Firepower PoC

Workshop INFN CCR – PAESTUM

Gianluca Peco

Panoramica

- Introduzione e soluzioni sicurezza Cisco
- Configurazione PoC
- Come funziona il Firepower
- Policy, Analysis e Overview
- Integrazioni con strumenti di analisi e remediation
- Conclusioni e Q&A

Capability Maturity Model Levels

NIST Cybersecurity Framework Functions	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimized
Identify	Little to no cybersecurity risk identification.	Process for cybersecurity risk identification exists, but it is immature.	Risks to IT assets are identified and managed in a standard, well defined process.	Risks to the business environment are identified and proactively monitored on a periodic basis.	Cybersecurity risks are continuously monitored and incorporated into business decisions.
Protect	Asset protection is reactive and ad hoc.	Data protection mechanisms are implemented across the environment.	Data is formally defined and protected in accordance with its classification.	The environment is proactively monitored via protective technologies.	Protection standards are operationalized through automation and advanced technologies.
Detect	Anomalies or events are not detected or not detected in a timely manner.	Anomaly detection is established through detection tools and monitoring procedures.	A baseline of "normal" activity is established and applied against tools/procedures to better identify malicious activity.	Continuous monitoring program is established to detect threats in real-time.	Detection and monitoring solutions are continuously learning behaviors and adjusting detection capabilities.
Respond	The process for responding to incidents is reactive or non-existent.	Analysis capabilities are applied consistently to incidents by Incident Response (IR) roles.	An IR Plan defines steps for incident preparation, analysis, containment, eradication, and post-incident.	Response times and impacts of incidents are monitored and minimized.	The capabilities of all IT personnel, procedures, technologies are regularly tested and updated.
Recover	The process for recovering from incidents is reactive or non-existent.	Resiliency and recovery capabilities are applied consistently to incidents impacting business operations.	A Continuity & Disaster Recovery Plan defines steps to continue critical functions and recover to normal operations.	Recovery times and impacts of incidents are monitored and minimized.	The capabilities of all IT personnel, procedures, technologies are regularly tested and updated.

Security resilience for the unpredictable

From operations to finances to supply chain, uncertainty looms around every corner for businesses today. Companies are investing in resilience —the ability to withstand unforeseen shocks and emerge stronger. But these investments will fall short without one key piece: security resilience.

Security resilience involves more than being reactive to a volatile environment. It requires organizations to proactively reduce risk and take necessary steps to safeguard the most vital aspects of their businesses. Security resilience confronts a new world where everyone and everything is connected while the threat landscape is ever-expanding.

Invest in security resilience with Cisco Secure. Our platform is open and infused with the latest threat data, enabling you to eliminate security gaps, utilize already-existing security investments, and prioritize alerts by importance. The Cisco Secure platform helps businesses see more, anticipate what's next, and take the right action.

Act with Confidence

Protect Integrity of Multi-Env IT

Never Go It Alone

The 5 dimensions of security resilience:

- Activate billions of signals across your ecosystem
- Anticipate what's next through shared intelligence
- Prioritize alerts with risk-based context analysis
- Close gaps across the ecosystem with integrations
- Grow stronger through orchestration and automation

© 2022 Cisco and/or its affiliates. All rights reserved.

SECURE

Cisco Talos Incident Response
Prepare, respond and recover from a breach with a full suite of proactive and emergency services to help you

Cisco SecureX
Gain contextual awareness across your security ecosystem for better detection and faster response times

User & device security

Cisco Secure Access by Duo
Verify the identity of users and inspect the devices trying to access your applications

Cisco Secure Email
Defend against spam, phishing, ransomware, and business email compromise and enhance Office 365 security

Kenna Security
Reduce the biggest risk to your business with risk-based vulnerability management

Cisco Secure Endpoint
Prevent attacks on your devices and quickly respond to threats

Cisco Secure Endpoint for iOS
See and block malicious traffic on iOS devices

Cisco Meraki SM
Secure endpoint devices with cloud-based mobile device management

Network security

Cisco Secure Firewall
Stop more threats and swiftly mitigate those that do breach your defenses

Cisco Identity Service Engine (ISE)
Enable secure network access, segmentation, and threat containment

Cisco Secure Network Analytics
Obtain enterprise-wide visibility, behavioral analytics, and threat detection

Cisco Cyber Vision
Gain visibility on your OT assets and processes to secure your industrial operations

Cisco AnyConnect
Empower remote workers with frictionless, highly secure access to your network

Cisco Secure Web Appliance
Automatically block risky websites and test unknown sites before allowing users to click them

Cisco Meraki MX
Safeguard your network with 100% centrally cloud-managed security and SD-WAN

Cloud & application security

Cisco Umbrella
Shield users from unsafe Internet destinations whether they are on or off the network

Cisco Cloudlock
Protect cloud users, data, and applications to more easily combat data breaches

Cisco Secure Cloud Analytics
Easily extend in-depth visibility and threat detection to the cloud

Cisco Secure Workload
Gain advanced workload protection with application visibility and micro-segmentation

Campus | Data Center | Cloud | Edge

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. 866554710 04/22

Perché prendere in considerazione Cisco come soluzione di Network Security?

- Secondo Forrester è il #1 per *current offering*, con il massimo dei punti nei campi di zero trust, workload protection, threat intelligence, cloud delivered components, micro-segmentation, firewall-as-a-service, usability
- #1 per presenza di mercato

Fonte: The Forrester Wave™: Enterprise Firewalls, Q3 2020
https://reprints2.forrester.com/#/assets/2/154/RES158796/report

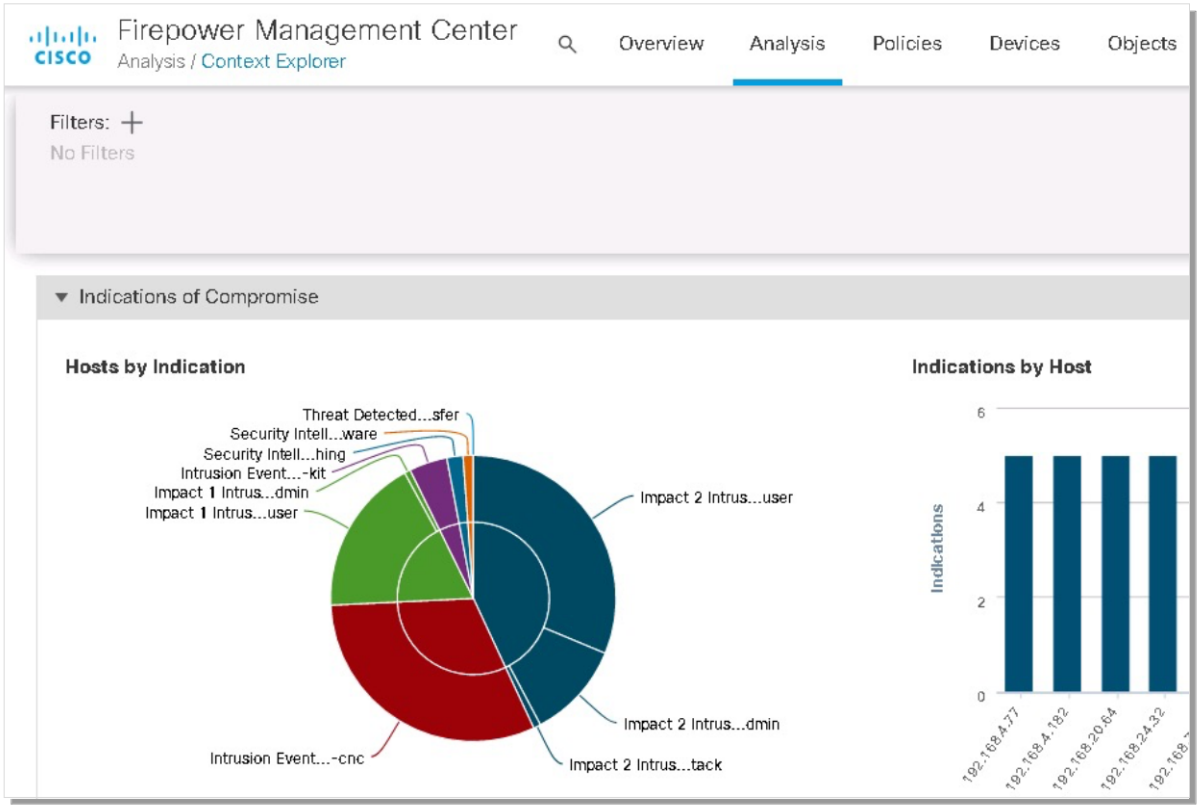
Come nasce l’idea del PoC

- Esigenza di differenziare le opzioni a disposizione per la sicurezza “perimetrale”
- Analisi di possibili approcci innovativi alla sicurezza integrata nord-sud est-ovest nei datacenter
- Necessità di iniziare a ragionare su funzionalità di analisi, threat hunting e detection and response (utile per i SoC)
- Possibilità di adottare soluzioni da branch-office compattando router e statefull firewall in unico oggetto volendo gestito “esternamente” (sedi remote , laboratori non presidiati, etc.)
- Nasce come attività del gruppo networking diventata poi di particolare interesse per Bologna vista l'esigenza di sostituire il NGFW in produzione (2016)

What is Firepower Threat Defense (FTD)?

