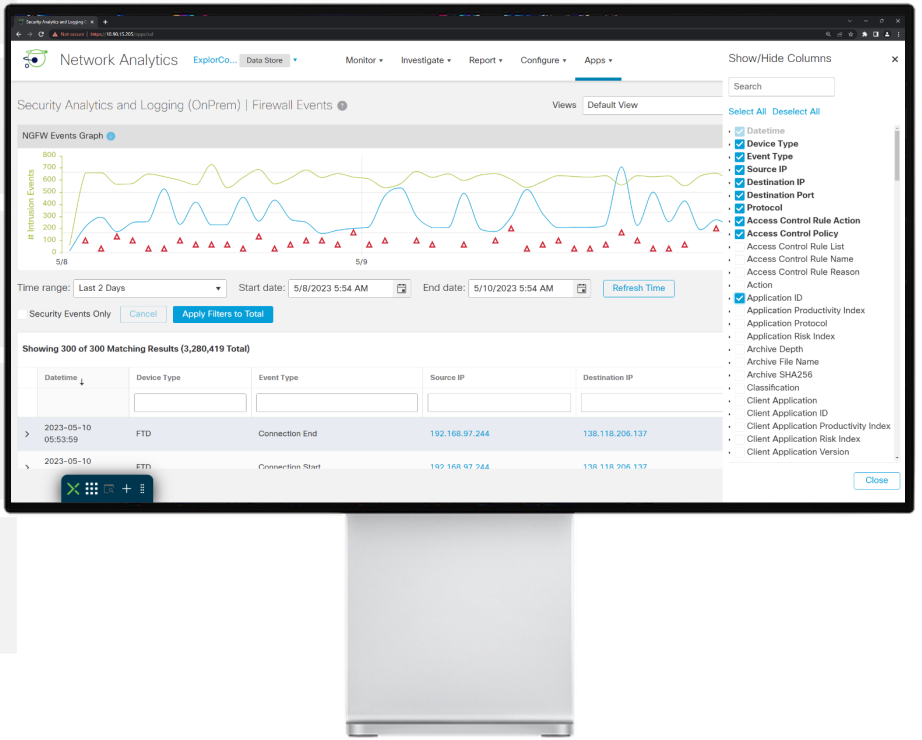
FTD (incluindo os logs do data plane) e ASA em um armazenamento de dados escalonável hospedado localmente

O assistente de log no FMC 7.0+ simplifica a configuração de registro no local e na nuvem

Capacidade extendida para logging e analytics drasticamente aumentada no FMC 7.0+ scale por uma magnitude significativa de 300X por meio de consulta remota no SNA

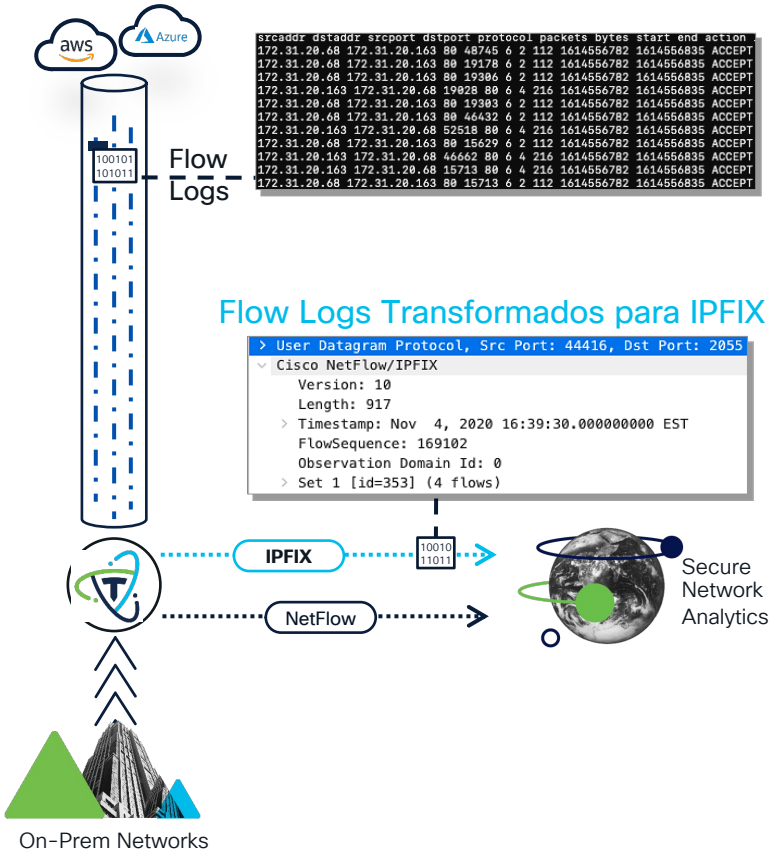
Faça o pivô diretamente do Event viewer para o Secure Network Analytics para contexto aprimorado

Suporte a vários Flow Collectors com mapeamento de Firewall para Flow Collector



Monitorando seu ambiente de nuvem híbrida

- Os Cloud Flow Logs da AWS e do Azure fornecem informações sobre as atividades dos hosts que residem em ambientes de nuvem
- Os metadados dos logs de fluxo giram em torno da atividade da rede, semelhante ao NetFlow/IPFIX
  - Há um total de 25 campos fornecidos nos Flow logs
- CTB puxa Flow Logs dos AWS S3 buckets e armazenamento Azure BLOB através de uma conexão HTTPS e transforma a telemetria em IPFIX
  - Depois que o fluxo VPC é transformado, ele é encaminhado aos consumidores



Visibilidade contextual em toda a rede

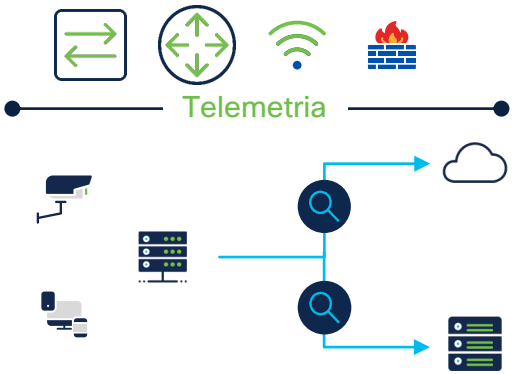
Sem agentes
Visibilidade sem agentes em toda a empresa, on premises e multicloud

Inteligência acionável
enriquecida com contexto do usuário, dispositivo, localização, time stamp, aplicação e etc.

Segmentação mais inteligente
com conhecimento de quem está na rede e o que está fazendo

Visibilidade de tráfego

A telemetria da rede e da nuvem fornece visibilidade de tráfego até a camada 4



Atribuição do dispositivo

Quem está por trás do IP descoberto? Que dispositivo eles estão usando? Onde eles estão localizados?

Quem: Usuário

O que: Tipo de dispositivo

Quando: Horário de login

Onde: Localização

Como: Postura de segurança

Processo: no dispositivo

Indicação de tráfego

Que tipo de tráfego um IP está enviando? Qual aplicativo de camada 7 é usado? Qual URL é acessada?

Aplicação: Layer 7 App

Web: Identificação de URL

NAT: Informação do NAT

Crypto: Versão de TLS

Estado do tráfego: ISE ANC Quarantine

Intrusão: Malware ou Evento de arquivo

Visibilidade de comunicação | Identidade | Contexto

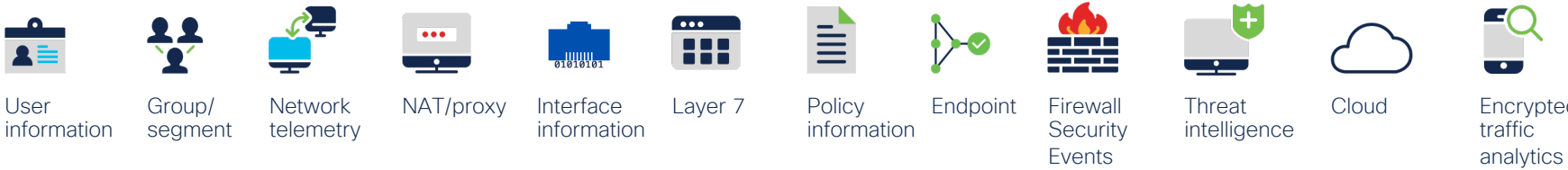
Telemetria aprimorada por meio de integrações diretas de produtos e via Cisco XDR

Inteligência acionável contextual

Dados da sessão | 100% responsabilidade da rede

Client	Server	Translation	Service	User	Application	Process #	Traffic	Group	Mac	SGT	Encryption TLS/SSL version
1.1.1.1	2.2.2.2	3.3.3.3	80/tcp	Doug	http	beab09fe3 45ac3217d d80fd46c...	20M	location	00:2b:1f	10	TLS 1.2

Visibilidade



Visibilidade contextual em toda a rede

Sem agentes
Visibilidade sem agentes em toda a empresa, on premises e multicloud

Inteligência acionável
enriquecida com contexto do usuário, dispositivo, localização, time stamp, aplicação e etc.

