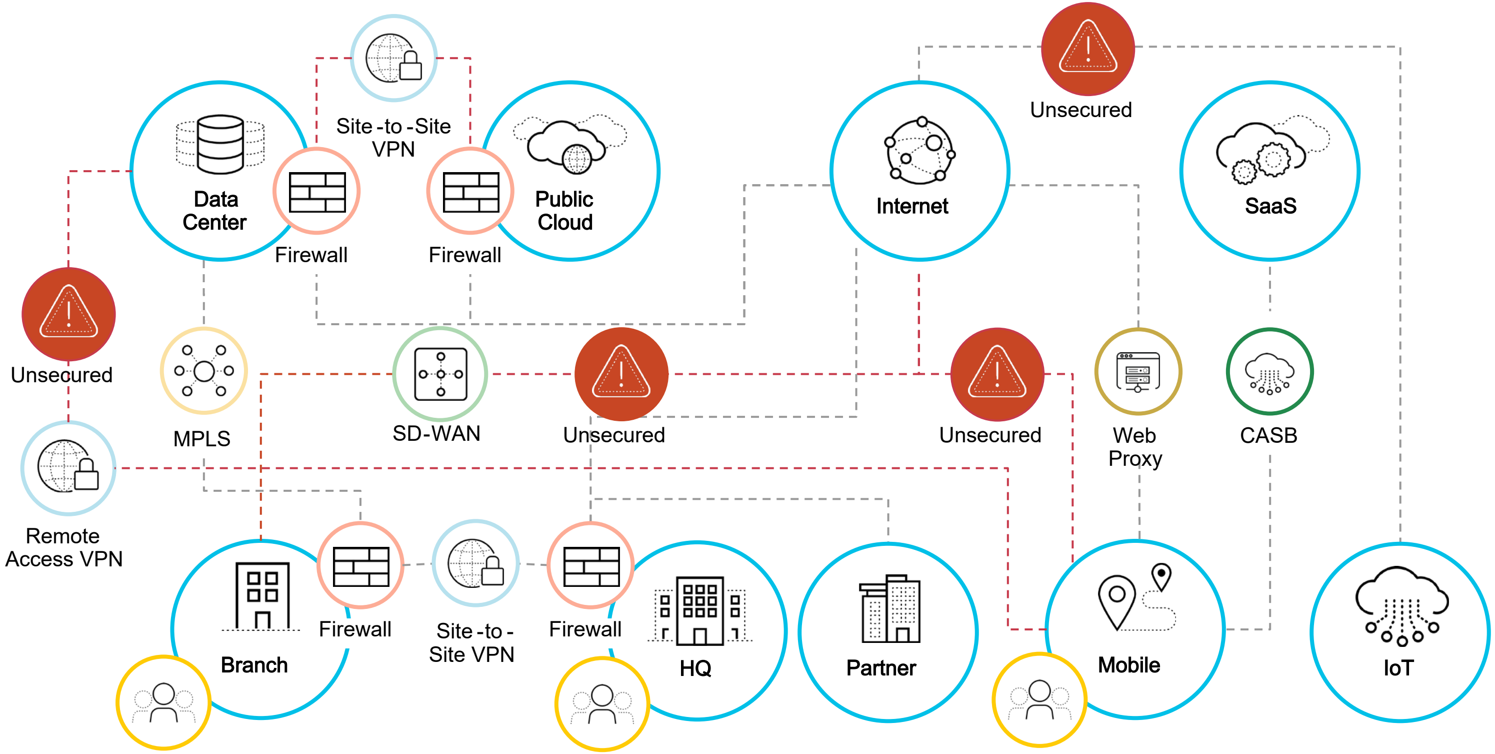
Simplifying Security with Industry -
Leading Services