Delivers nearly 100% efficacy on blocking malicious flows and guards the network against threats

- Key Benefits
  - Tenant management separation
  - Scale as you grow
  - Impact analysis
  - Prioritize administration
- Features
  - Firewall
  - Intrusion Prevention
  - Integrated TLS Decryption
  - VPN
  - Cisco Threat Intelligence Director
  - Malware Continuous Analysis with Retrospection



cisco SECURE © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential

Firepower 2120

Detailed performance specifications and feature highlights

Table 1. Performance specifications and feature highlights for 2100 Series with Cisco Threat Defense software

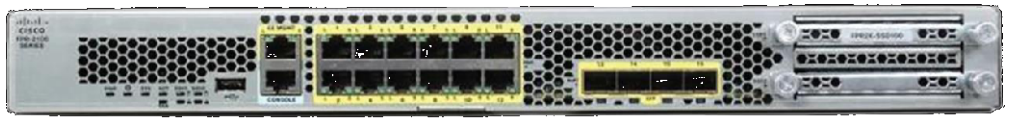
Features	2110	2120	2130	2140
Throughput: FW + AVC (1024B)	2.6 Gbps	3.4 Gbps	5.4 Gbps	10.4 Gbps
Throughput: FW + AVC + IPS (1024B)	2.6 Gbps	3.4 Gbps	5.4 Gbps	10.4 Gbps
Maximum concurrent sessions, with AVC	1 million	1.5 million	2 million	3 million
Maximum new connections per second, with AVC	14K	18K	30K	57K
TLS	365 Mbps	475 Mbps	760 Mbps	1.4 Gbps
Throughput: IPS (1024B)	2.6 Gbps	3.5 Gbps	5.4 Gbps	10.5 Gbps
IPSec VPN Throughput (1024B TCP w/Fastpath)	950 Mbps	1.2 Gbps	1.9 Gbps	3.6 Gbps
Maximum VPN Peers	1,500	3,500	7,500	10,000
Cisco Firepower Device Manager (local management)	Yes	Yes	Yes	Yes
Centralized management	Centralized configuration, logging, monitoring, and reporting are performed by the Management Center or alternatively in the cloud with Cisco Defense Orchestrator			
Application Visibility and Control (AVC)	Standard, supporting more than 4000 applications, as well as geolocations, users, and websites			
AVC: OpenAppID support for custom, open source, application detectors	Standard			
Cisco Security Intelligence	Standard, with IP, URL, and DNS threat intelligence			
Cisco Firepower NGIPS	Available; can passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence			
Cisco AMP for Networks	Available; enables detection, blocking, tracking, analysis, and containment of targeted and persistent malware, addressing the attack continuum both during and after attacks. Integrated threat correlation with Cisco Secure Endpoint is also optionally available			
Cisco AMP Threat Grid sandboxing	Available			
URL Filtering: number of categories	More than 80			
URL Filtering: number of URLs categorized	More than 280 million			

Cisco Firepower 2100 Series appliances

The Cisco Firepower 2100 Series is a family of four threat-focused security platforms that deliver business resiliency and superior threat defense. They offers exceptional sustained performance when advanced threat functions are enabled. These platforms uniquely incorporate an innovative dual multicore CPU architecture that optimizes firewall, cryptographic, and threat inspection functions. The series' firewall throughput range addresses use cases from the Internet edge to the data center. Network Equipment Building Standards (NEBS)-compliance is supported by the Cisco Firepower 2130 platform. 2100 Series platforms run either the Cisco Secure Firewall ASA or Threat Defense (FMC) software. They can be deployed in both firewall and dedicated IPS modes.

Model overview

Cisco Firepower 2110/2120 Model



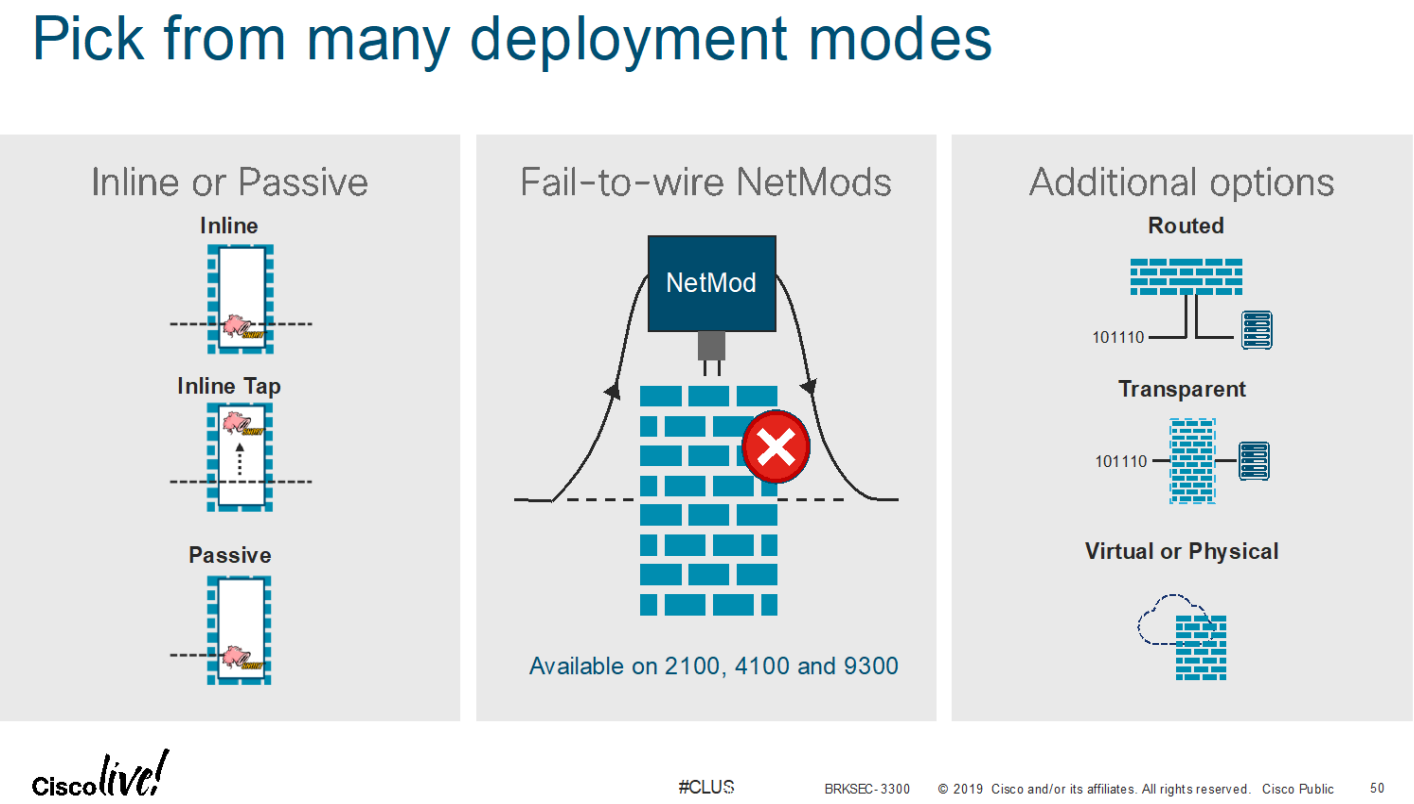
Cisco Firepower 2130/2140 Model

Cisco Firepower 2100 series summary:

Model	Firewall	NGFW	IPS Throughput	Interfaces	Optional interfaces
FPR-2110	3G	2.6G	2.6G	12 x RJ45, 4 x SFP	N/A
FPR-2120	6G	3.4G	3.5G	12 x RJ45, 4 x SFP	N/A
FPR-2130	10G	5.4G	5.4G	12 x RJ45, 4 x SFP+	10G SFP+, 1/10G FTW
FPR-2140	20G	10.4G	10.5G	12 x RJ45, 4 x SFP+	10G SFP+, 1/10G FTW

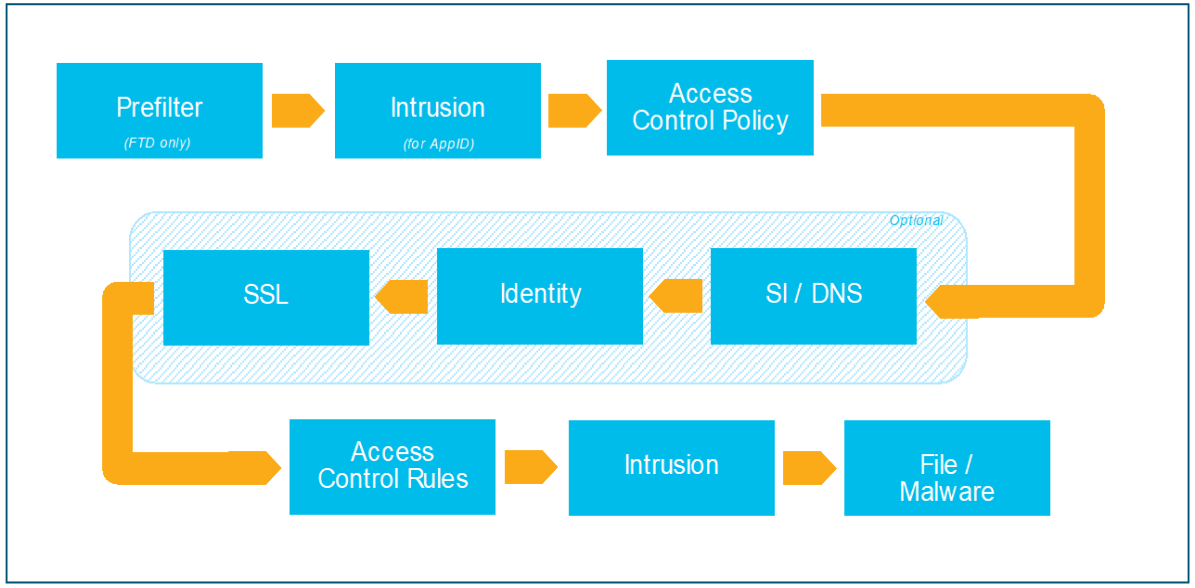
Inserimento del Firepower nel traffico di rete

- L'inserimento nel flusso del traffico può essere effettuato in varie modalità più o meno invasive e di conseguenza con un grado differente di risposta alla minaccia
- La modalità di inserimento nel traffico influisce anche sulle funzionalità implementabili (NAT, Routing, VPN, SSL, etc.)