Segmentação mais inteligente
com conhecimento de quem está na rede e o que está fazendo

Segmentação funcional da rede por grupos

Um grupo de hosts é um agrupamento de hosts que compartilham atributos e políticas

O grupo de hosts é monitorado para estabelecer limites e comportamento de linha de base

Alertas são enviados quando os hosts se comportam fora do comportamento do grupo

3 maneiras de segmentar:

1. Criação manual de grupos de hosts
2. APIs usando dados IPAM, IND e Threat Intelligence
3. Serviço de automação de grupo de hosts

Casos de uso relevantes:
Network Segmentation and Policy development

Visualize comunicações de grupo entre SGTs

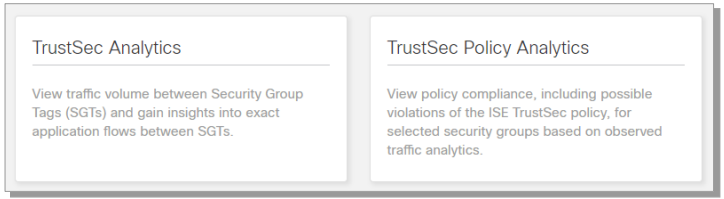
- Relatório sobre todas as comunicações observadas do grupo SGT
- Veja rapidamente quais SGTs estão comunicando
- Clique em qualquer célula para exibir a quantidade de dados transmitidos
- Visualize até 300 SGTs

No traffic seen

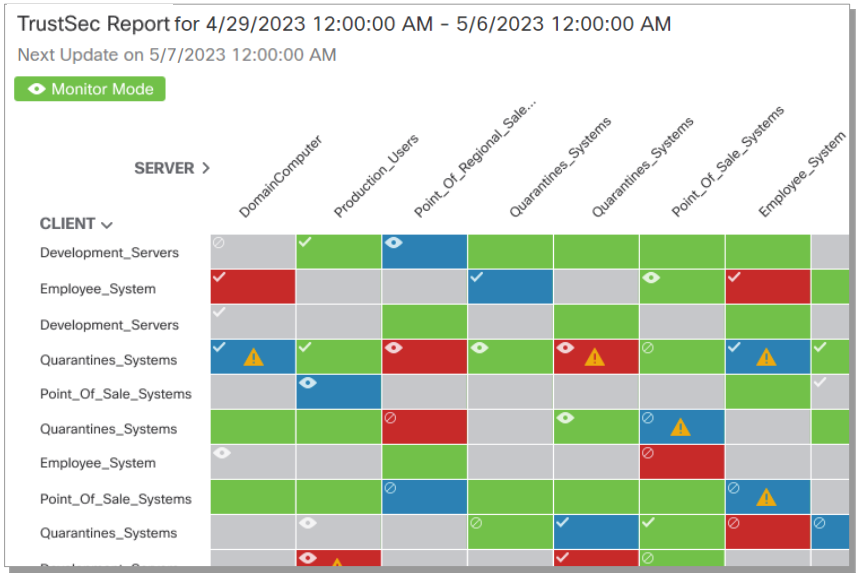
Traffic seen, default policy allows IP traffic

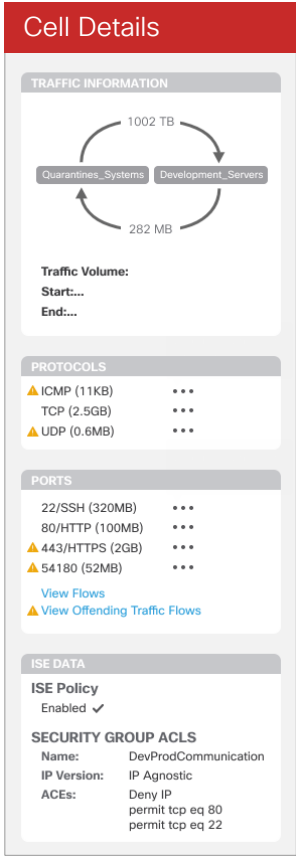
Traffic seen, policy allows some traffic and has default Deny IP

Traffic seen, policy is complex,



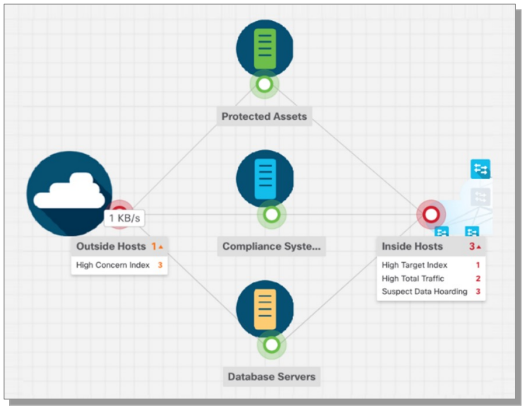
90 dias de dados históricos de política





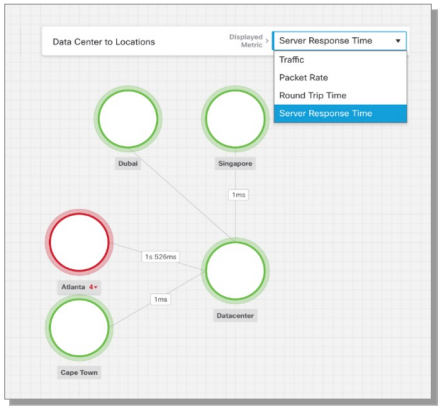
Crie mapas para focar em métricas críticas

Alarmes disparados



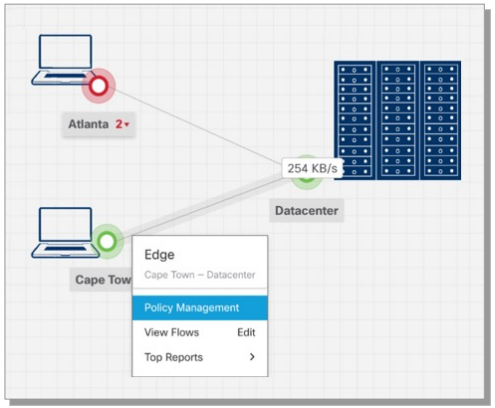
- Veja o resumo dos alarmes acionados por grupos de hosts
- Detalhes dos alarmes acionados por grupo de hosts

Desempenho da rede



- Visualize métricas de desempenho de rede
  - RTT, SRT, taxa de pacotes e banda

Política de relacionamento



- Criação de política de relacionamento baseada em representação gráfica
- Monitore o tráfego de rede segmentado
- Detecte fluxos anormais mais rapidamente

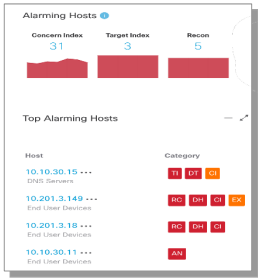
Análise preditiva de ameaças

Detecção de anomalias em tempo real usando análise de comportamento de rede, personalizada de acordo com a lógica de negócios

Deteção de ameaças de alta **fidelidade**, incluindo malware **desconhecido e criptografado**, usando machine learning

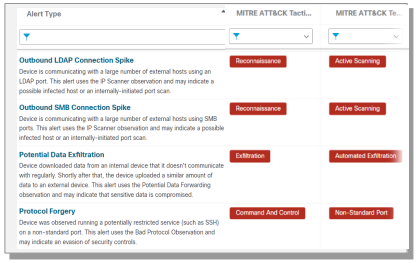
Correlação de ameaças locais e globais alimentado alimentado pela inteligência de ameaças **Talos**

Combina detecções locais e assistidas pela nuvem



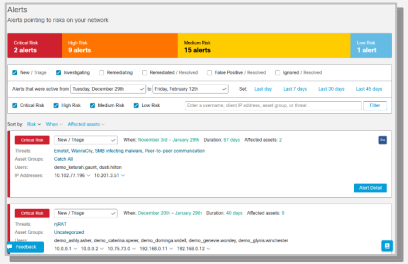
Behavioral analytics

- Detecção de anomalias por meio de linhas de base de aprendizagem estatística
- Mecanismo de aprendizagem não supervisionado
- 98 eventos de segurança de análise comportamental integrados
- Eventos de segurança personalizados permitem detecções criadas pelo usuário para corresponder especificamente ao seu ambiente
- Ajuste de eventos com políticas customizadas
- Todas as detecções abrangem a telemetria do trabalhador remoto na rede para usuários de VPN



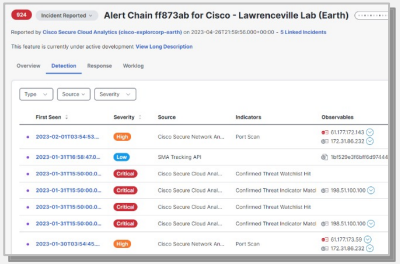
Converged Analytics

- Modelagem de entidades e detecção automatizada de funções de dispositivos
- Detecções mapeadas para a matriz MITRE ATT&CK Framework Enterprise
- 48 novas detecções locais baseadas em NetFlow
- As detecções são aplicadas à telemetria do trabalhador remoto na rede
- Exemplos incluem:
  - Amplification Attack
  - Exceptional Domain Controller
  - Geographically Unusual Remote Access
  - LDAP Connection Spike



Global Threat Alerts

- Inteligência reunida de todo o ecossistema Cisco
- Detecte ameaças no tráfego criptografado sem descriptografar
- Análise hospedada na nuvem
- Aprendizado de máquina multicamadas
- Detecção de anomalias por meio de aprendizado estatístico e aprendizado de máquina não supervisionado
- Mecanismo de aprendizado supervisionado para classificação de malware
- Conhecimento e correlação de campanhas globais com ameaças locais
- Alarme hierarquizado por risco, com contexto e cronograma relevantes



Cisco XDR

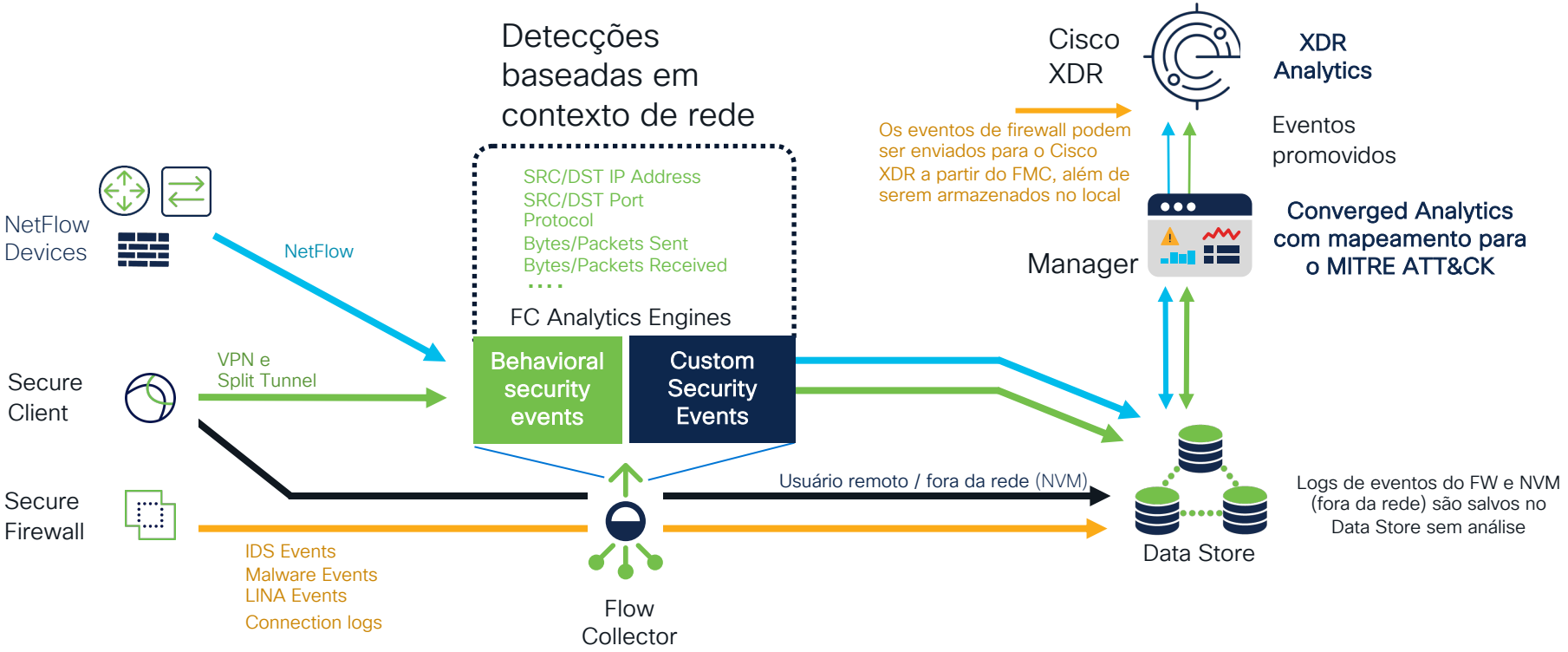
- As detecções correlacionadas simplificam as investigações de resposta a incidentes
- Enriquecimentos de detecção automática para contexto adicional
- Inteligência privada sobre ameaças – adicione indicadores e julgamentos específicos ao seu ambiente