Nov 2020

Legacy Network Security Architecture



1 Complex

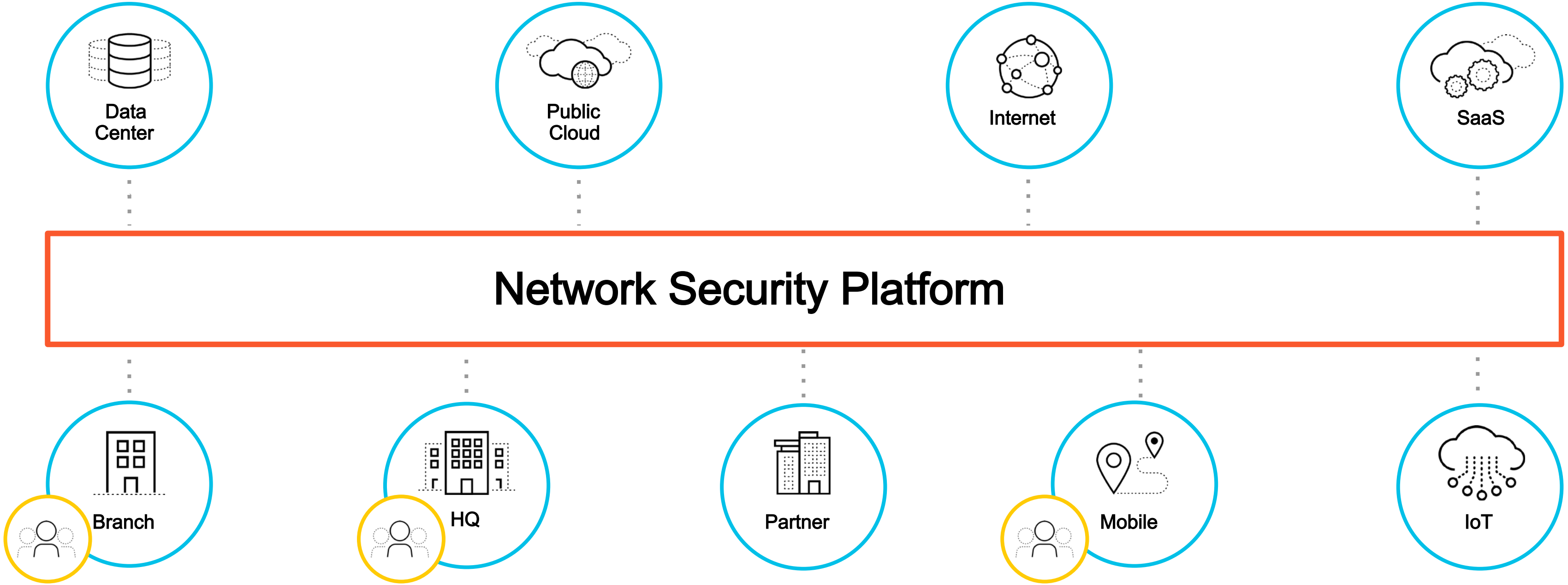
2 Security Gaps

3 Poor User Experience

Legacy Multi -Vendor Approach vs. Platform Approach

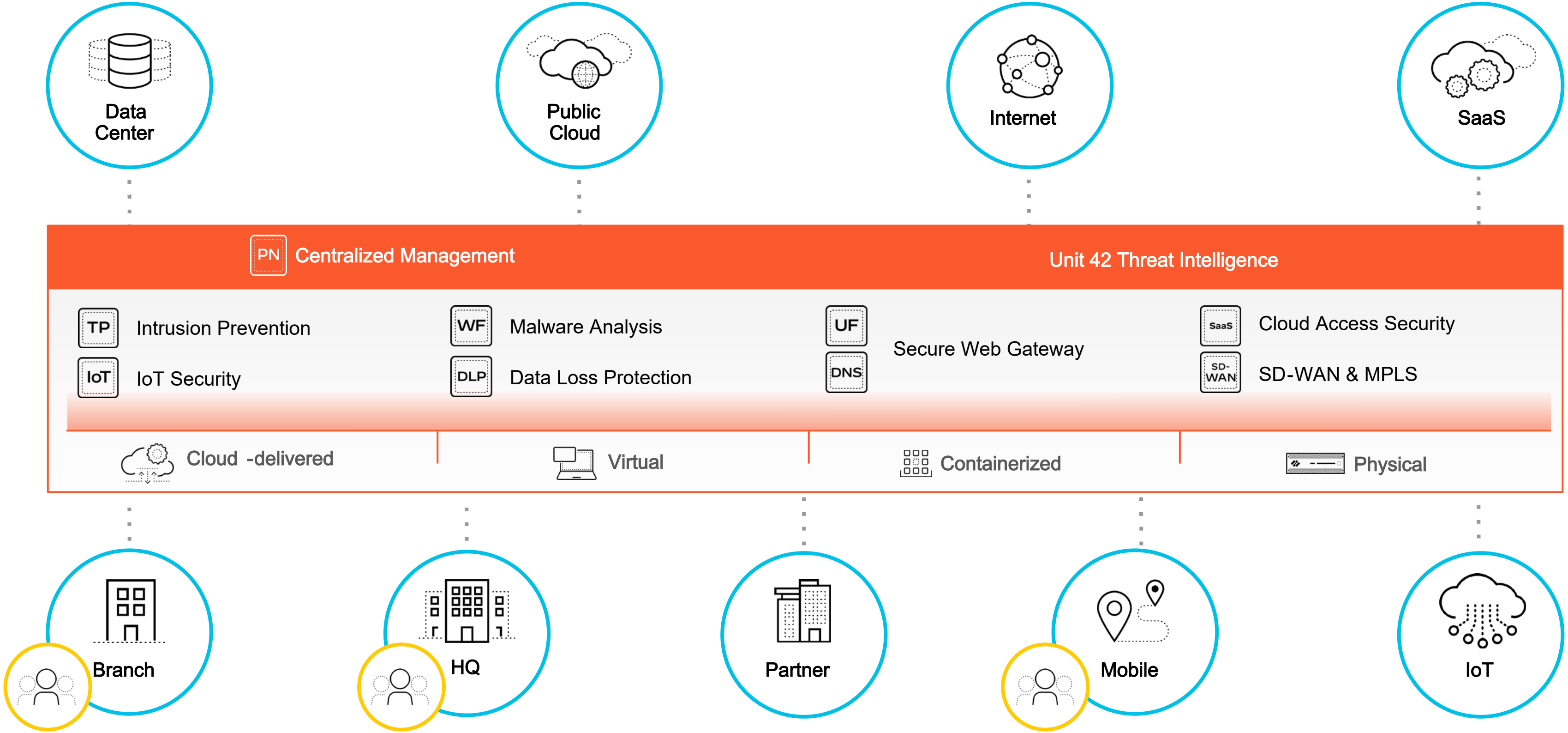
Capability (examples)	Current State	Future State – Platform	paloalto NETWORKS
Firewall	Check Point SOFTWARE TECHNOLOGIES LTD	NGFW	CN-Series PA-Series VM-Series
Intrusion Detection	TREND MICRO	Threat Prevention	TP
URL Filtering	BROADCOM	URL Filtering	UF
Sandbox Detection	FIREEYE	WildFire	WF
DNS Security	CISCO	DNS Security	DNS
IoT Security	ARMIS.	IoT Security	IoT
Data Loss Prevention (DLP)	BROADCOM	Enterprise DLP	DLP
Remote Access for Users	CISCO	GlobalProtect	GP
Endpoint + EDR Security	CROWDSTRIKE	Cortex™ XDR	
Public Cloud Security / Compliance	netskope	Prisma™ Cloud	
Secure Web Gateway	zscaler	Prisma™ Access	
SaaS Security / SaaS Compliance	FORCEPOINT POWERED BY Raytheon	Prisma™ SaaS	
SD-WAN	velocloud	SD-WAN	SD-WAN