Analisi di sessione

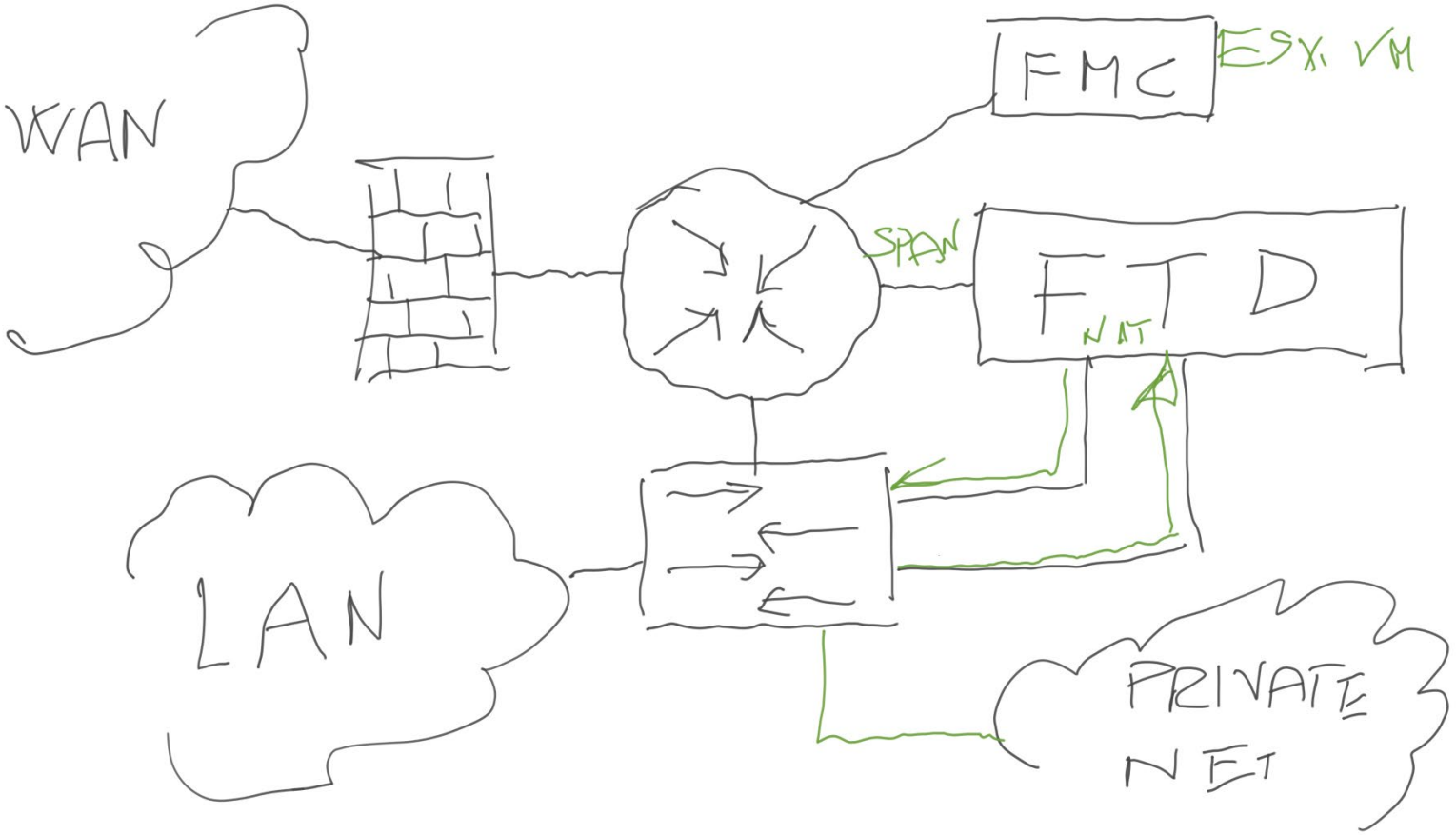
Policy Order of Operation



Cisco live!
#CLUS
BRKSEC-3300
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

- L' analisi della sessione si interrompe alla prima evenienza che genera una scelta
- Cresce la complessità computazionale insieme alla profondità di analisi nella pila ISO/OSI (L3-L7)
- Interessante la funzionalità di prefilter che permette di eliminare dall'analisi particolari flussi di traffico fidati o che non necessitano di analisi deep

Deployment

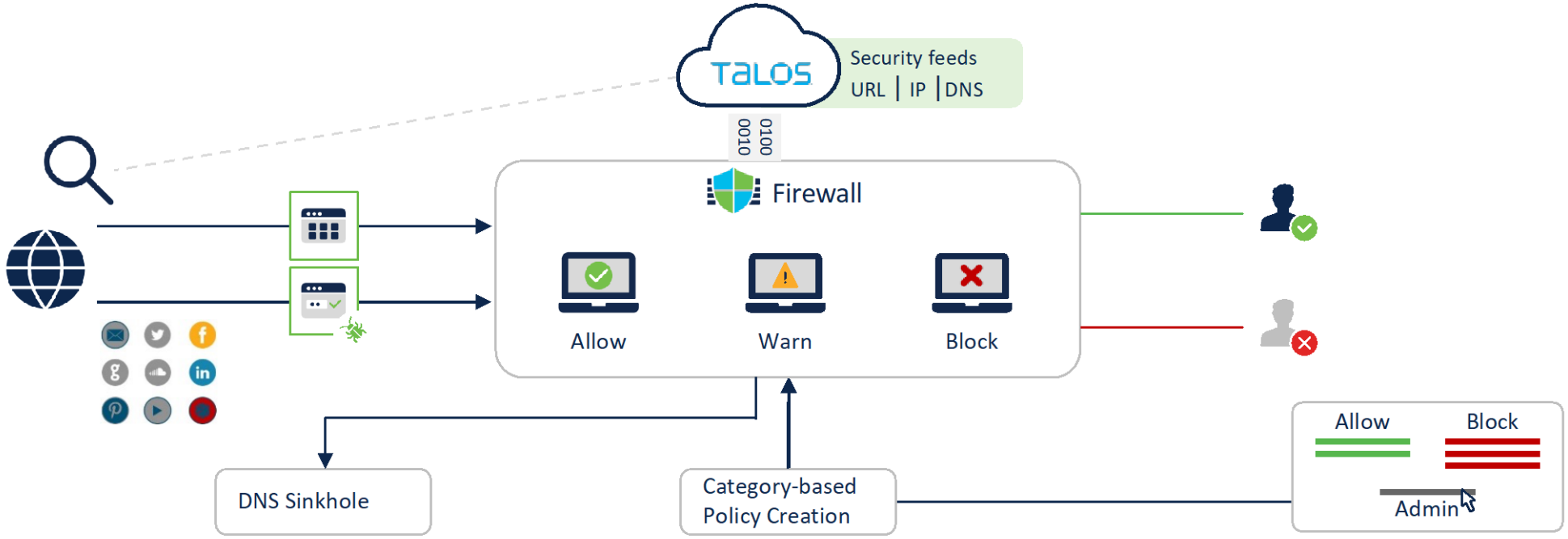


ETH0 in modalità SPAN/MIRROR del collegamento geografico verso GARR
ETH1 su VLAN/SUBNET per il NAT terminata sul Firepower
ETH2 sulla VLAN/SUBNET con accesso a GARR
MGMT sulla rete di management con accesso alla FMC e OUTBOUND
FMC su Vmware e accesso OUTBOUND

Configurazione 1 span mirror del traffico geografico per analisi dei flussi , applicazioni, malware e IDS
Configurazione 2 doppia porta per il traffico NAT con analisi dei flussi, applicazioni, malware e IPS

Firewall Policy Powered by Talos and OpenAppID

Control traffic based on IP, URL, FQDN, or application



Security Intelligence:
Block latest malicious IPs, URLs and FQDNs

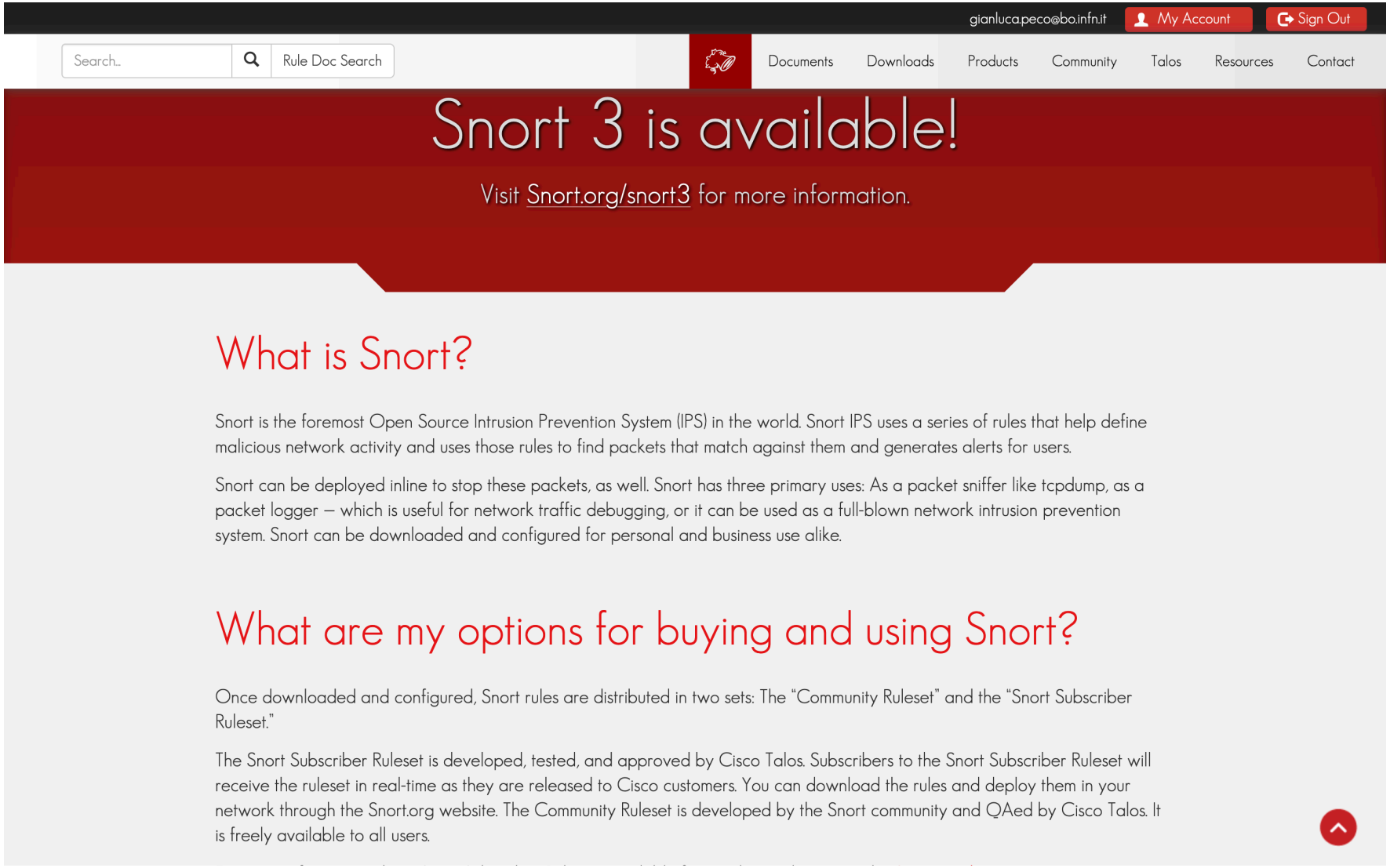
AVC with OpenAppID:
Identify and control over 4,000+ pre-defined apps

AVC with OpenAppID:
Easily create custom application detectors

URL Categories:
Classify **280M+** URLs using **80+** categories

cisco SECURE © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential 7

IPS snort2/3



- Noto motore di analisi real-time di eventi di sicurezza
- Comunità ampia supportata da Cisco
- Sintassi per le rules documentata e standard
- Una versione community driven ed una arricchita dalla comunità Cisco
- Motore alla base della parte IDS/IPS di tutte le soluzioni di sicurezza Cisco
- Possibilità di creare regole di detection personalizzate

Advance Malware Protection (AMP)

Understand the motion and behavior of files through network and endpoint visibility.