Talos threat intel

- Classificação de malware
- Conhecimento e correlação de campanhas globais com ameaças locais
- Detecções ameaçadoras de IP, URL e comunicação de domínio

Cloud Assisted Analytics

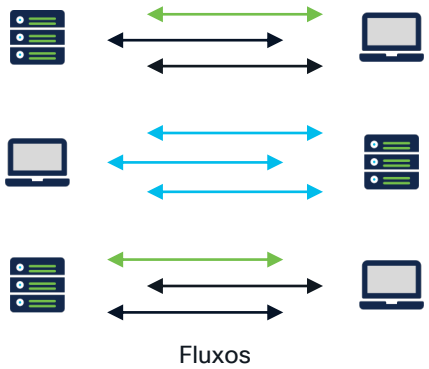
Arquitetura de detecção do Secure Network Analytics



Detecção de anomalias usando modelagem comportamental

Coletar e analizar a telemetria

Conjunto de dados abrangente otimizado para remover redundâncias



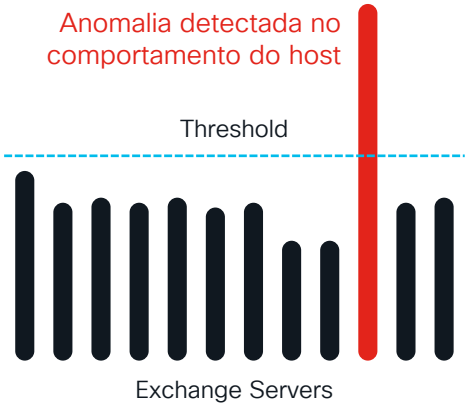
Criar uma linha de base de comportamento normal

Eventos de segurança para detectar anomalias e mau comportamento conhecido

Observações de segurança		
Número de fluxos simultâneos	Novos fluxos criados	Número de SYNs recebidos
Pacotes por segundo	Número de SYNs enviados	Taxa de *resets* de conexão
Bits por segundo	Horário do dia	Duração do fluxo

Alarmar sobre anomalias e mudanças comportamentais

Categorias de alarme para alertas de alto risco e baixo ruído para resposta mais rápida



Alarmes lógicos baseados em eventos suspeitos

Source or target of malicious behavior

Cada evento contribui para pontuações de origem e alvo que aumentam para detectar ataques lentos e repetidos

Reconnaissance

Detecção baseada em varreduras e reconhecimento de rede

Command and Control

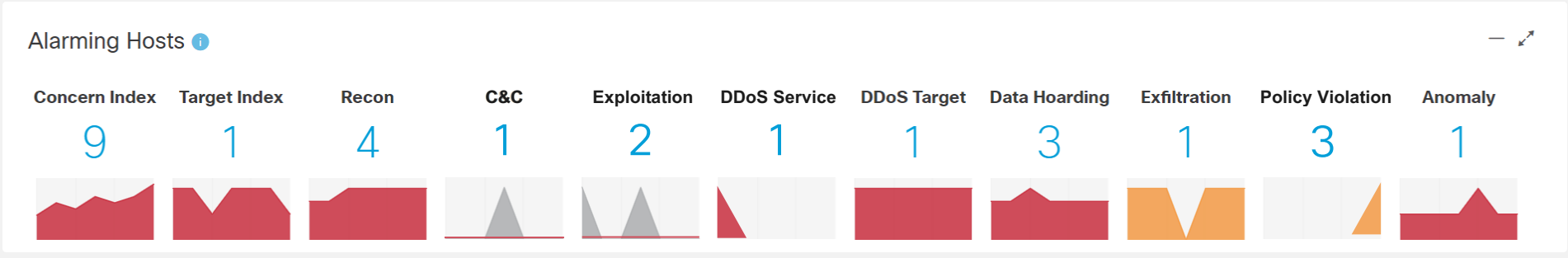
Detecção de comunicação baseada em URL e IP com redes de C&C Botnet e Tor

DDoS Activity

Detecção estatística de DDoS com base em análise de tráfego de base

Insider threats

Detecções baseadas em movimentação de dados lateral e verticalmente em uma rede



Detectando anomalias com Converged Analytics

Coletar informações

Telemetria IP

Trabalhadores remotos

Rede

Data center

Realizar análise

Modelagem de entidade dinâmica

- Função
- Grupo
- Consistência
- Regras
- Forecast

Tirar conclusões

Qual é a função do dispositivo? Seu comportamento é consistente com esse tipo de função?

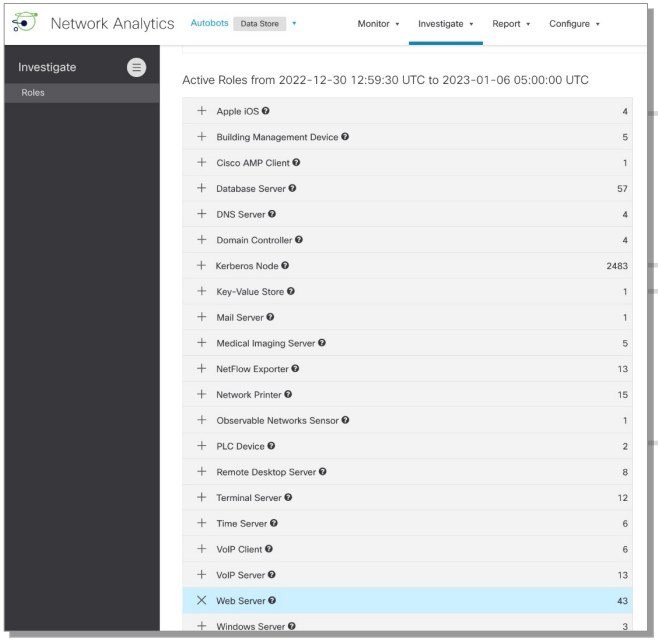
Quais portas/protocolos o dispositivo acessa continuamente? Outras funções semelhantes fazem o mesmo?

Que conexões ele faz continuamente? Qual é a reputação dos IPs aos quais ele se conecta?

Ele se comunica apenas internamente? Com quais geografias ele normalmente se comunica?

Quantos dados o dispositivo normalmente envia/recebe? É consistente com as expectativas?

O Converged Analytics mapeia dinamicamente entidades por função



Modelagem baseada em tipo

Modelagem funcional

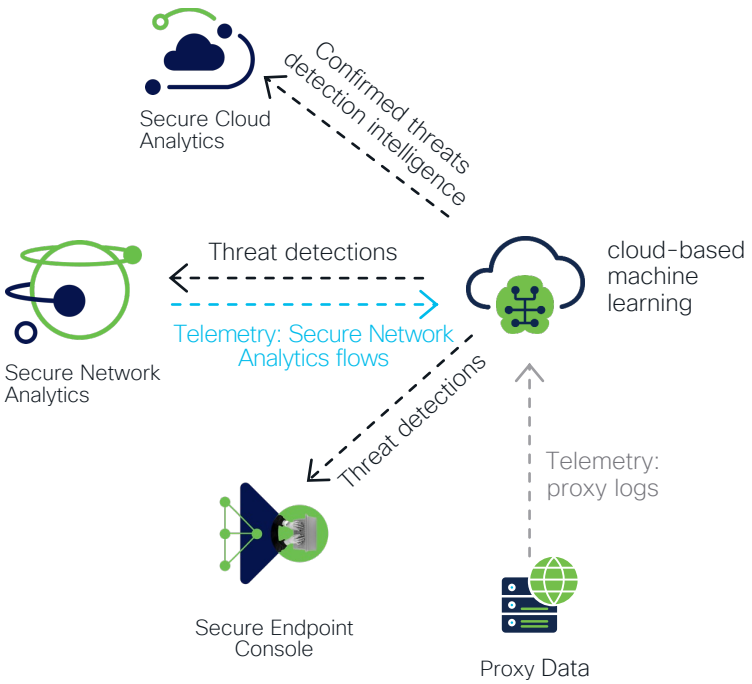
As funções incluem :