A Single Platform to Connect and Secure Everything



✓ Consistent ✓ Integrated ✓ Best -in -class

A Single Platform to Connect and Secure Everything



Data Center

Public Cloud

Internet

SaaS

PN Centralized Management

Unit 42 Threat Intelligence

TP Intrusion Prevention

IoT IoT Security

WF Malware Analysis

DLP Data Loss Protection

UF DNS Secure Web Gateway

SaaS Cloud Access Security

SD-WAN SD-WAN & MPLS

Cloud -delivered

Virtual

Containerized

Physical

Branch

HQ

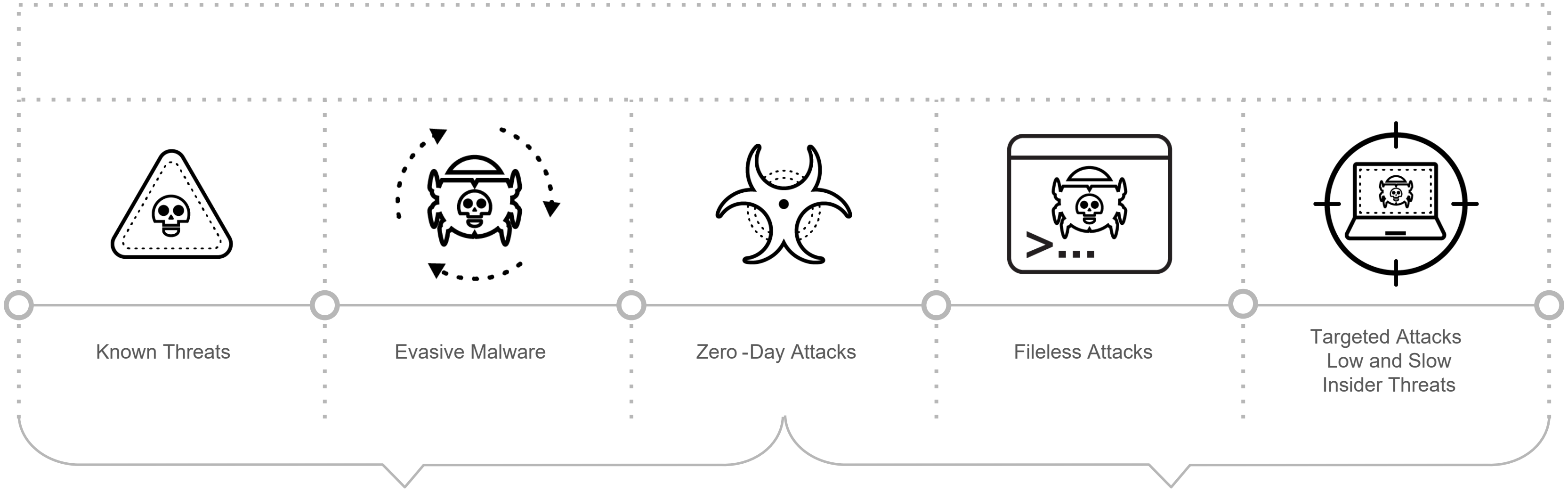
Partner

Mobile

IoT

Threat Prevention

Challenges: Stopping Threats in Today’s Threat Landscape



Known Threats

Evasive Malware

Zero -Day Attacks

Fileless Attacks

Targeted Attacks
Low and Slow
Insider Threats

Easiest to Execute

Most Sophisticated & Damaging

Organizations are ***33% more likely to be breached in 2019*** than they were just 5 years ago.

Challenges in Preventing Known Threats

Limited Visibility

Traffic only inspected on certain parts of network

Poor Performance

Requires tradeoff of security vs. performance

Failure to Evolve

Lack of innovation beyond basic IPS/IDS

Palo Alto Networks Threat Prevention Eliminates Known Threats

Vulnerability Protection

Detect and block Exploitation

Anti -Virus Protection

Based on Content Not hash

Command & Control Protection

Research grade signatures

Combine with WildFire, URL Filtering and DNS Security to extend protection at every stage of the attack lifecycle, including from both known and unknown threats

Category -Defining Network Protection

Threat Category	**Vulnerability**	**Brute Force**	**Antivirus**	**Command -and - Control**	**File Identification**	**Malicious IP**
Protection Against	• Exploit attempts • Vulnerabilities • Evasion techniques • Obfuscation attempts • SQL Injection	• Port scans • Buffer overflows • Protocol fragmentation	• Content based signatures not hash based • Known malware and unknown variants.	• Command Shells • Malicious domains • Payload inspection • DNS sinkholing	• Known bad or risky file types • Identify password protected	• Known malicious • High -risk • Bulletproof hosting

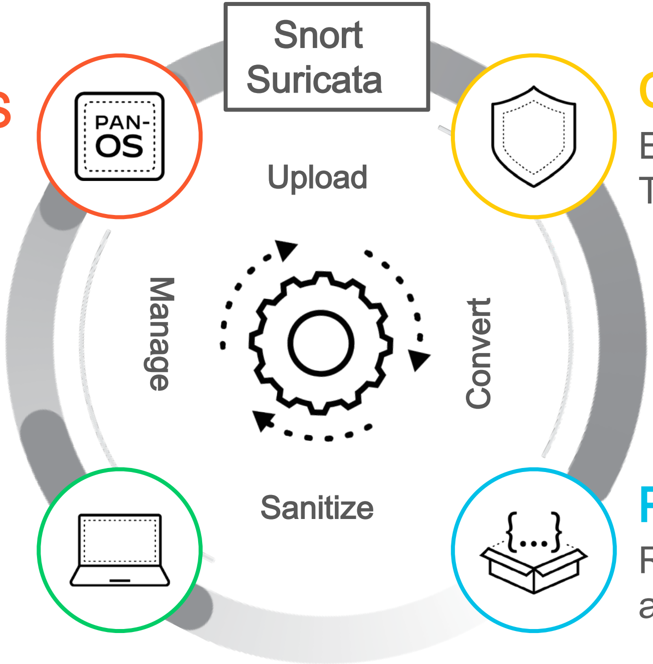
2019 NSS Labs Next -Generation Intrusion Prevention System (NGIPS) Test

Test*	Result
Security Effectiveness	98%
Exploit Block Rate	99.01%
Evasions Blocked	493/494
Stability & Reliability	PASS
NSS-Tested Throughput	21.252 Gbps

*Palo Alto Networks PA -5250 NGFW running PAN -OS 9.0.3-h2 with Threat Prevention