Breadth and Control points

Email | Endpoints | Web | Network | IPS | Devices

Threat Visibility

Retrospective Detection | Behavioral IoCs | File Trajectory | Threat Hunting

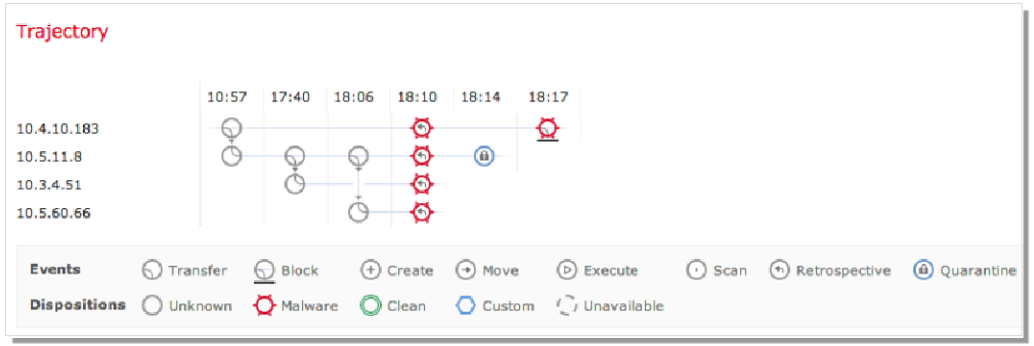
Telemetry Stream

File and Network I/O

File Fingerprint and Metadata

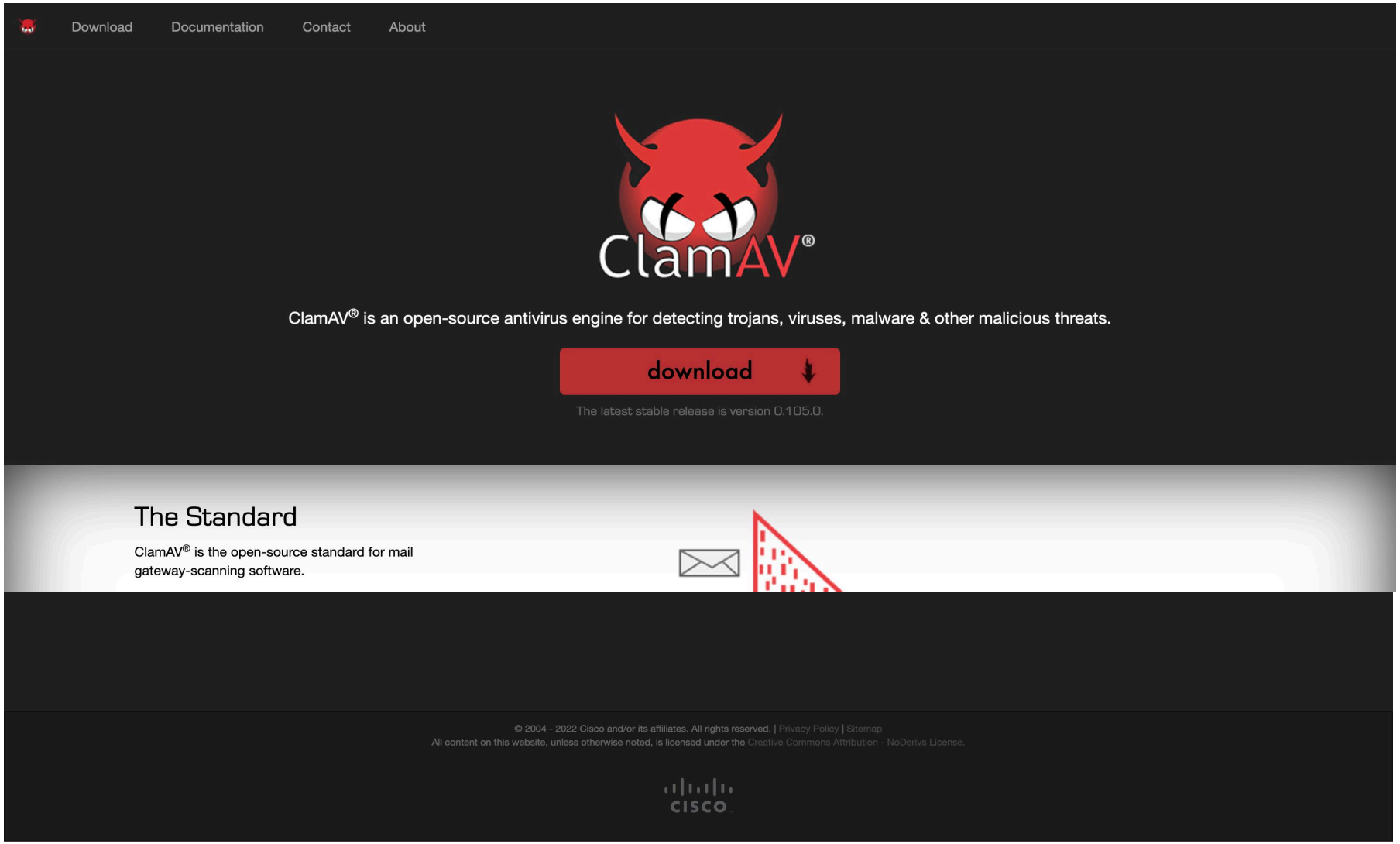
Process Information

Talos and Malware Analytics Intelligence



cisco SECURE © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential

Malware analysys ClamAV

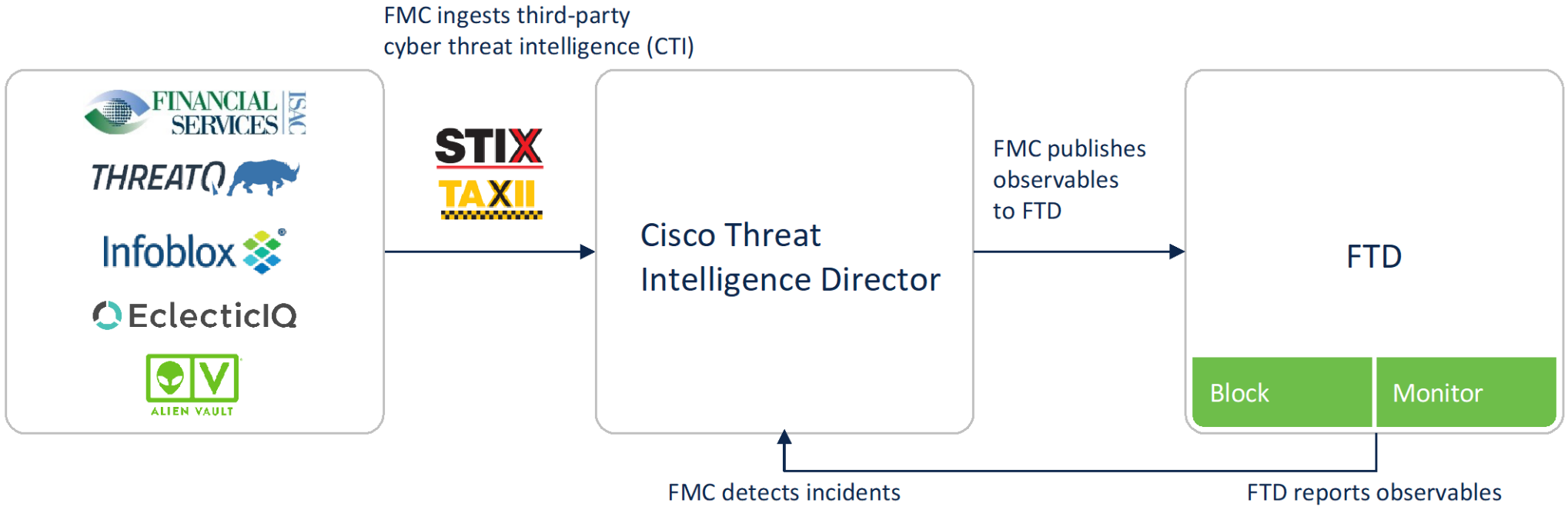


- Noto motore di analisi real-time di file per la rilevazione di malware
- Comunità ampia supportata da Cisco
- Motore alla base della parte file analisys di tutte le soluzioni di sicurezza Cisco
- Nella soluzione Secure for Endpoint viene affiancato da altri motori per l'analisi comportamentale e la network detetction

Cisco Threat Intelligence Director (CTID)

Support of open integration

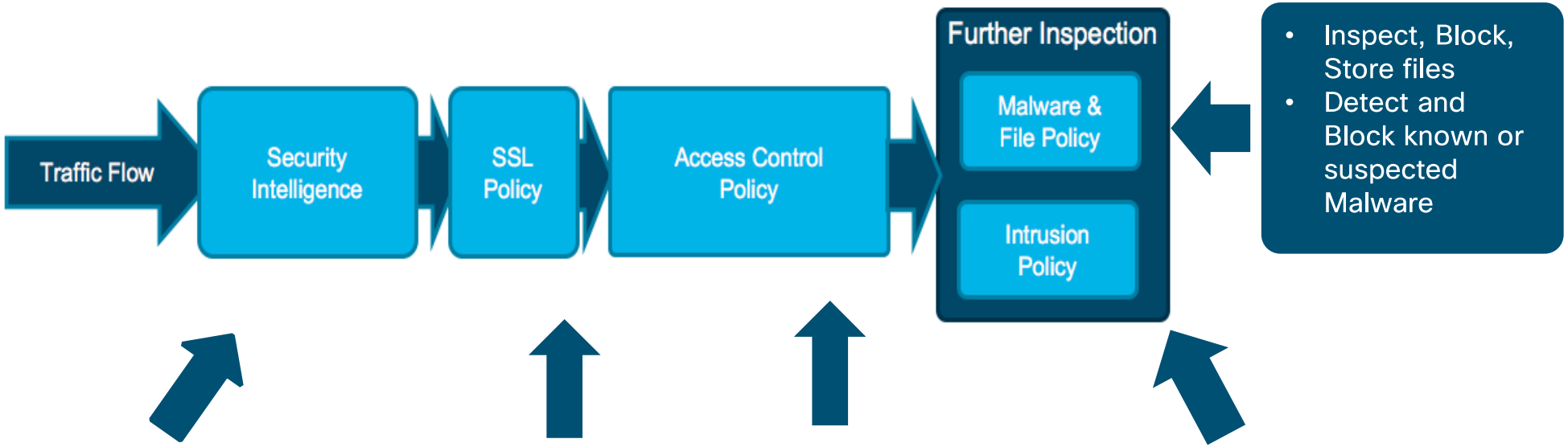
- Extend Talos Security Intelligence with 3rd party cyber threat intelligence
- Parse and operationalize simple and complex threat indicators



cisco SECURE © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential

https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKCRT-2215.pdf

Firepower Security Inspections



- Inspect, Block, Store files
- Detect and Block known or suspected Malware

- Blocks blacklisted IPs, DNS, and URLs before inspection by ACP
- Traffic blocked here never enters the later policies

- Decrypts, blocks and controls SSL/TLS traffic
- Decrypted traffic can be seen by the later policies

- Application-aware Firewall
- Direct traffic to further security inspections
- Trust and Block traffic

- IPS… your SNORT rules

Cisco live!