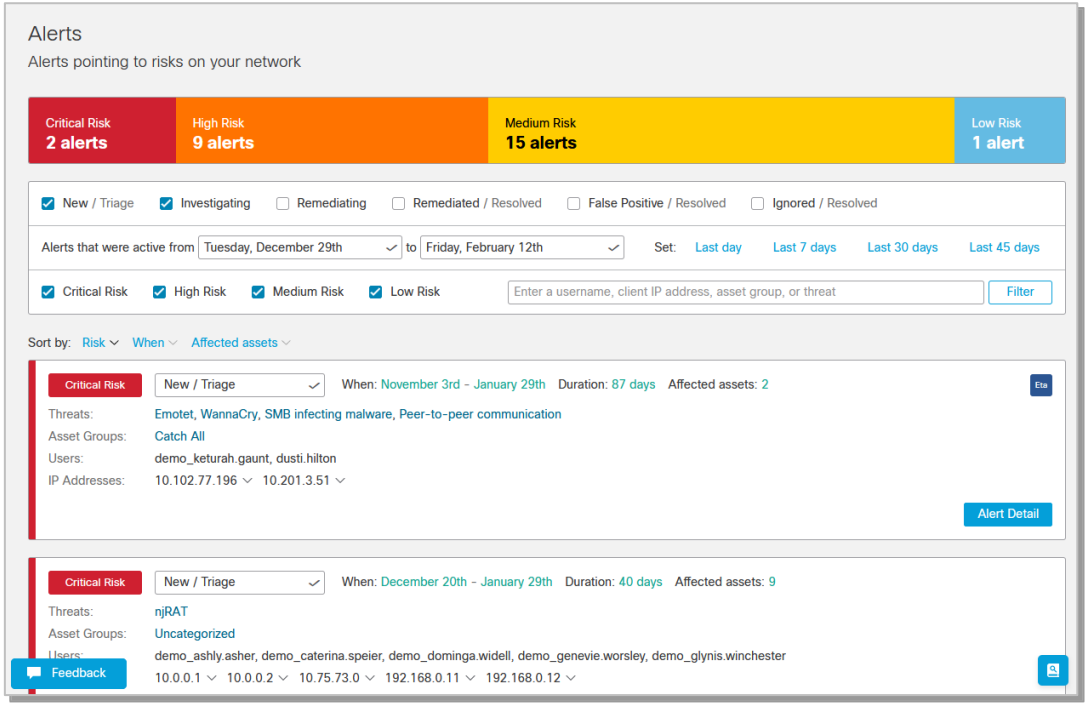
- Android
- Web server
- VoIP client
- Mail server
- Medical imaging client
- Citrix PVS server
- Apple iOS
- Remote desktop server
- DNS server
- Windows workstation
- Wireless LAN controller
- Domain controller

... **50+** entidades são suportadas !

- Classificação automática de funções disponível em um novo relatório, aproveitando o novo recurso do Converged Analytics
- As funções estão disponíveis imediatamente, sem ajuste, e fornecem detalhes sobre dispositivos para investigação e detecções.

Usando telemetria global para análise de ameaças



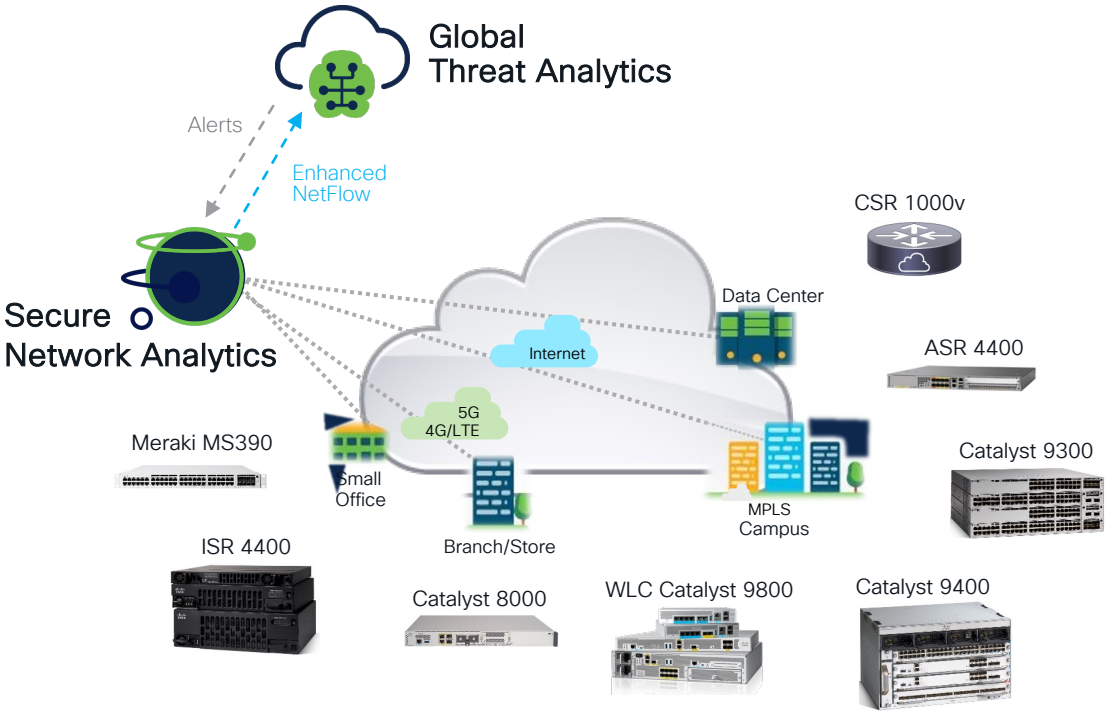


Relevant use cases:
- Detecting Malware in Encrypted Traffic
- Encryption Auditing

Global Threat Alerts

Detecção de malware no tráfego criptografado (ETA)

- Habilite o Enhanced NetFlow em switches e roteadores Cisco para obter visibilidade do tráfego criptografado
- Aplique o Global Threat Analytics para encontre eventos e comportamentos maliciosos (sem descriptografar o tráfego)
- A análise de detecção de malware é feita na nuvem, a auditoria criptográfica é feita no local
- Dados de eventos e telemetria mantidos por 45 dias



Threat intelligence license powered by Talos

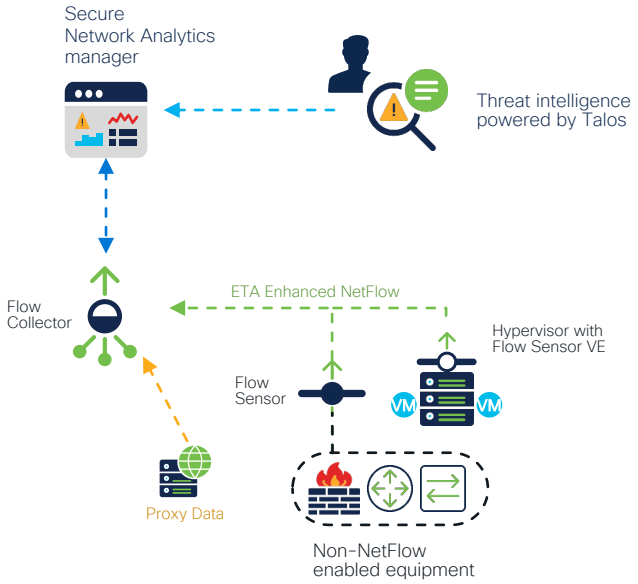
Inteligência global sobre ameaças

Detecta conexões para:

- Bogons
- C&C conhecidos
- Nós Tor de entrada e saída
- Talos IP block list (uma vez por dia)

Requer dados de URL data dos logs do Proxy ou Flow Sensor para alertas de alta fidelidade

- Atualizações periódicas automáticas do Cisco Cloud
- *Polling* a cada meia hora



Relevant use cases:
- Detecting Bogon Traffic
- Detecting C&C Traffic
- Detecting Tor Traffic

Detectar, investigar e responder

Alarmes priorizado pela gravidade da ameaça, juntamente com um relatório detalhado sobre a origem e o alvo

Network audit traiTrilhas de auditoria de rede para investigações forenses de eventos passados e monitoramento de conformidade

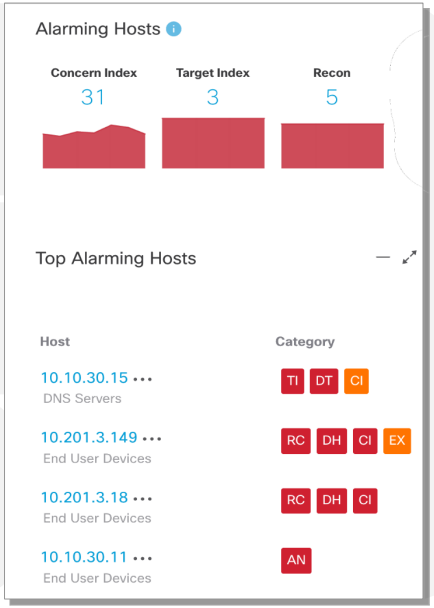
Rápida contenção de ameaças usando a rede, sem qualquer paralisação dos negócios

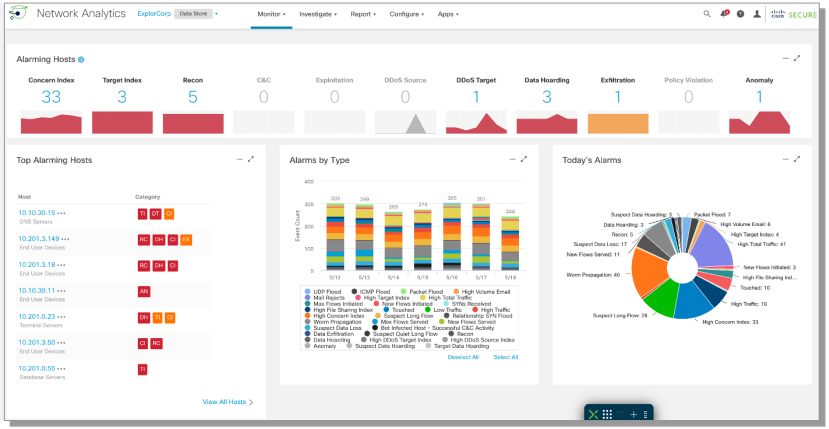
Alarmes detectados vinculados a entidades