Comprehensive protection against server - and client -side network evasion techniques, exploit kits, command -and -control activity and phishing attacks

Snort/Suricata Compatibility in Threat Prevention



Snort on PAN -OS

Delivered

Customized Protection

Easily add unique rules to Threat Prevention coverage

Flexible Management

GUI, CLI, or API

Powerful API Support

Rapidly apply new coverage across environment

Threat Prevention Stands Apart

Single pass architecture enabling unbeatable, predictable performance

Comprehensive protection across the attack lifecycle

Innovative integrations for popular IDS/IPS formats

WildFire

The Challenge: Increasing Attacker Innovation

Speed and Proliferation of Attacks

Easy-to -bypass legacy analysis techniques

Increasing attack surface

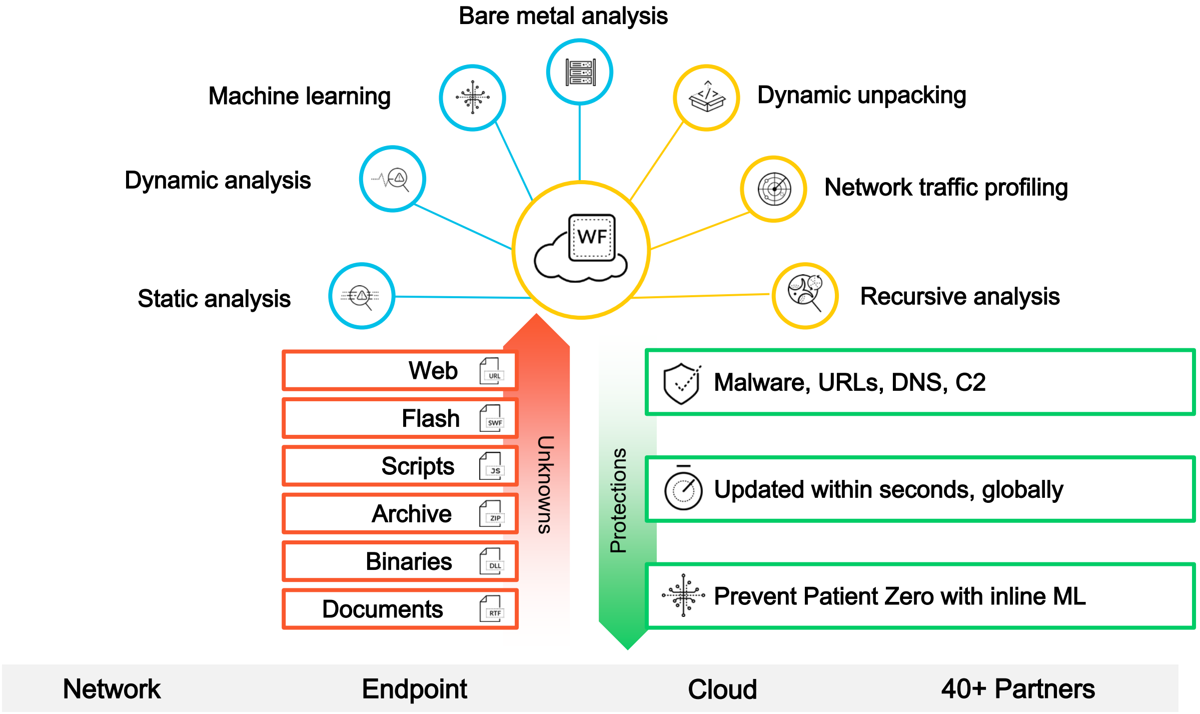
WildFire Goes Beyond Traditional Sandboxing