BRKCRT-2215

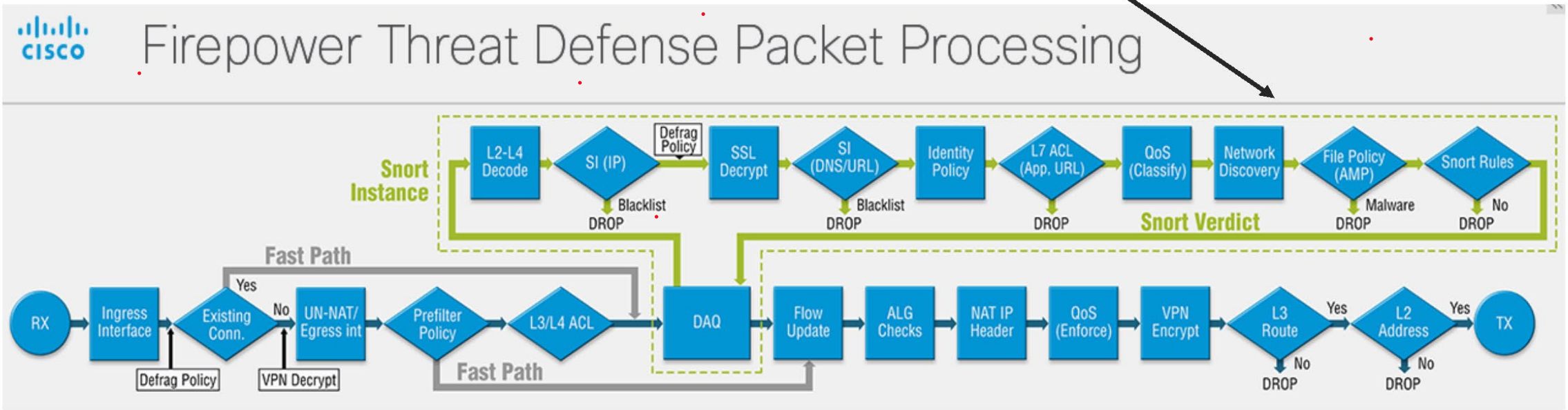
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

17

https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKCRT-2215.pdf

Firepower Threat Defense Packet Flow

Firepower OS



ASA OS (Lina)

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

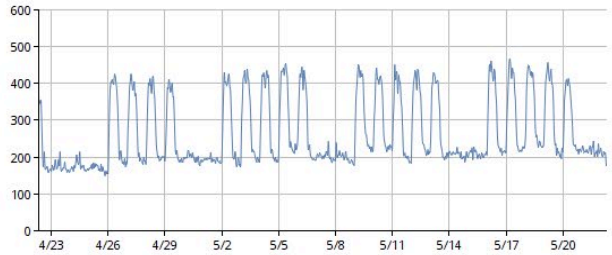
Overview-network

Firepower Management Center
Overview / Dashboards / Dashboard

Overview | Analysis | Policies | Devices | Objects | AMP | Intelligence

Deploy | admin

Unique Applications over Time



Last updated 57 minutes ago

Traffic by Application Category

Category	Total Bytes (KB)
network protocols/services	6,178,353,475.97
web browser	4,440,908,166.08
N/A	2,256,307,913.34
web services provider	1,257,366,184.31
security management	1,025,575,767.80
business	830,741,115.39
vpn/tunnel	716,330,157.13
multimedia (tv/video)	712,287,543.06
remote file storage	654,675,470.14
instant messaging	457,520,584.18

Last updated 57 minutes ago

Interface Traffic

Update Every:
1 minute

Current Rx | Tx

System Load

Show Load Avg:
☑
Update Every:
1 minute

Top Web Applications Seen

Application	Total Bytes (KB)
QUIC	610,283,279.96
Microsoft	405,955,296.13
Microsoft Teams	353,440,710.67
Zoom	294,871,046.77
Apple Update	211,178,493.19
Skype	200,250,475.53
SSH	176,258,212.50
Office 365	166,447,802.19
iCloud	155,562,210.08
SFTP	150,489,878.70
WebRTC	138,370,388.16
Sharepoint Online	131,365,792.15
Google APIs	58,190,277.56
YouTube	57,387,499.53
Akamai	56,833,300.56

Last updated 57 minutes ago

Top Client Applications Seen

Application	Total Bytes (KB)
QUIC	610,283,279.96
Zoom	294,871,046.77
Apple Update	211,178,493.19
Skype	200,250,475.53
SSH	176,258,212.50
OpenSSH	138,453,496.22
urlgrabber	107,060,358.04
Mac App Store	73,004,161.69
Firefox	60,663,496.23
YouTube	57,387,499.53
Amazon Web Services	42,406,289.41
Facebook	38,220,147.84
Advanced Packaging Tool	30,039,776.50
Dropbox	29,791,393.90
RDP	29,003,490.60

Last updated 57 minutes ago

Top Server Applications Seen

Vendor	Count
Apache	10
OpenSSH	7
Microsoft	3
embOS	1
ISO_CLASS_A	1
nginx	1

Last updated 57 minutes ago

Top Operating Systems Seen

OS Name	Count
Linux	443
Enterprise Linux	148
Android	142
Chromium	140
Windows	127
Firepower Management Center Firmware	120
FXOS	120
Mac OSX	67
iOS	59
AIX	5

Last updated 57 minutes ago

Risky Applications with Low Business Relevance

Application	Total Connections
Dropbox Download	56,063
Synology DSM	54,624
Facebook	52,440
Moat	49,435
YouTube	48,428
BitTorrent	40,456
Googlebot	25,678
Lijit	21,505
schuelerVZ	19,260

Traffic by User

Username	Total Bytes (KB)
No Authentication Required	7,419,387,487.72

Last updated 57 minutes ago

Overview-threats

Firepower Management Center
Overview / Dashboards / Dashboard

Overview | Analysis | Policies | Devices | Objects | AMP | Intelligence

Deploy | admin

Reporting

Summary Dashboard (switch dashboard)

Provides a summary of activity on the appliance

Network | Threats | Intrusion Events | Status | Geolocation | QoS

Show the Last 30 days

Add Widgets

Indications of Compromise by Host

IP Address	Count
131.154.1[illegible]2	8
131.154.1[illegible]	6
131.154.1[illegible]9	6
131.154.1[illegible]	5
131.154.1[illegible]	5
131.154.[illegible]6	5
131.154.[illegible]	5
131.154.[illegible]	5
131.154.[illegible]08	5
131.154.1[illegible]3	5

Last updated 58 minutes ago

Indications of Compromise by User

No Data

Last updated 57 minutes ago

Connections by Security Intelligence Category

Security Intelligence Category	Total Connections
Attackers	745,732
Response	108,764
Malware	79,289
CnC	16,332
Tor_exit_node	1,655
DNS Cryptomining	1,545
DNS Malware	1,191
DNS Malicious	910
URL Cryptomining	544
DNS Phishing	401

Last updated 58 minutes ago

Malware Threats

Detection Name	Count
Osx.Revoked.Certificate-7589543-0	10
PDF.0862b7a593.MalPDF.MRT.Talos	6
Osx.Dropper.Cowhand::in03.talos	3
Osx.Exploit.Callme::tpd	3
Osx.Keylogger.Aobokeylogger::1201	3
Osx.Keylogger.LogKext-1	3
Win.Downloader.Nemucod::locky.talos	3
Auto.003A2E2E5D.Sbmt.tht.Talos	2
Eicar-Signature	2
Emotet::mURLin::W32.F07BA2BBBC-90.SBX.TG	2

Last updated 58 minutes ago

Intrusion Events

Last 30 days	Total
	0
0	505
1	2,396
2	3,026
3	44,715
4	1
All	50,643

Traffic by Security Intelligence Category

Security Intelligence Category	Total Bytes (KB)
Attackers	46,967.26
Response	6,512.89
Malware	4,710.05
CnC	1,196.42
DNS Cryptomining	537.95
URL Cryptomining	412.72
DNS Malware	344.35
DNS Malicious	281.05
DNS Phishing	137.38
Tor_exit_node	117.55

Last updated 58 minutes ago

https://firepoc1.bo.infn.it/dashboard/view.cgi?id=643a2ae0-8376-11ec-a07c-bebdf0abb990#

Overview-Intrusion

Firepower Management Center
Overview / Dashboards / Dashboard

Overview | Analysis | Policies | Devices | Objects | AMP | Intelligence

Deploy | admin

Network | Threats | Intrusion Events | Status | Geolocation | QoS

Show the Last 30 days

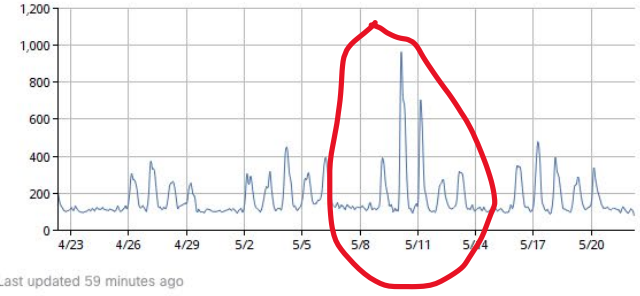
Add Widgets

Top Attackers

Source IP	Count
131.154.11	16,050
131.154.12	12,927
131.154.10	4,229
131.154.10	3,608
131.154.1	2,231
131.154.10	2,142
131.154.1	1,184
131.154.1	518
131.154.1	202
199.249.1	189