Visualização rápida de atividades maliciosas

Comportamento suspeito ligado a alarmes lógicos

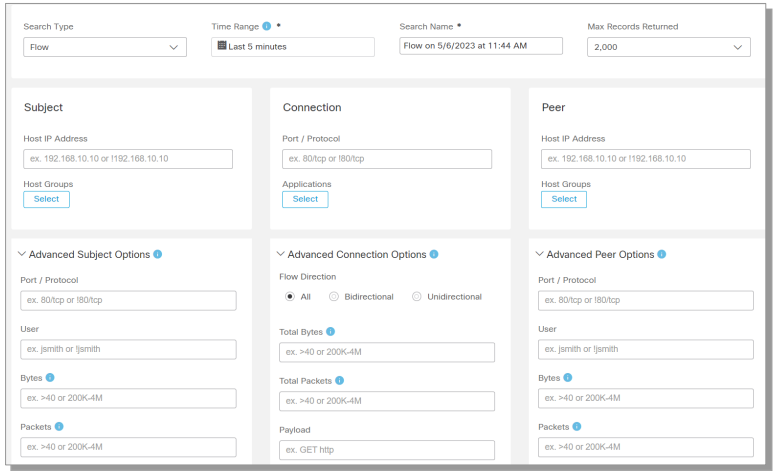
Riscos priorizados para tomar medidas imediatas



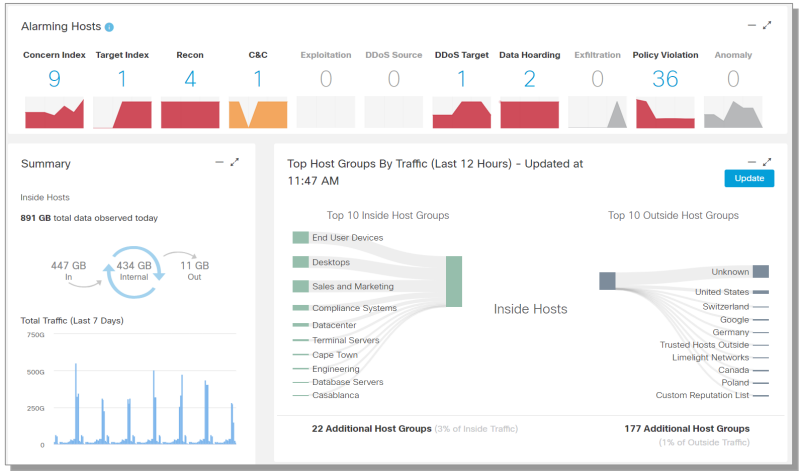


Relevant use cases:
Detecting Top Alarming Hosts on the network

Investigue com *Flow Search* e relatórios de host

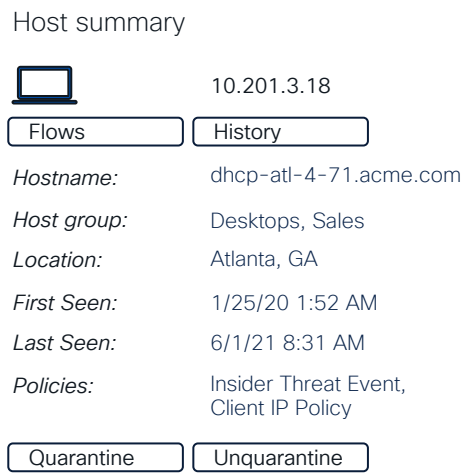


- Parâmetros de pesquisa comuns via pesquisa básica
- Os parâmetros de pesquisa são organizados por subject, host e peer na pesquisa avançada
- Identificar/pesquisar com base no usuário, dispositivo, identidade de segmentação

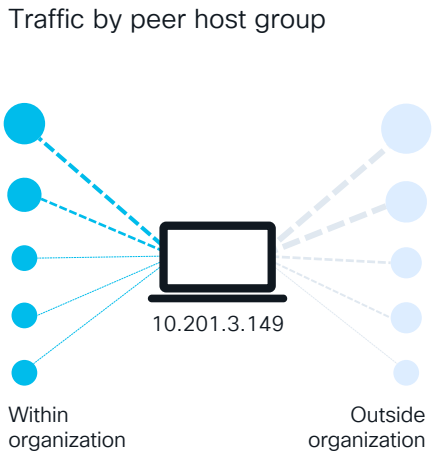


- Concentre a investigação na severidade dos alarmes principais do host principal e em toda a cadeia de destruição
- Visualize as comunicações dos grupos em toda a organização
- Entenda por que os alarmes são acionados e veja políticas violadas e valores limite (threshold)

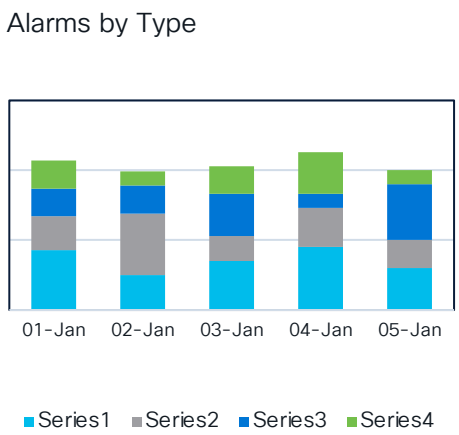
Investigação abrangente do host



Resumo das informações agregadas do host



Padrões de comunicação observados



Comportamento histórico dos alarmes

Aprendizado e detecção automatizados com Converged Analytics

48 alertas baseados em rede

- New Remote Access
- LDAP Connection Spike
- Outbound LDAP Spike
- Protocol Forgery
- Repeated Umbrella Sinkhole Communications

Fontes de telemetria

- NetFlow
- Endpoint Network Visibility Module

Alertas mapeados ao MITRE Tactics and Techniques

Alert Type	MITRE ATT&CK Tacti...	MITRE ATT&CK Te...
Outbound LDAP Connection Spike Device is communicating with a large number of external hosts using an LDAP port. This alert uses the IP Scanner observation and may indicate a possible infected host or an internally-initiated port scan.	Reconnaissance	Active Scanning
Outbound SMB Connection Spike Device is communicating with a large number of external hosts using SMB ports. This alert uses the IP Scanner observation and may indicate a possible infected host or an internally-initiated port scan.	Reconnaissance	Active Scanning
Potential Data Exfiltration Device downloaded data from an internal device that it doesn't communicate with regularly. Shortly after that, the device uploaded a similar amount of data to an external device. This alert uses the Potential Data Forwarding observation and may indicate that sensitive data is compromised.	Exfiltration	Automated Exfiltration
Protocol Forgery Device was observed running a potentially restricted service (such as SSH) on a non-standard port. This alert uses the Bad Protocol Observation and may indicate an evasion of security controls.	Command And Control	Non-Standard Port

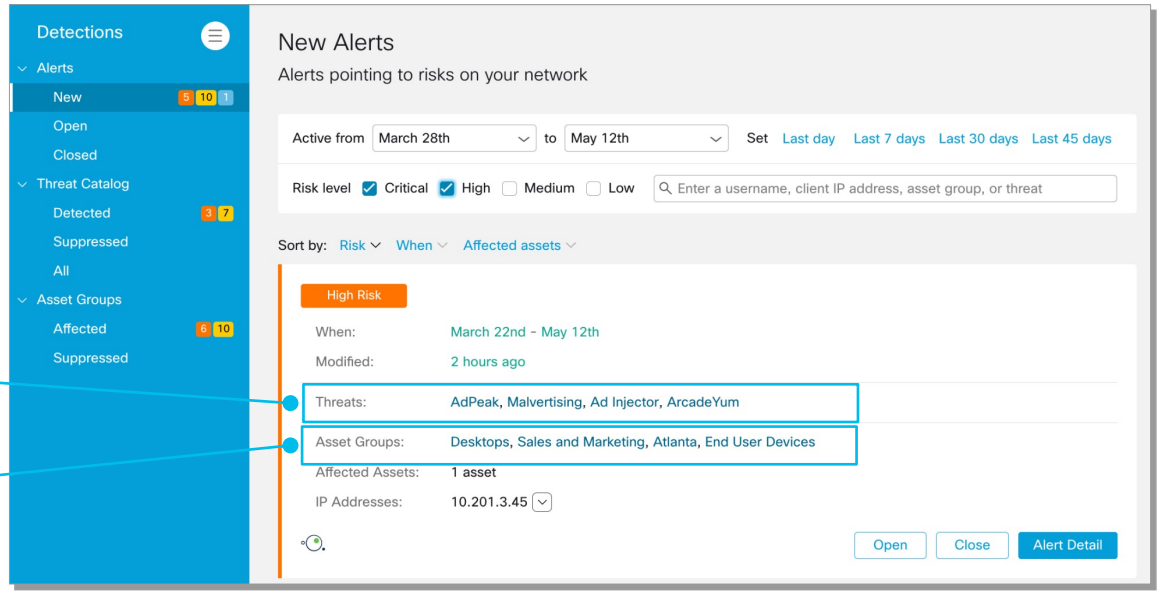
Desbloqueando o poder do desenvolvimento de detecção focada na nuvem do MITRE em implantações on premises

Detecte rapidamente ataques sofisticados com Global Threat Analytics

- Priorização tridimensional
  - Alert Severity
  - Asset Value
  - Confidence
- Cada alerta é uma unidade natural de trabalho para investigação

Detecte diferentes ameaças que ocorrem ao mesmo tempo ao ativo

Detecte quais grupos de ativos com valores de negócios semelhantes são afetados

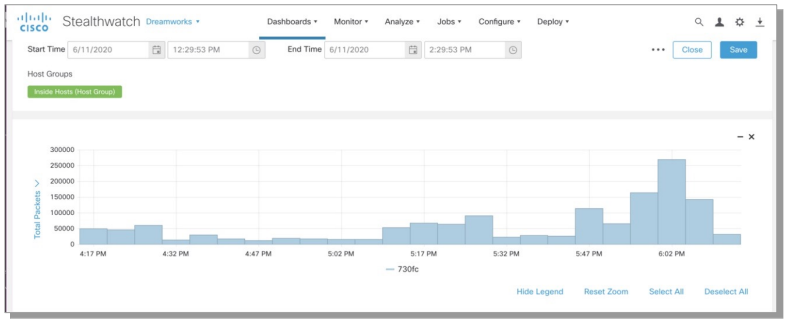


Relatórios dinâmicos e personalizados

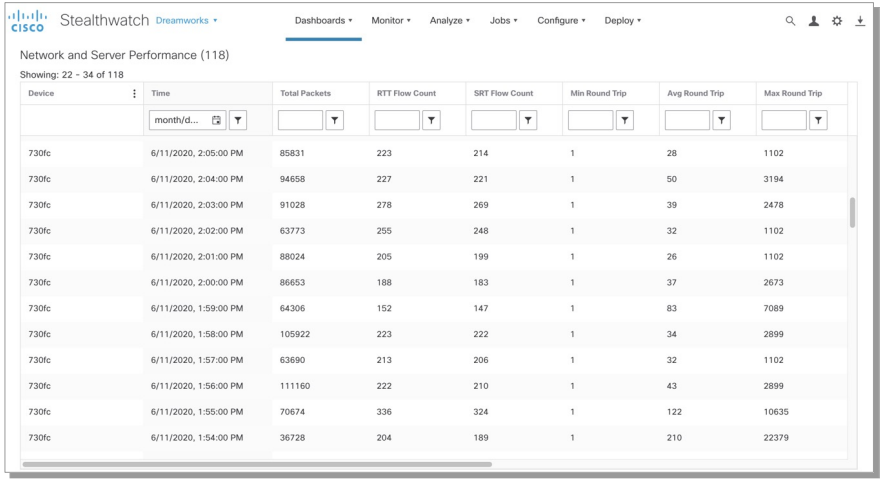
- Aproveite o valor dos dados armazenados criando relatórios altamente personalizáveis
- Altere formatos e valores de dados para aperfeiçoar a forma como são exibidos
- Layout modernizado e fácil de usar