Detect and prevent unknown threats with data from a global community

Stay ahead of the latest attack techniques

Automate prevention and gain threat intelligence for advanced attacks

Detect and Prevent New Threats with WildFire Malware Analysis

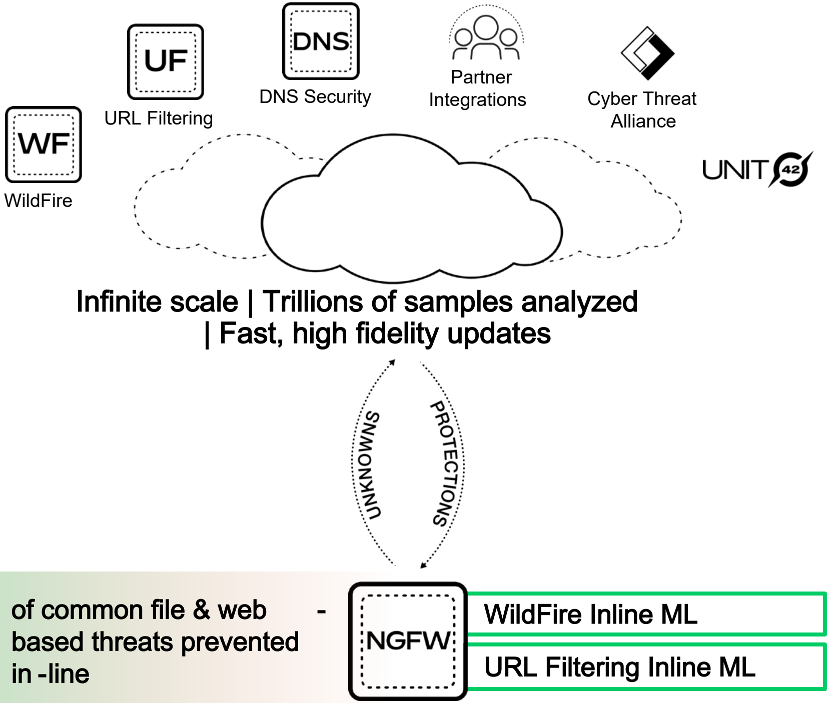


Data collected from a vast global community

Analysis techniques far beyond traditional sandboxing

Automated protection against multiple attack variants

Today’s Prevention of Unknown Threats Through Cloud Scale



Infinite scale | Trillions of samples analyzed | Fast, high fidelity updates

WildFire Inline ML

URL Filtering Inline ML

Up to 95% of common file & web - based threats prevented in -line

Cloud -delivered security services **scale prevention** capabilities

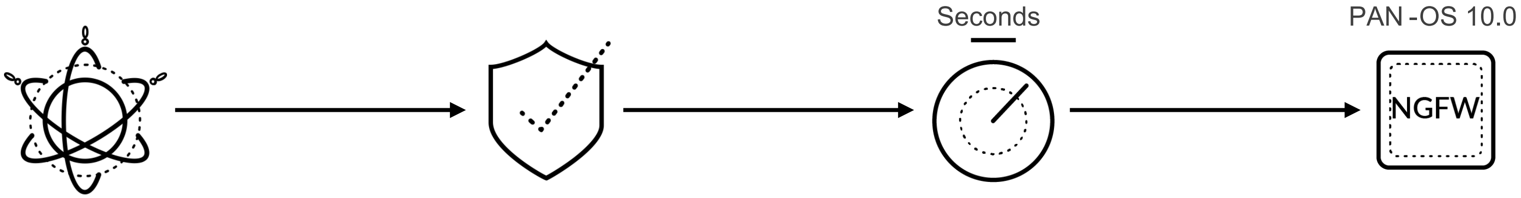
Shared intelligence allows the **fastest distribution** of protections

File Protections: Instant

URL Protections : Instant

DNS Protections: Instant

Slashing Our Industry -Leading Time for Distributed Protections



Threat detected across 35K+ WF installed base

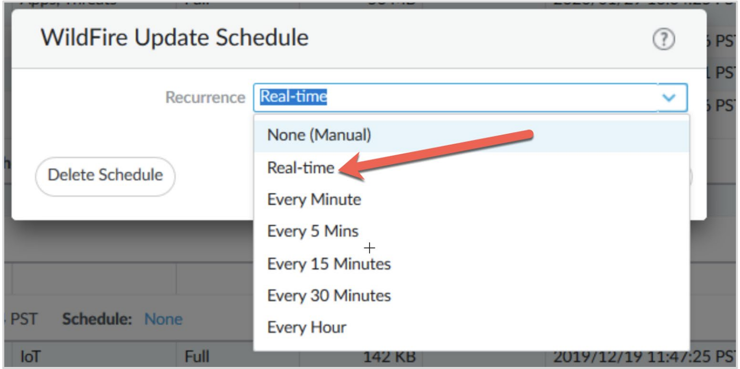
Content -Based Signature Created

Protection streamed in seconds

All customers with WildFire updated

BEFORE

Industry-leading *5-minute* signature generation/ distribution time



WildFire Update Schedule

Recurrence: Real-time

None (Manual)
Real-time
Every Minute
Every 5 Mins
Every 15 Minutes
Every 30 Minutes
Every Hour

With PAN -0S 10.0

Protection streams to NGFW in *single -digit seconds*

The WildFire Advantage

Industry -First inline ML prevention

Up to

95%

Unknown threats blocked at the NGFW

Cloud Analysis with Massive Data Set

16B+

Unique Malware Samples (6x more than Virus Total)

Crowdsourced Threat Intel

37k+

Customers for Network Effect

DLP

Pressing Problems with Sensitive Data

Data Breaches

Personally identifiable information (PII),

Intellectual property (IP)

Regulatory Compliance

GDPR, CCPA etc. - data privacy

PCI-DSS - payment card data

HIPAA - health information privacy

SOX - financial data accuracy

Insider Behavior

Malicious insiders

Negligent insiders

Unsolved Challenges - Where Legacy Solutions Fall Short

DLP has become too complex

- Fragmented deployment
- Configurations and upgrades
- Siloed environments

DLP has become too expensive

- Many products / licenses
- On -prem infrastructure
- Dedicated team

DLP is resource intensive

- Data protection program
- Policy tuning / incident response
- Too many alerts

DLP Answers Organizations’ Critical Questions About Their Data

Automatically discover, monitor and protect sensitive data

Discover

Locate where your sensitive data is across your clouds, networks, endpoints...