Last updated 59 minutes ago

All Intrusion Events



Last updated 59 minutes ago

Total Events by Application Protocol

Application	Total Events
DNS	29,543
WhatsApp	5,880
HTTP	3,975
SSH	3,495
SMTPS	1,369
Telegram	863
Apple Update	270
SMTP	195
IMAP	109
HTTPS	53

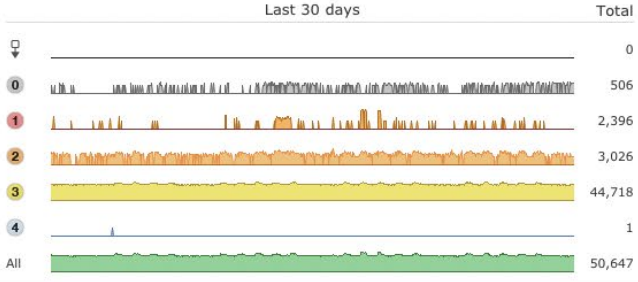
Last updated 59 minutes ago

Top Targets

Destination IP	Count
185.21.1	6,855
185.21.1	6,851
185.21.1	6,004
185.21.1	5,587
157.240.	5,282
131.154.	2,444
93.51.35.	2,139
131.154.	1,184
131.154	795
131.154.	695

Last updated 59 minutes ago

Intrusion Events



Impact 1 Events by Application Protocol

Application	Impact 1 Events
HTTP	2,296
DNS	49
Microsoft	6
BITS	4
Google Play	3
FTP Data	2
Office 365	2
IMAP	1

Last updated 59 minutes ago

Impact 2 Events by Application Protocol

Application	Impact 2 Events
SMTPS	1,369
DNS	532
HTTP	439
HTTPS	53
SSH	49
SMTP	27
Outlook	8
Googlebot	5
Bingbot	4

Firepower Management Center
Analysis / Intrusions / Events

Overview | Analysis | Policies | Devices | Objects | AMP | Intelligence

Deploy | admin

Bookmark This Page | Reporting | Dashboard | View Bookmarks | Search | Predefined Searches

Events By Priority and Classification (switch workflow)

2022-04-22 13:29:13 - 2022-05-22 13:29:13
Static

No Search Constraints (Edit Search)

Drilldown of Event, Priority, and Classification | Table View of Events | Packets

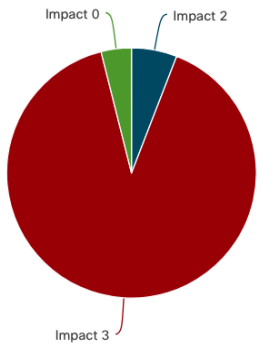
Jump to...

Message	Priority	Classification	Count
SQL 1 = 1 - possible sql injection attempt (1:19439:10)	high	Web Application Attack	64
SERVER-WEBAPP GPON Router authentication bypass and command injection attempt (1:46624:2)	high	Web Application Attack	30
SERVER-WEBAPP Apache HTTP Server httpd directory traversal attempt (1:58276:3)	high	Web Application Attack	22
SERVER-WEBAPP Spring Cloud Gateway Spring Expression Language injection attempt (1:59388:2)	high	Web Application Attack	4
SQL use of concat function with select - likely SQL injection (1:24172:2)	high	Web Application Attack	3
SERVER-WEBAPP PHPUnit PHP remote code execution attempt (1:45749:2)	high	Web Application Attack	3
SERVER-WEBAPP Laravel Framework PendingCommand arbitrary command execution attempt (1:54602:1)	high	Web Application Attack	2
INDICATOR-OBFUSCATION select concat statement - possible sql injection (1:19437:6)	high	Web Application Attack	2
SERVER-WEBAPP ThinkPHP 5.0.23/5.1.31 command injection attempt (1:48837:6)	high	Web Application Attack	1
SERVER-WEBAPP vBulletin pre-authenticated command injection attempt (1:51620:4)	high	Web Application Attack	1
POLICY-OTHER F5 iControl REST interface tm.util.bash invocation attempt (1:57336:1)	high	Potential Corporate Policy Violation	7
POLICY-OTHER HP Universal CMDB default credentials authentication attempt (1:31846:7)	high	Potential Corporate Policy Violation	1
FILE-MULTIMEDIA Microsoft Windows Transport Stream Program Map Table Heap overflow attempt (1:38124:4)	high	Attempted User Privilege Gain	2,529
PROTOCOL-DNS Microsoft SMTP excessive answer records buffer overflow attempt (1:32959:3)	high	Attempted User Privilege Gain	2,107
FILE-MULTIMEDIA Microsoft Windows Transport Stream Program Map Table Heap overflow attempt (1:38125:4)	high	Attempted User Privilege Gain	854
SERVER-OTHER Apache Log4j logging remote code execution attempt (1:58743:6)	high	Attempted User Privilege Gain	39
SERVER-OTHER Apache Log4j logging remote code execution attempt (1:58742:7)	high	Attempted User Privilege Gain	39
SMTP_RESPONSE_OVERFLOW (124:3:2)	high	Attempted User Privilege Gain	30
FILE-OTHER Kaspersky antivirus library heap buffer overflow - without optional fields (1:16295:13)	high	Attempted User Privilege Gain	5
SERVER-OTHER Symantec MIME parser updateheader heap buffer overflow attempt (1:39380:6)	high	Attempted User Privilege Gain	5
SERVER-OTHER Apache Log4j logging remote code execution attempt (1:58723:5)	high	Attempted User Privilege Gain	2
SERVER-OTHER Apache Log4j logging remote code execution attempt (1:58737:4)	high	Attempted User Privilege Gain	
SERVER-OTHER Apache Log4j logging remote code execution attempt (1:58726:6)	high	Attempted User Privilege Gain	
OS-WINDOWS Microsoft WebDAV MiniRedir remote code execution attempt (1:13474:12)	high	Attempted User Privilege Gain	
FILE-PDF Adobe Acrobat Reader PDF JBIG2 remote code execution attempt (1:32786:3)	high	Attempted User Privilege Gain	1

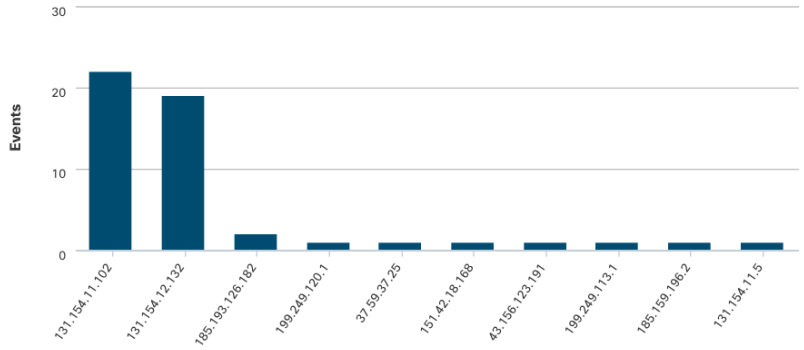
1 Tracker
Google Tag Mana...

Intrusion Information

Intrusion Events by Impact

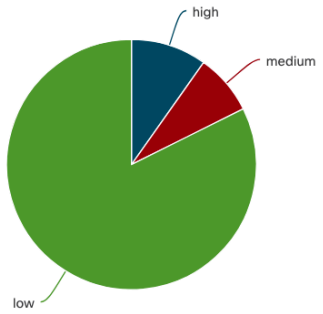


Top Attackers

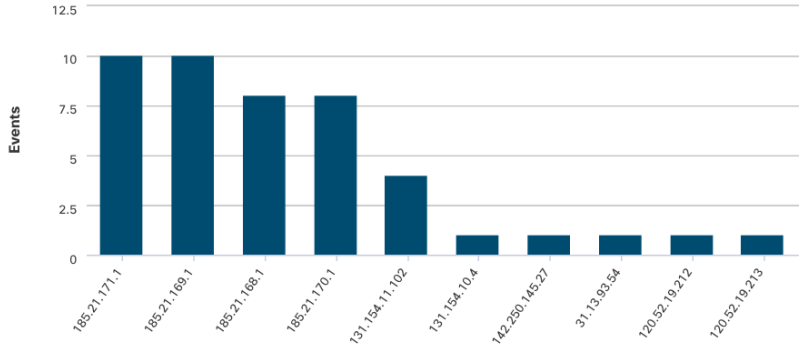


Top Users

Intrusion Events by Priority



Top Targets



Top Ingress Security Zones

Intrusion Event Details

Event	Classification	Priority	Events
INDICATOR-COMPROMISE Suspicious .ml dns query (1:39866:4)	Misc Activity	low	36
INDICATOR-COMPROMISE Suspicious .top dns query (1:43687:2)	Misc Activity	low	5
PROTOCOL-DNS Microsoft SMTP excessive answer records buffer overflow attempt	Attempted User Privilege Gain	high	3
SSH_EVENT_PROTOMISMATCH (128:4:2)	Detection of a Non-Standard Protocol or Event	medium	2
PROTOCOL-DNS DNS query amplification attempt (1:28556:3)	Attempted Denial of Service	medium	2