Seleções de visualização

Fornece várias visualizações de dados



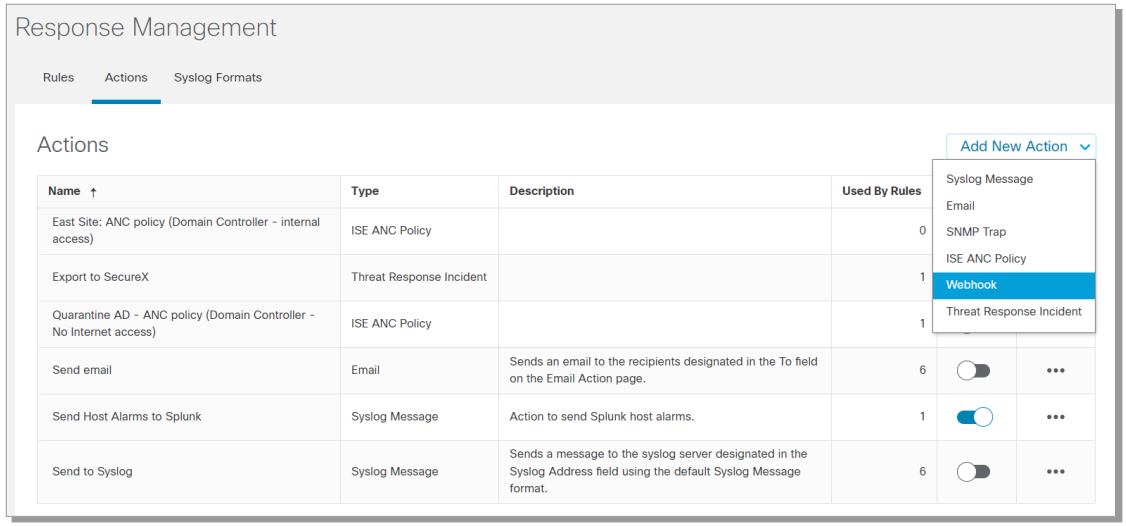
Opções robustas de filtragem de dados



Device	Time	Total Packets	RTT Flow Count	SRT Flow Count	Min Round Trip	Avg Round Trip	Max Round Trip
	month/d...						
730fc	6/11/2020, 2:05:00 PM	85831	223	214	1	28	1102
730fc	6/11/2020, 2:04:00 PM	94658	227	221	1	50	3194
730fc	6/11/2020, 2:03:00 PM	91028	278	269	1	39	2478
730fc	6/11/2020, 2:02:00 PM	63773	255	248	1	32	1102
730fc	6/11/2020, 2:01:00 PM	88024	205	199	1	26	1102
730fc	6/11/2020, 2:00:00 PM	86653	188	183	1	37	2673
730fc	6/11/2020, 1:59:00 PM	64306	152	147	1	83	7089
730fc	6/11/2020, 1:58:00 PM	105922	223	222	1	34	2899
730fc	6/11/2020, 1:57:00 PM	63690	213	206	1	32	1102
730fc	6/11/2020, 1:56:00 PM	111160	222	210	1	43	2899
730fc	6/11/2020, 1:55:00 PM	70674	336	324	1	122	10635
730fc	6/11/2020, 1:54:00 PM	36728	204	189	1	210	22379

Automação de resposta nativa e compartilhamento de alertas

- Use webhooks para aprimorar o compartilhamento de dados com ferramentas de terceiros, adicionando flexibilidade incomparável no gerenciamento de respostas
- Envie detecções de malware para o Cisco XDR, promovendo investigações forenses
- Limite o acesso à rede de um endpoint à medida que ocorrem detecções combinando Adaptive Network Control (ANC) e Cisco ISE.



Respostas totalmente automatizadas

Identity Services Engine

Cisco XDR

servicenow

SIEMs

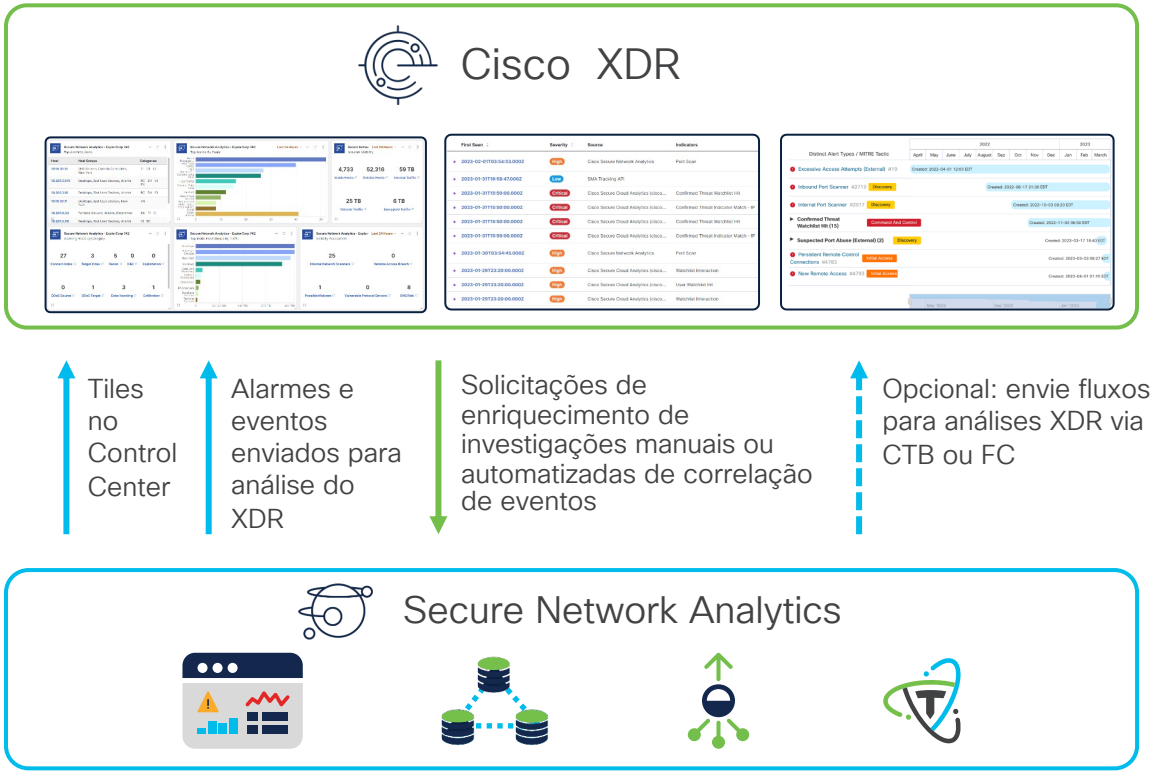
Amplificando o NDR local com Cisco XDR

Correlação cruzada de dados
Correlação de descobertas de NDR com outros mecanismos de detecção, incluindo detecções baseadas em EDR, e-mail e outros

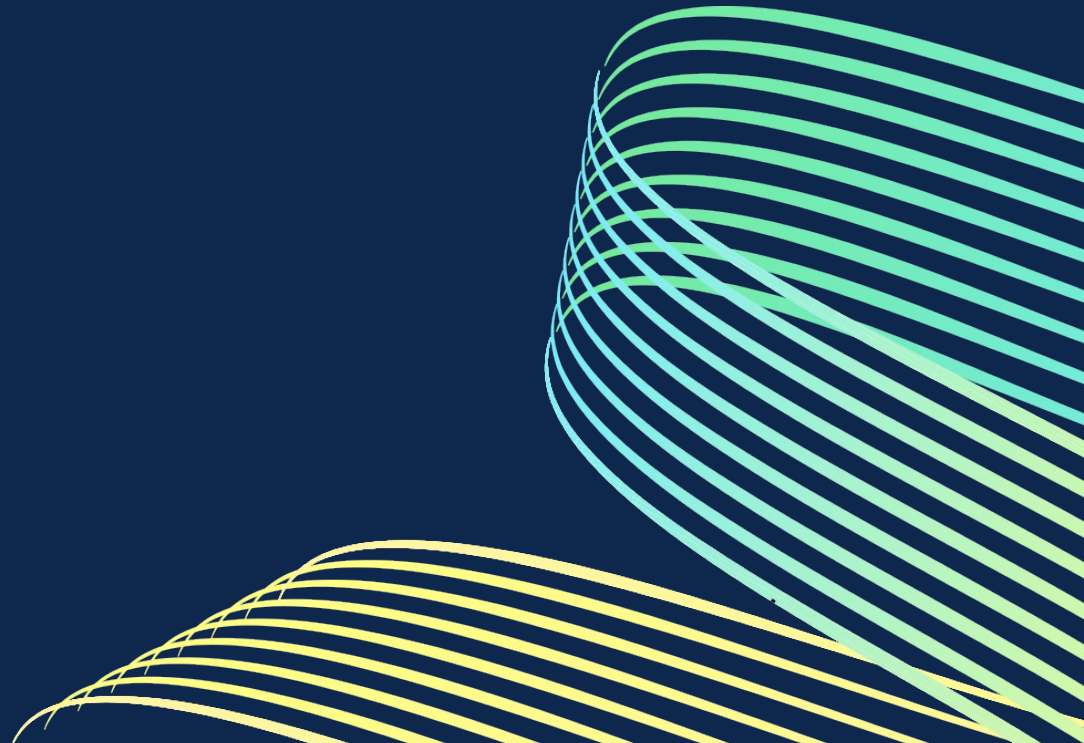
Análise de impacto
Entenda o impacto de um incidente aproveitando o XDR Incident Manager