Monitor

Understand how your sensitive data is being used

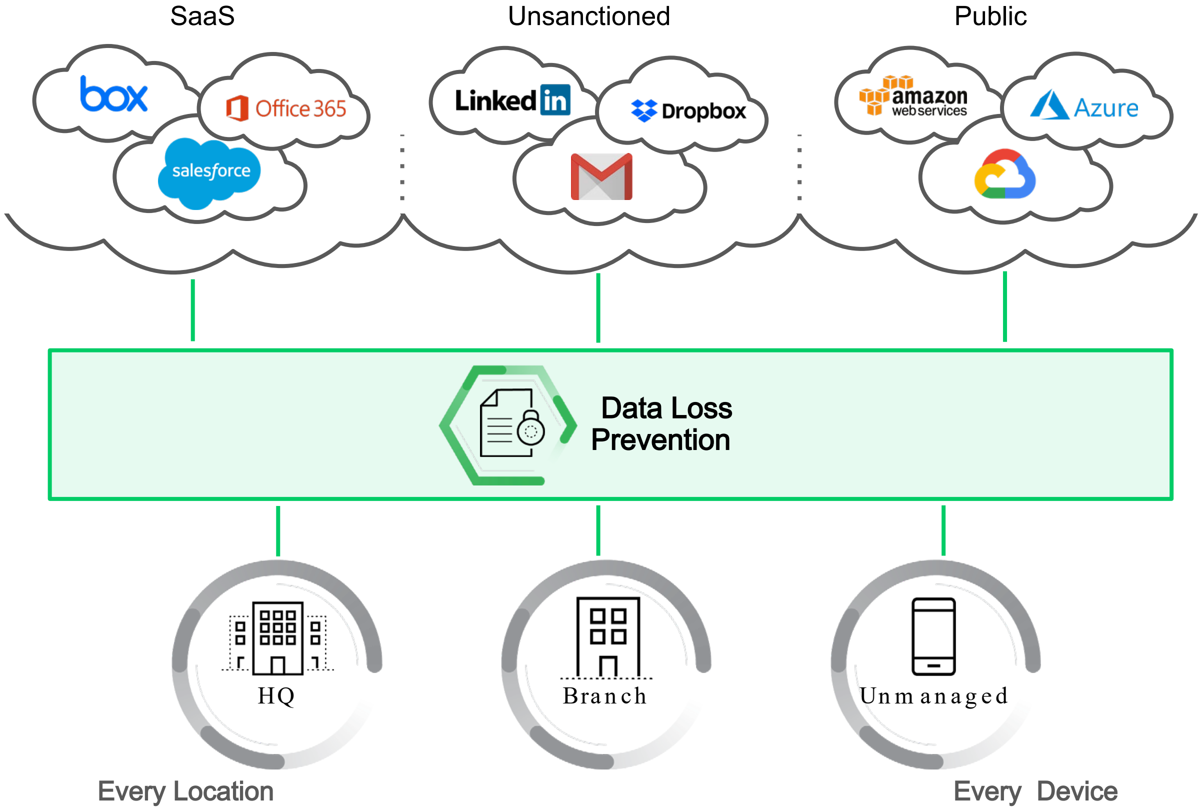
Protect

Stop sensitive data leakage by enforcing protection policies and educating employees

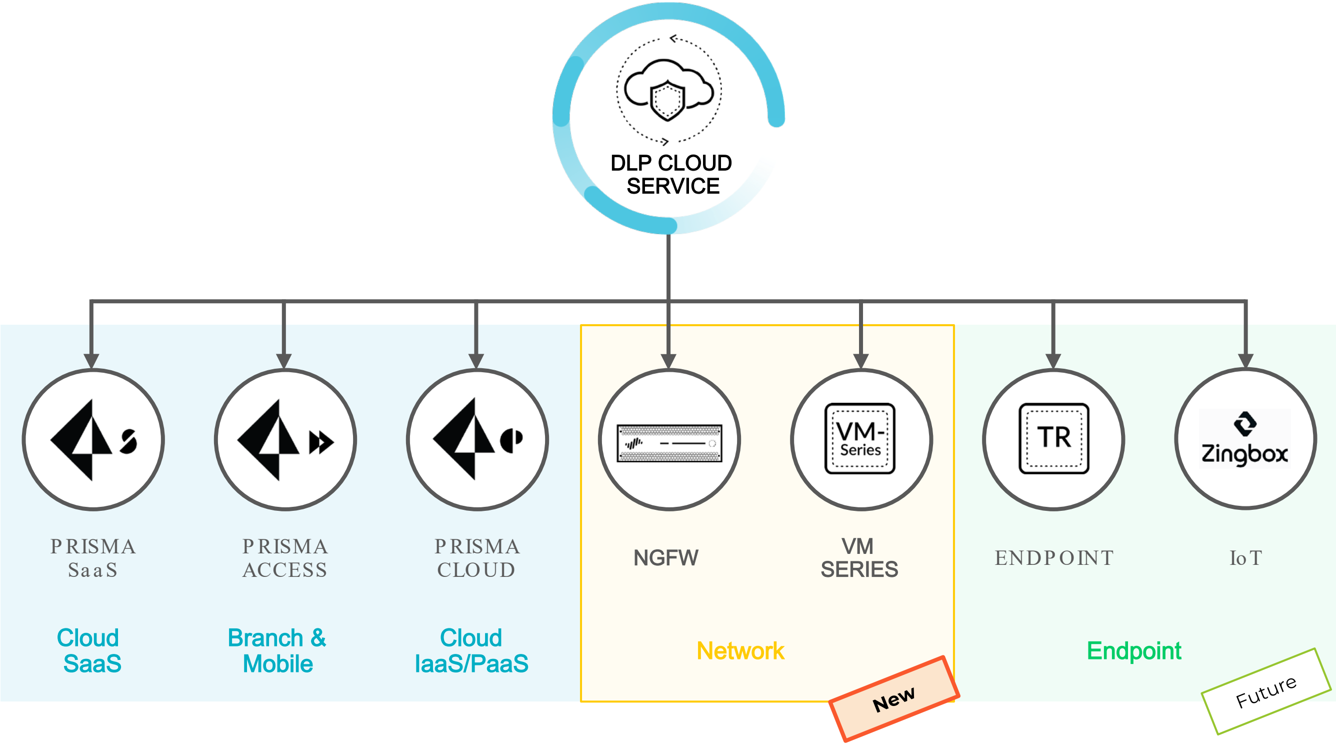
Digital Transformation Requires New Way of Data Protection

Comprehensive coverage. Consistent protection. Easy deployment.

- Comprehensive coverage
- Consistent protection
- Easy deployment



Our Vision: DLP Easily and Consistently Delivered Everywhere

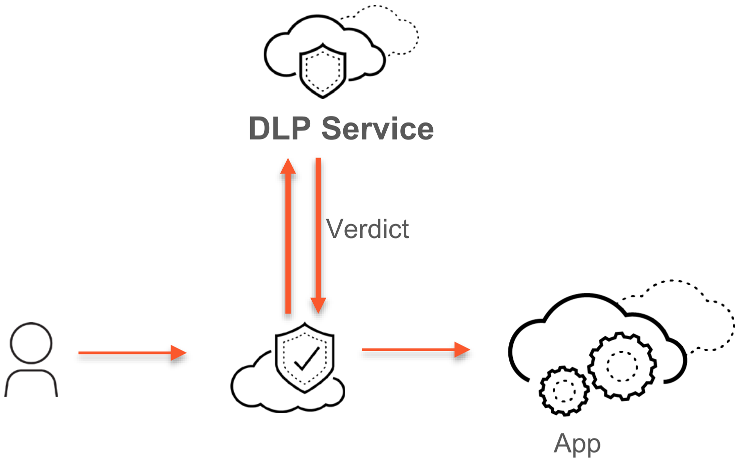


Single cloud DLP service embedded in existing control points

- Comprehensive Coverage
- Consistent Protection
- Easy Deployment

Note: the information contained herein is subject to change. It is not a commitment, promise or legal obligation and is inten ded to outline general product direction.