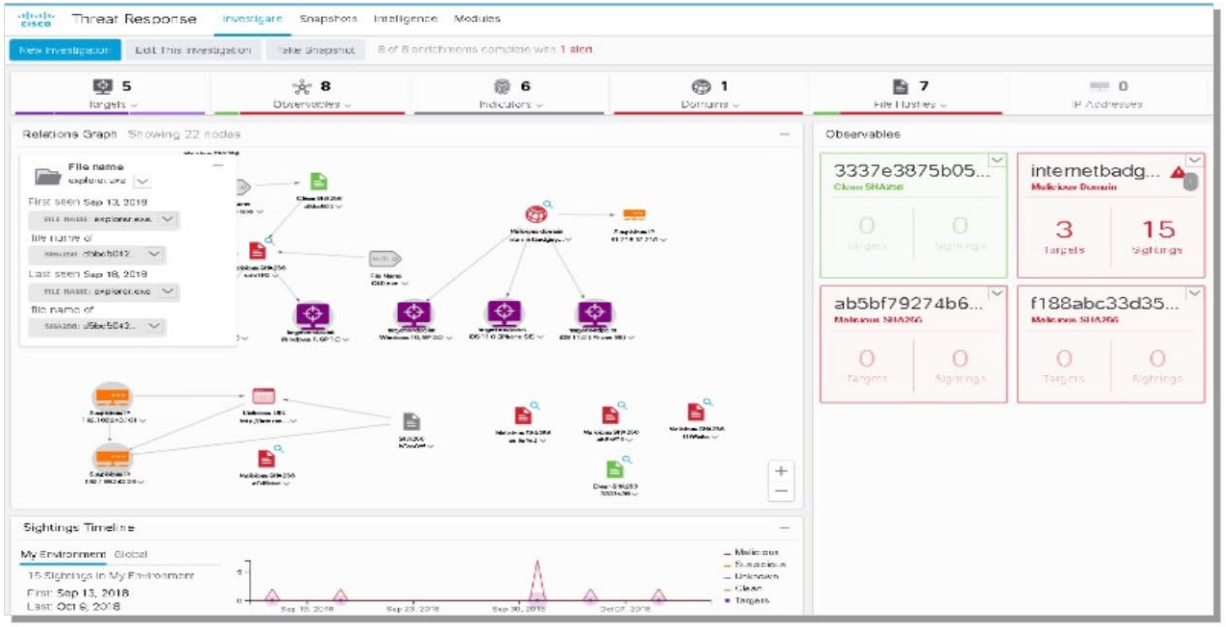
Integrazioni sperimentate

- Cisco SecureX – piattaforma in SaaS per la gestione, integrazione, correlazione e analisi degli eventi di sicurezza (quasi SIEM)
- Cisco Secure Endpoint (ex APM) - soluzione di endpoint protection
- Cisco Orbital (osquery) - soluzione per l'analisi realtime dei sistemi
- Cisco Umbrella - soluzione per la protezione DNS dei remote device (OpenDNS)
- IBM Qradar, OTX exchange, VirusTotal, Shodan, urlscan.io nelle rispettive versioni free (quantità a volte limitata di API query)

Cisco SecureX

Automates integrations across networks, endpoints, and Cloud environments

- Key Benefits
  - Out of box integrations
  - Speed cyber investigations
  - Included with Cisco security product licenses
  - Reduce burden of other security products
- Features
  - Aggregated threat intelligence
  - Automated enrichment
  - Incident tracking
  - Seamless drill down
  - Direct remediation



cisco SECURE © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential

Considerazioni e conclusioni

- Non siamo riusciti per questioni di tempo a realizzare test approfonditi con simulatori di traffico per la valutazione delle performance (Trex, Ostinato, etc.)
- Alcune valutazioni di carattere del tutto generale si possono ricavare dalle performance sul traffico reale in IPS mode sulla porta SPAN. Considerando una differenza di occupazione media dei core su FTD intorno al 3% ed un aumento di banda intorno ai 100 Mb/s ed estrapolando i valori otteniamo 3.3Gb/s (3.5 Gb/s full threat di targa)
- E' nostra intenzione realizzare una relazione ed una presentazione ad uso interno per mostrare ed analizzare in modo più approfondito funzionalità e possibili use case

Considerazioni e conclusioni

- Utilizzo di intelligenza open source. Aperto alle “signature” esterne
- Semplicità di configurazione ed uso
- Baseline dei flussi – per utilizzare prefilter
- Sistema integrato di gestione, configurazione, analisi delle minacce, gestione IoC, incidenti
- Orientato all’analisi dei flussi e delle minacce (detect and response for SoC)
- Necessita di attenta valutazione nel dimensionamento per limitare i costi per porta/traffico

Ringrazio Cisco Italia e ITCentric per averci fornito i dispositivi ed il supporto
In particolare Luigi, Federico e Giovanni

Q&A

Backup Slides

Policies rules

- Access Control (L3-L7 ACL)
- Intrusion detection and prevention (SNORT2/3 configuration)
- Malware e File (Signature based analisys – File access control)
- Application ID (TALOS intelligence)
- DNS (DNS blacklist – DNS intelligent analysys)
- SSL (SSL/TLS decryption rules)
- Prefilter
- Anyconnect VPN (encryption lan to lan and endpoint isolation)
- NAT and routing protocol

Threat hunting 1 - Intrusion

Threat hunting 2 – Malware file

Secure Endpoint
Premier

Dashboard | Analysis | Outbreak Control | Management | Accounts

Search

Dashboard

Dashboard | Inbox | Overview | Events | iOS Clarity

Refresh All | Auto-Refresh | Reset | New Filter | 30 days | 2022-04-21 21:38 | 2022-05-21 21:38 | UTC

25% compromised

Inbox Status
2 Require Attention | 0 In Progress | 0 Resolved

Global Threat Alerts
unresolved threats
0

Compromises — Inbox

Quarantined Detections — Quarantine Events

Vulnerabilities — View

SECURE X | Incidents

Search... | Enrich...

MacBook Air C17F579XQ6L4 in group Protect @ 20220510 06:47:46

Investigate Incident | Status | Manage Incident | Link

High Impact 1

MacBook Air C17F579XQ6L4 in group Prot...
Secure Endpoint — 12 mag 2022
High — Enriched

Other 139

- Intrusion event 1-43687 — NGFW Event Service — 21 mag 2022
- Intrusion event 1-39866 — NGFW Event Service — 21 mag 2022
- Intrusion event 1-43687 — NGFW Event Service — 21 mag 2022
- Intrusion event 1-32959 — NGFW Event Service — 21 mag 2022
- Intrusion event 1-43687 — NGFW Event Service — 21 mag 2022
- Intrusion event 1-43687 — NGFW Event Service — 21 mag 2022
- Intrusion event 1-32959 — NGFW Event Service — 21 mag 2022
- Intrusion event 1-43687 — NGFW Event Service — 21 mag 2022
- Intrusion event 1-43687 — NGFW Event Service — 21 mag 2022

Add short description...

New · Created By Secure Endpoint on 2022-05-10 06:47:46 UTC

Enriched - View Enrichments

Summary | Events | Observables | Timeline | Linked References (1)

Targets (4) · Investigate these Targets

501334ac-dd5d-4e4c-b6af-d41eb62b33d3
Endpoint · Targeted by 4 unique observables, 8 times in the last 12 days
AMP GUID · 501334ac-dd5d-4e4c-b6af-d41eb62b33d3
Hostname · MacBook Air C17F579XQ6L4
IP Address · 146.241.193.144
IP Address · 192.168.1.159
s1_agent_id · 73a90946-5bb2-5974-a9bb-fbdf5e2348e8
First: 2022-05-10T06:47:47.000Z · Last: 2022-05-12T12:20:48.000Z

501334ac-dd5d-4e4c-b6af-d41eb62b33d3
Endpoint · Targeted by 1 unique observable, 3 times in the last 4 days
AMP GUID · 501334ac-dd5d-4e4c-b6af-d41eb62b33d3
Hostname · MacBook Air C17F579XQ6L4
IP Address · 146.241.193.144
IP Address · 169.254.42.222
IP Address · 192.168.1.159
s1_agent_id · 73a90946-5bb2-5974-a9bb-fbdf5e2348e8
First: 2022-05-17T13:39:30.000Z · Last: 2022-05-17T13:39:30.000Z

501334ac-dd5d-4e4c-b6af-d41eb62b33d3
Endpoint · Targeted by 1 unique observable, 4 times in the last 7 hours
AMP GUID · 501334ac-dd5d-4e4c-b6af-d41eb62b33d3

Info

ASSIGNEES · Add
No one is assigned - assign yourself

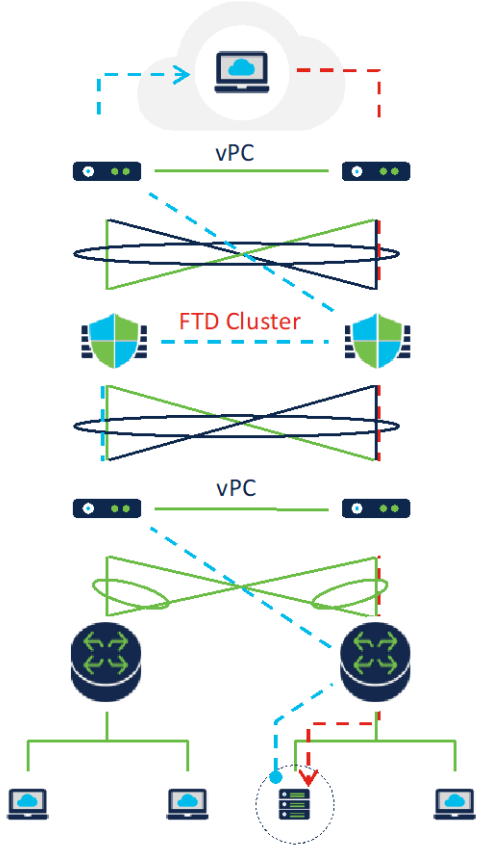
KEY PROPERTIES
Categories: Select ...
Disc. Method: Select ...
Intend. Effect: Select ...
Confidence: High
TLP: Amber

Clustering

Drive high return on investment while maintaining high availability

- Combine multiple devices to make a single scalable logical device
- Scale as you grow
  - Scale throughput, concurrent and new connection
  - Can span multiple datacenters
- N+1 resilience
- Handles asymmetric traffic seamlessly

Example: 6 node cluster created by 2 x FPR9300 fully loaded chassis (with SM-56)
336 Gbps AVC
307 Gbps AVC+IPS



cisco SECURE © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential

Secure Endpoint
Premier

Dashboard | Analysis | Outbreak Control | Management | Accounts

Search

Dashboard

Dashboard | Inbox | Overview | Events | iOS Clarity

Refresh All | Auto-Refresh | Reset | New Filter | 30 days | 2022-04-21 21:38 | 2022-05-21 21:38 | UTC

25% compromised

Inbox Status

2 Require Attention | 0 In Progress | 0 Resolved

Global Threat Alerts

unresolved threats
0

Compromises

Inbox

Top 2 / 8

Server
Protect
Audit

21 22 23 24 25 26 27 28 29 30 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
APR MAY

Quarantined Detections

Quarantine Events

Top 2 / 8

Server
Protect
Audit

21 22 23 24 25 26 27 28 29 30 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
APR MAY