Reduza o tempo de resposta
Reduzindo o tempo de resposta aproveitando a automação XDR e os recursos de múltiplas respostas

Estenda a capacidade de resposta
Expanda os recursos de resposta NDR com diversas tecnologias por meio de integrações XDR com tecnologias da Cisco e de terceiros

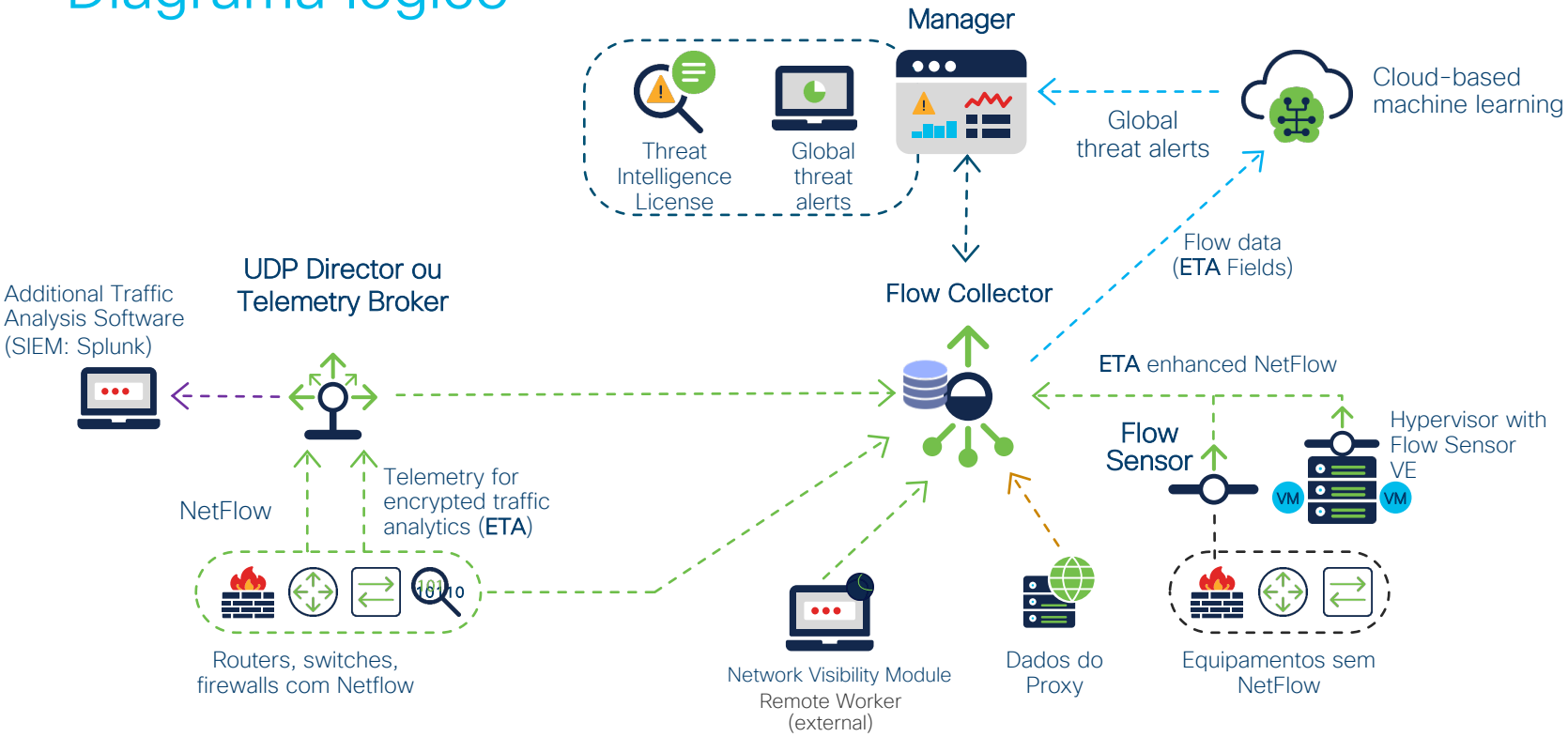


Componentes de implantação



Componentes da implantação

Diagrama lógico



Componentes obrigatórios

Secure Network Analytics Manager

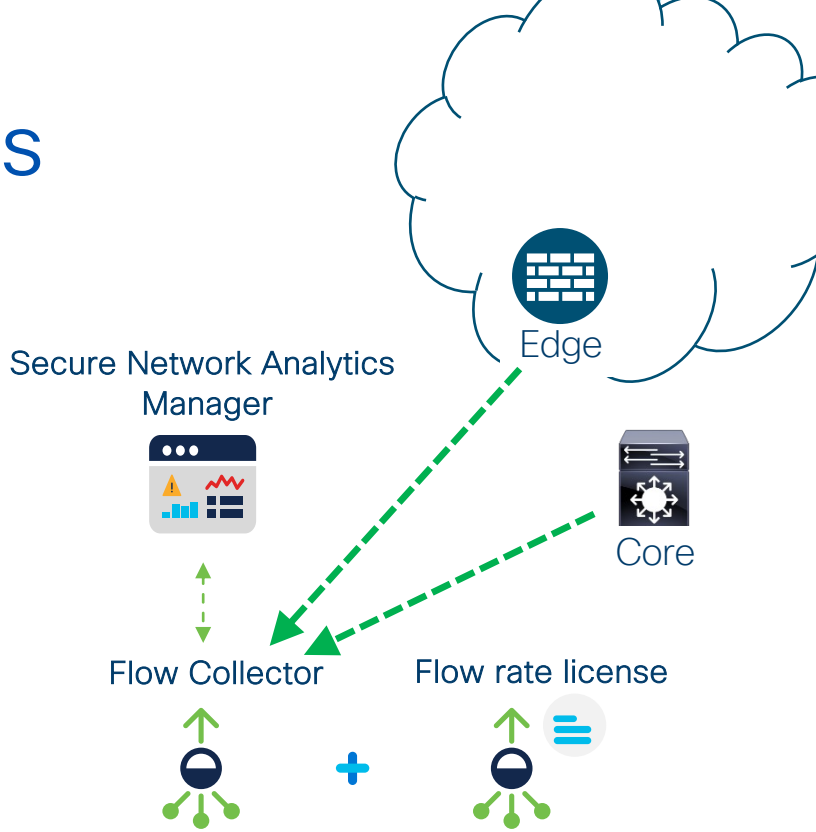
- Físico (UCSC-M4/5) ou virtual.

Flow Collector (FC)

- Físico (UCSC-M4/5) ou virtual.

Flow rate license

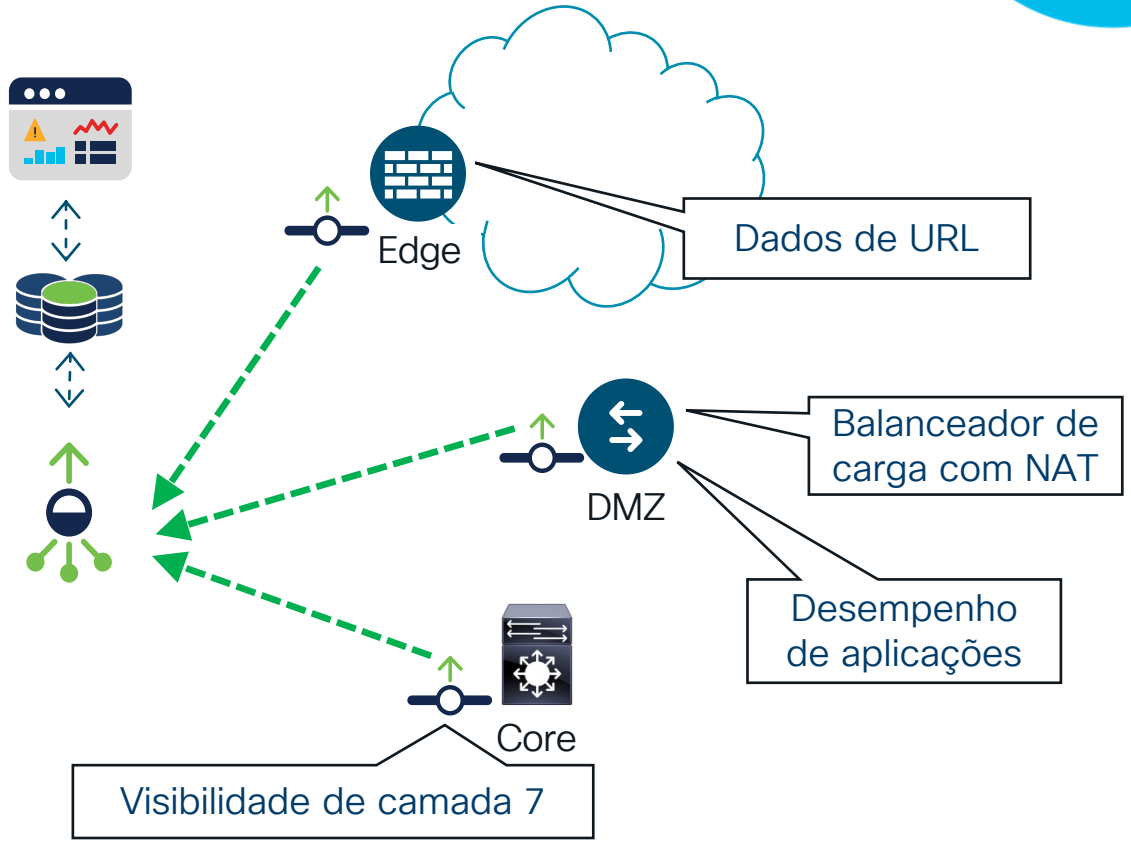
- O sistema coleta, gerencia e analisa NetFlow e é licenciado com base em fluxos por segundo (FPS) e a duração do contrato (subscrição).
- Métodos para estimativa de FPS.



Versão recomendada de software atual **7.4.2**

Onde necessito de um Flow Sensor?