Main Capabilities



- Cloud-based DLP engine
  - **No deployments** or updates needed
  - **No ICAP or Proxies** needed
  - Configure once - **Auto sync** everywhere
  - Embedded in Palo Alto Networks products

- Predefined industry standard data classifiers
  - **Data Profiles** (GDPR, CCPA, PII, etc)
  - **350+ predefined** Data Patterns
    - Boolean Operations
    - Proximity analysis
    - Confidence levels
    - Weighted Regex
  - ML Classifiers
  - Flexible document properties
- Data in-motion and data at-rest

We Solve Our Customers’ Challenges with Data Protection

~~DLP has become too complex~~

Simpler Architecture

Centralized engine and unified detection policies everywhere data is

~~DLP has become too expensive~~

Lower TCO

Cloud delivered service - locally embedded everywhere in existing control points

~~DLP is resource intensive~~

Automation + Accuracy

Machine Learning for accuracy.
Scan all data always

URL Filtering

Challenges with Preventing Web -based Threats

$ ¥ €

Enable Business Without Compromising Security

Encrypted Web Content

Silo Management

URL Filtering

WEB SECURITY

Protection from web - based threats including malware, phishing, credential theft and C2

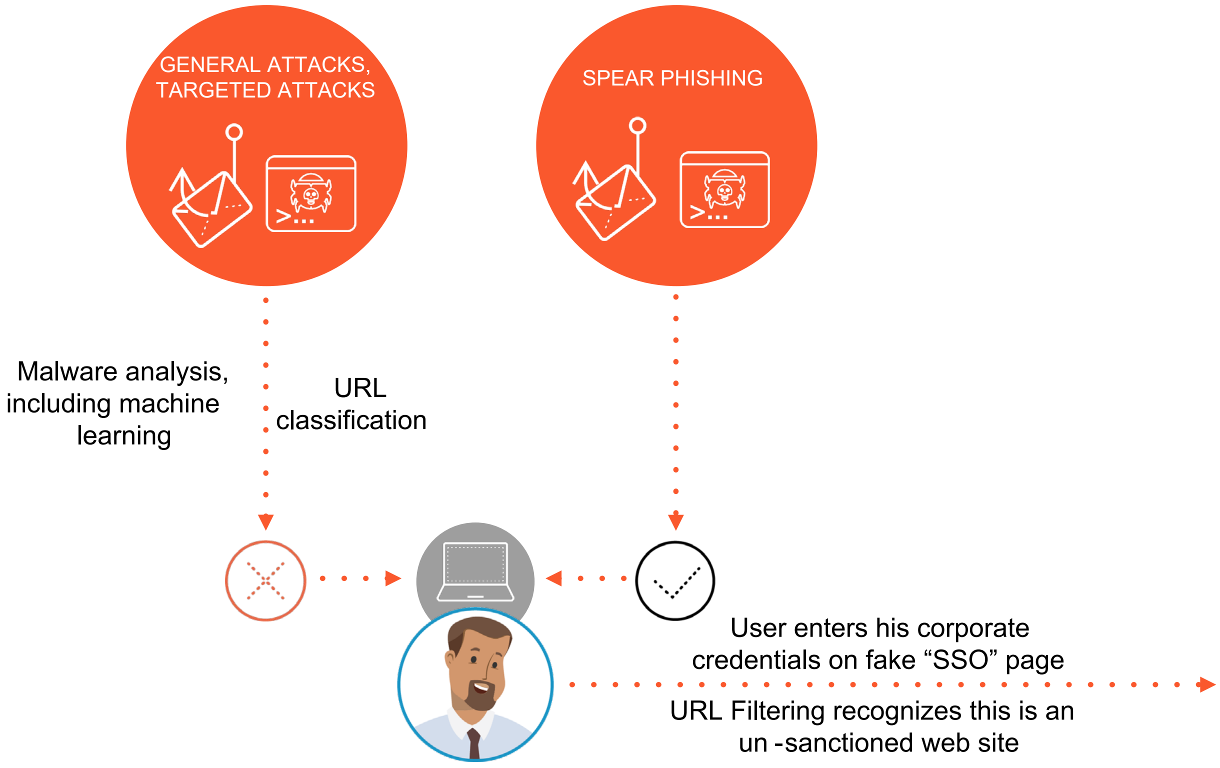
MADE SIMPLE

Extension of firewall policies, radically easy to enable SSL decryption and credential theft

MAXIMIZE EFFICIENCY

No additional hardware; automatically updated; streamlined innovation

User’s Identity Protected From a Variety of Attacks

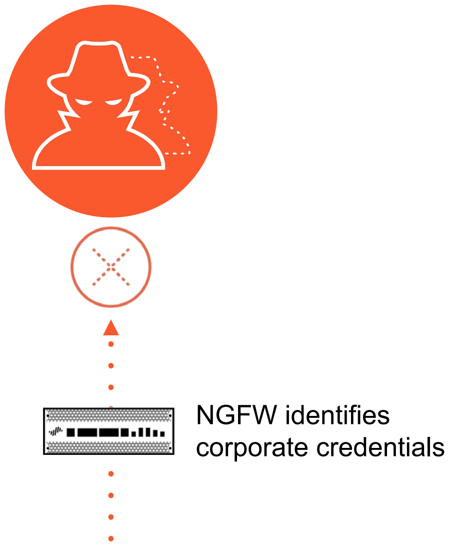


Malware analysis, including machine learning

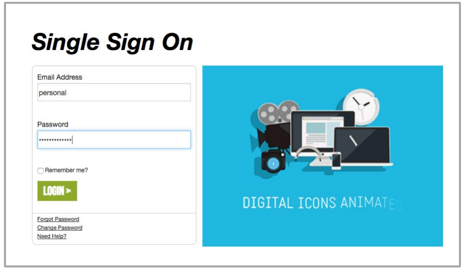
URL classification

User enters his corporate credentials on fake “SSO” page

URL Filtering recognizes this is an un -sanctioned web site



NGFW identifies corporate credentials



Single Sign On

Email Address: personal

Password: ••••••••••••••

☐ Remember me?