Vulnerabilities

View

Top 0 / 8

Server
Protect
Audit

Secure Malware Analytics

1 Automatic Analysis Submissions
0 Retroactive Threat Detections

Statistics

144K Files Scanned
22K Network Connections Logged

Connectors

8 Connectors
6 Installs
0 Install Failures

Quick Start

Set Up Windows Connector
Set Up Mac Connector
Set Up Linux Connector

Significant Compromise Observables

FILE	24acedc8...e1a423ba	IMG_31082016_95143...	1
FILE	2eadd0dd...2b118eef	2970040.emlx	1
FILE	33fc43e3...9f250cbf	Info-2011-752_05387....	1
FILE	35ddefc0...01f15617	Photo(5009).zip	1
FILE	381d7d88...21a91ebf	2970123.emlx	1

1 2 3 4 5 6 7

Compromise Event Types

Medium	Threat Quarantined	2
Medium	Threat Detected	2
Medium	Quarantine Failure	2

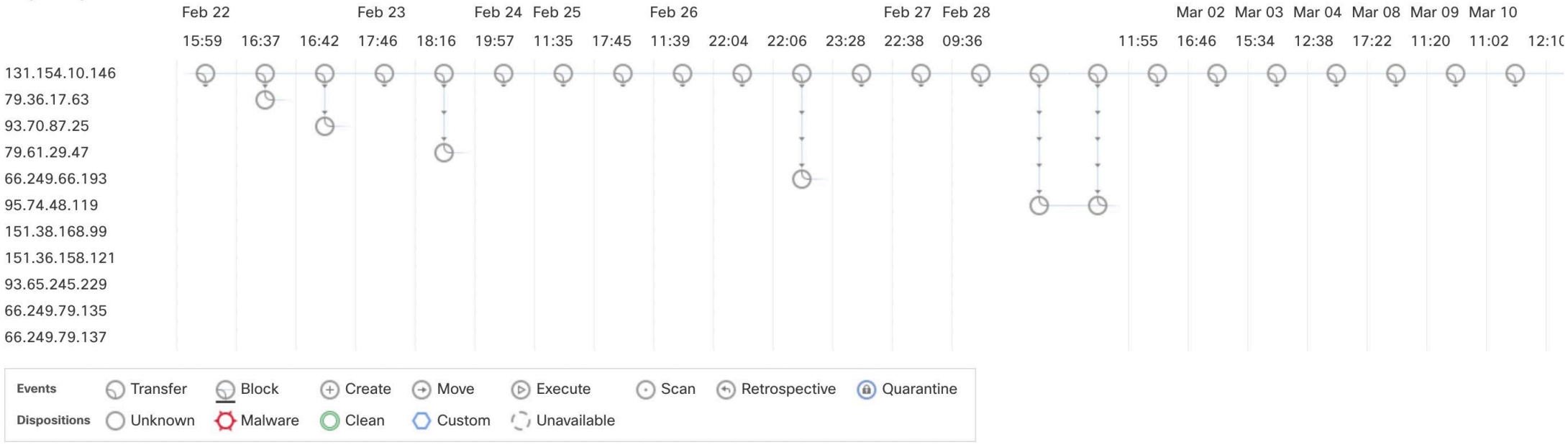
Firepower Management Center
Analysis / Files / Network File Trajectory

Overview | Analysis | Policies | Devices | Objects | AMP | Intelligence | Deploy | admin

Network File Trajectory for 662bfeb0...f8d9564d

File SHA256	662bfeb0...f8d9564d	**First Seen**	2022-02-22 15:59:31 on 131.154.10.146
File Name	Met_Num_21.pdf	**Last Seen**	2022-05-20 16:25:00 on 131.154.10.146
File Size (KB)	89.249	**Event Count**	67
File Type	PDF	**Seen On**	11 hosts
File Category	PDF files	**Seen On Breakdown**	1 sender → 10 receivers
Current Disposition	Unknown		
Threat Score	None		

Trajectory



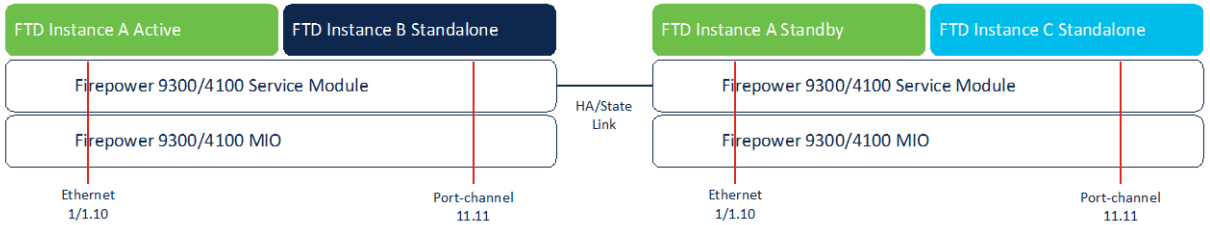
Events

Time	Event Type	Sending IP	Receiving IP	User	File Name	Disposit	Action	Protocol	Client	Web Appli	De...
2022-02-22 15:...	Transfer	131.154.10.146	93.47.42.249		Met_Num_21.pdf	Unk...	Malware Block	HTTP	Chrome	Google	
2022-02-22 16:...	Transfer	131.154.10.146	79.36.17.63		Met_Num_21.pdf	Unk...	Malware Clo...	HTTP	Chrome		

Multi-Instance

- Install multiple FTD logical devices on a single module or appliance
  - Container architecture
  - Instance failure does not affect other instances
- Allows tenant management separation, independent instance upgrade
- Supports HA between identical instances on different physical devices
- Example: 54 instances on a FPR9300 chassis with 3 x SM-56 modules
- Improved crypto acceleration in hardware

NEW



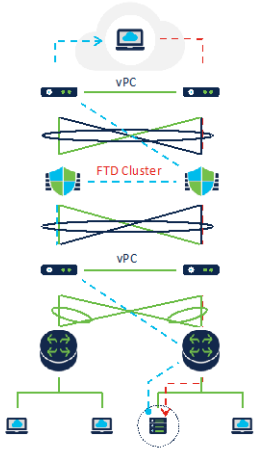
cisco SECURE © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential

Clustering

Drive high return on investment while maintaining high availability

- Combine multiple devices to make a single scalable logical device
- Scale as you grow
  - Scale throughput, concurrent and new connection
  - Can span multiple datacenters
- N+1 resilience
- Handles asymmetric traffic seamlessly

Example: 6 node cluster created by 2 x FPR9300 fully loaded chassis (with SM-56)
336 Gbps AVC
307 Gbps AVC+IPS



cisco SECURE © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Partner Confidential

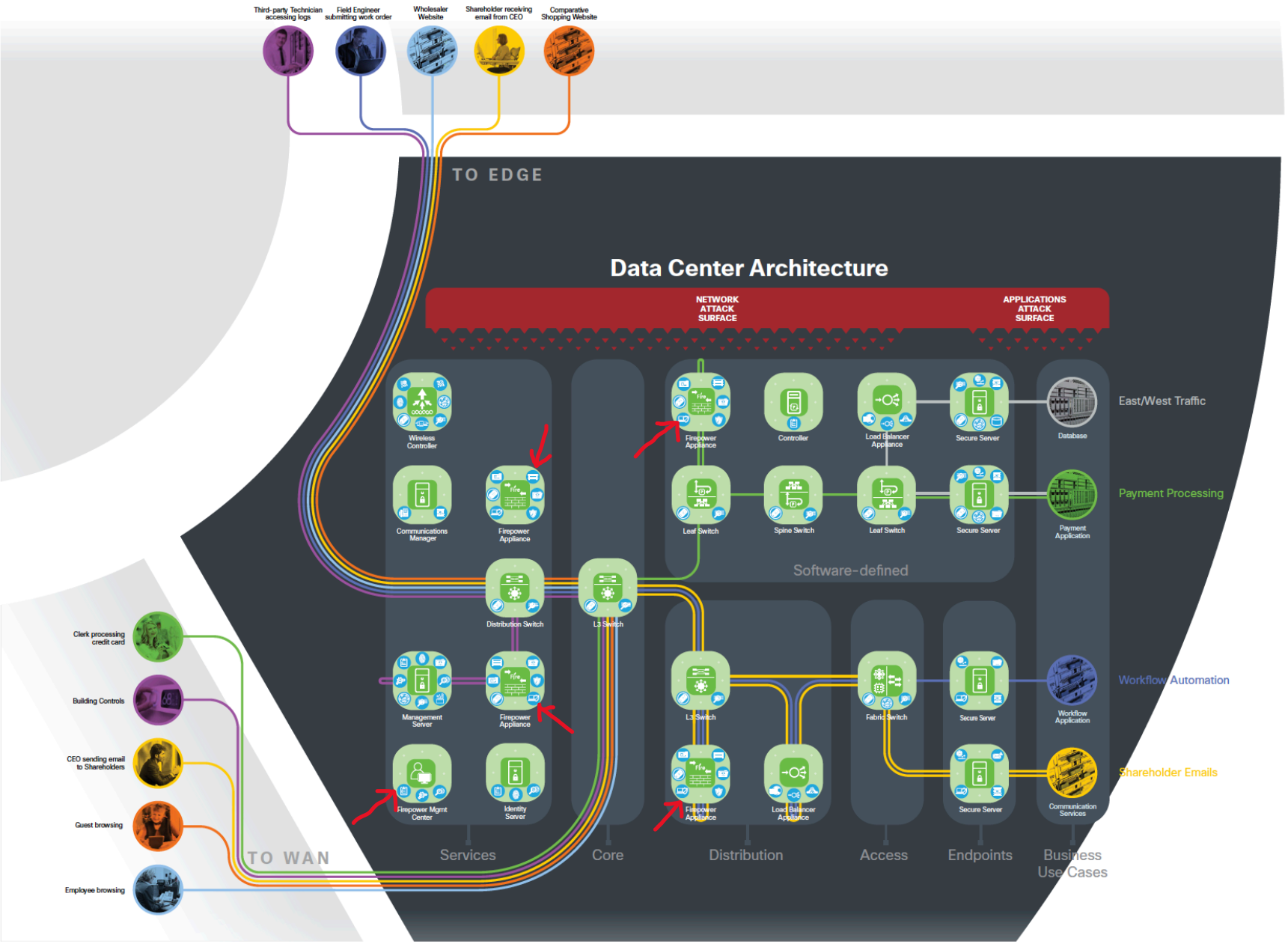


Figure 8 ***Secure Data Center.*** *The Secure Data Center business flows and security capabilities are arranged into a logical architecture. The colored business use cases flow through the green architecture icons with the required blue security capabilities.*

Gartner & Co (NGFW e EPP)