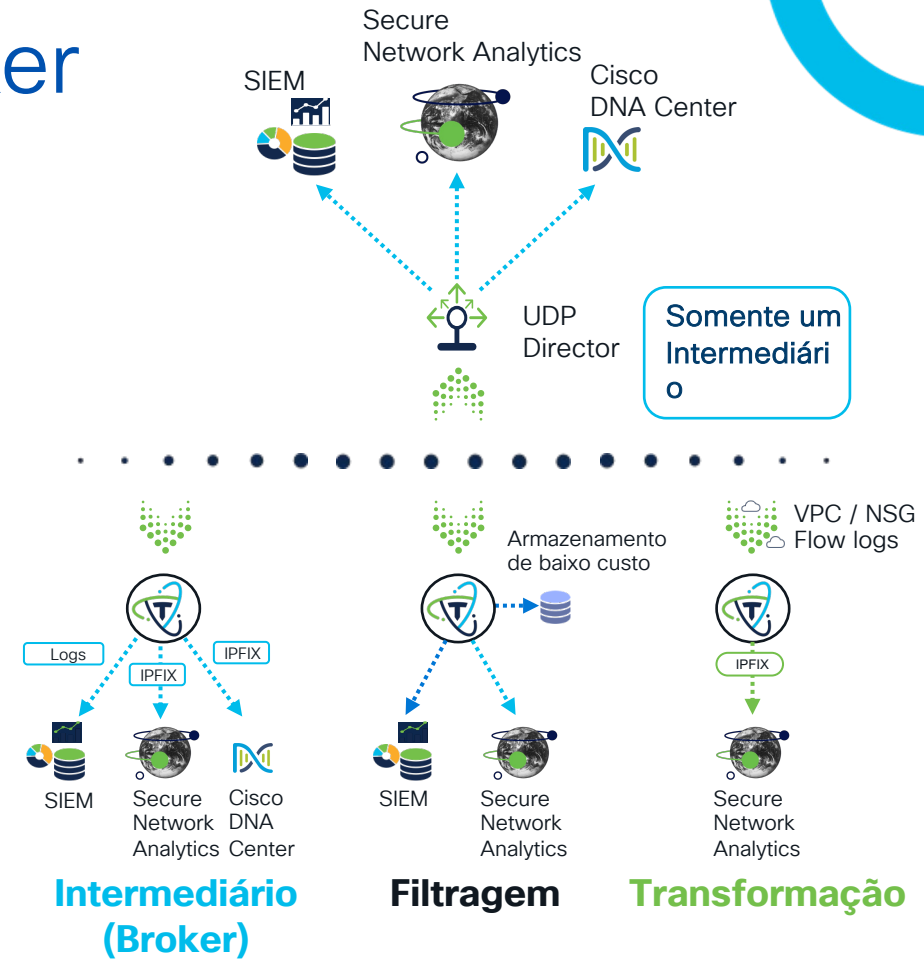
- Áreas sem visualização
- Equipamentos sem recursos nativos de exportação por NetFlow
- Equipamentos com apenas sampled NetFlow
- Áreas onde você deseja mais telemetria contextual
- TLS Finger Printing
- ETA



Cisco Telemetry Broker

Visão geral

- O Cisco Telemetry Broker (CTB) melhora o conjunto de recursos do UDP Director.
  - O CTB melhora o desempenho, a simplicidade e oferece novas funcionalidades e recursos.
- O CTB pode usar um arquivo de configuração existente do UDPD para integrar perfeitamente as regras de encaminhamento existentes.
- As arquiteturas são diferentes
  - Leve em consideração a adição de nós no desenho já existente.
  - Leve em consideração o novo modelo de licenciamento.



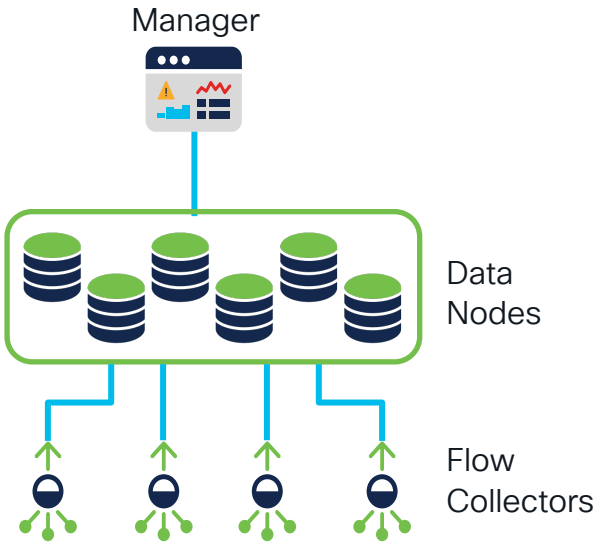
O que é o SNA Data Store?

O Data Store é uma novo e melhorado design de arquitetura de banco de dados para o Secure Network Analytics.

A ingestão de fluxos pelos coletores de fluxo é separada do armazenamento.

Pesquisas são processadas pelo Data Store efetivamente aumentando o desempenho em todas as métricas.

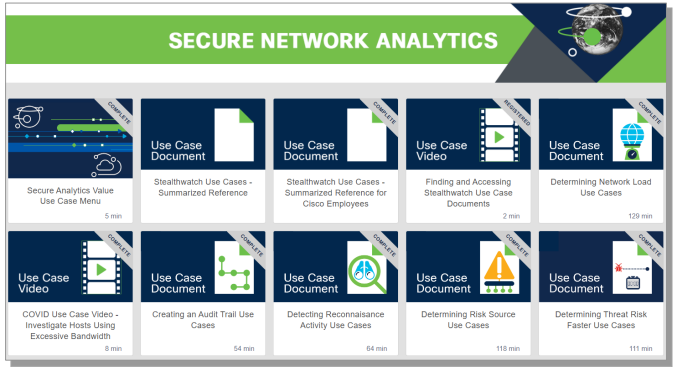
Misturar nós baseados em *hardware* e virtuais no mesmo cluster não é suportado.



Demonstração

Secure Network Analytics - Recursos

Training Center: http://cs.co/SNA-use-cases

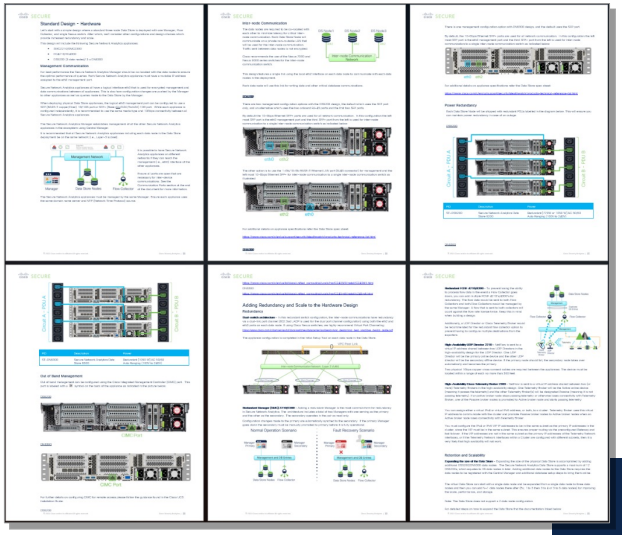


- Biblioteca abrangente de documentação técnica para obter visibilidade, detectar ameaças, aprimorar integrações de produtos de segurança e acelerar o tempo de obtenção de valor.
- Aulas ministradas por instrutor e acesso ao vivo a especialistas em produtos
- Mais de 120 documentos de casos de uso baseados em resultados, cobrindo duas dúzias de categorias de tópicos

Data Store Design Guide

http://cs.co/SNA-Data-Store-Design-Guide

- Abrange os principais detalhes do design
  - Architecture Overview
  - Redundancy and Scaling
  - Resiliency and Fail-Over
  - Configurations
    - Inter-node
    - Management
  - E muito mais..

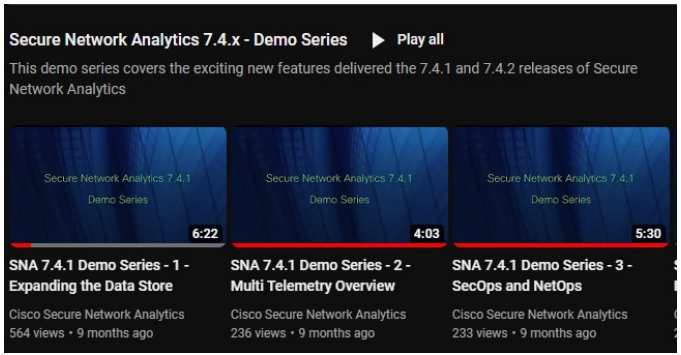


Secure Network Analytics – Videos e demos

http://cs.co/SecureAnalyticsVideos

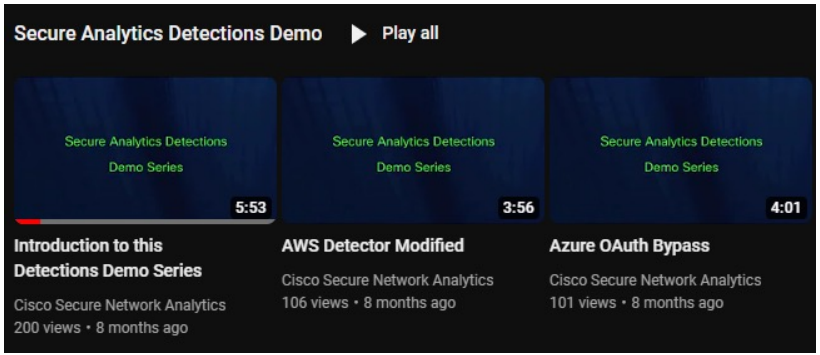
SNA 7.4.x demo series

- Mais de uma dúzia de vídeos curtos demonstrando os novos recursos e capacidades do 7.4.x
- Vídeos detalhados sobre instalação de armazenamento de dados e redundância
- Disponível em Secure Network Analytics 7.4.x – Demo Series



Detection demo series

- Apresenta alertas por meio de demonstração de produtos de ataques do mundo real
- Pacote abrangente que abrange um ciclo de vida de alerta específico e insights de especialistas
- Disponível Secure Analytics Detections Demo playlist



Muito obrigado!