LOGIN >

Forgot Password
Change Password
Need Help?

DIGITAL ICONS ANIMATED

How it works: ML -based prevention for web -based attacks

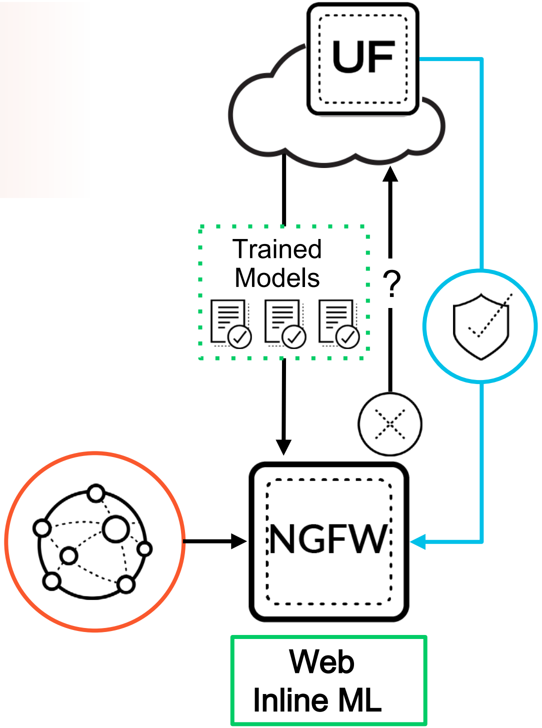
Cloud -based analysis

- Malicious or benign categories
- Categorization in minutes
- Policy -based actions

Up to **85%** of Web -based threats prevented in -line

⊘ Phishing Attacks

⊘ JavaScript Attacks



Thousands of brand new phishing attacks are launched every day

Over **30%** of phishing emails are opened within 60 seconds of being sent

Why Customers Prefer URL Filtering

Inline machine learning
at NGFW blocks new threats

Automated real -time
credential theft protection

Cloud scale with
Continuous Innovation

DNS Security

Modern Risks Presented by the DNS Protocol

80% of Malware

DNS is abused for command and control and data theft

UNIT 42

Rate of New Domains

Malware using domain generation algorithms evade detection

Data Exfiltration

Modern adversaries using DNS tunneling

OilRig

DNS Security

Blocks known bad domains

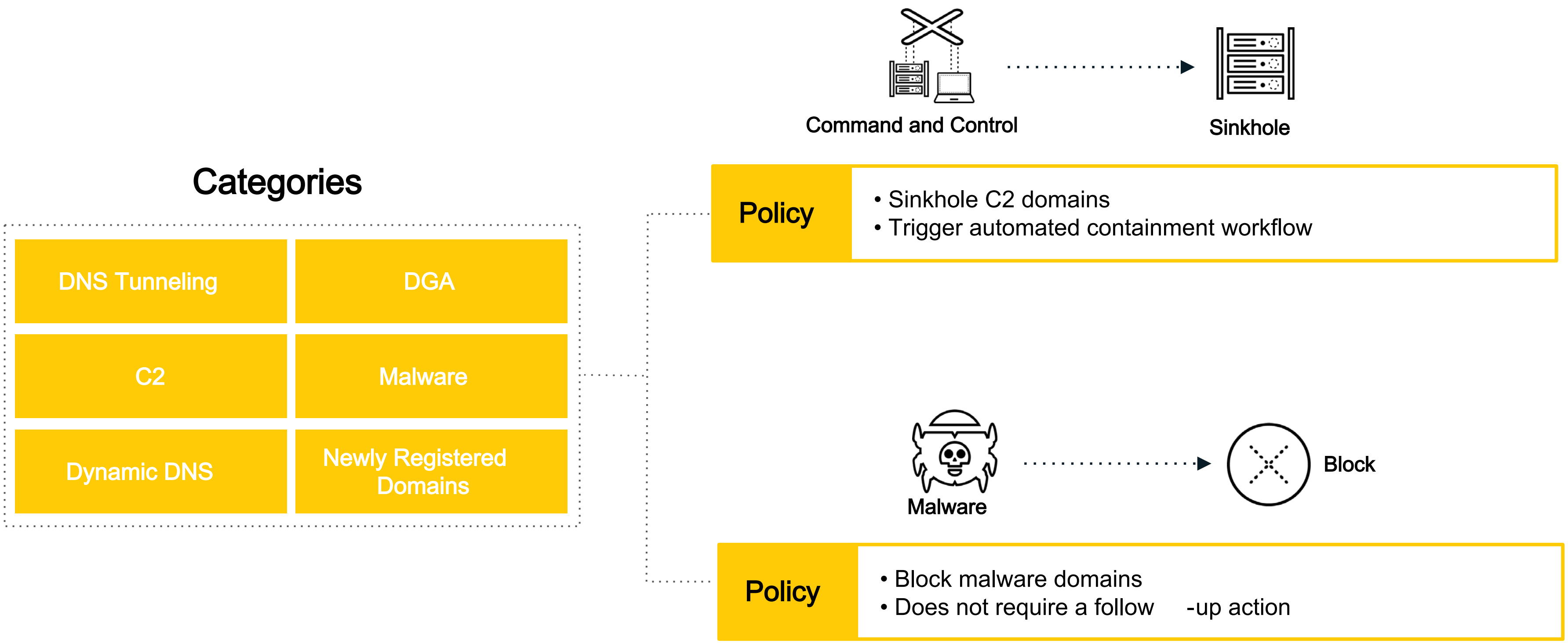
Stops malicious DNS traffic with ML and predictive analytics

Integration with NGFW means it cannot be bypassed

Data

- WildFire Analysis
- Passive DNS
- URL Filtering
- Honeynets
- Unit 42
- Whois

Category -Based Visibility and Control for DNS



Categories

DNS Tunneling	DGA
C2	Malware
Dynamic DNS	Newly Registered Domains

Policy

- Sinkhole C2 domains
- Trigger automated containment workflow

Policy

- Block malware domains
- Does not require a follow -up action

DNS Analytics

DNS Visibility

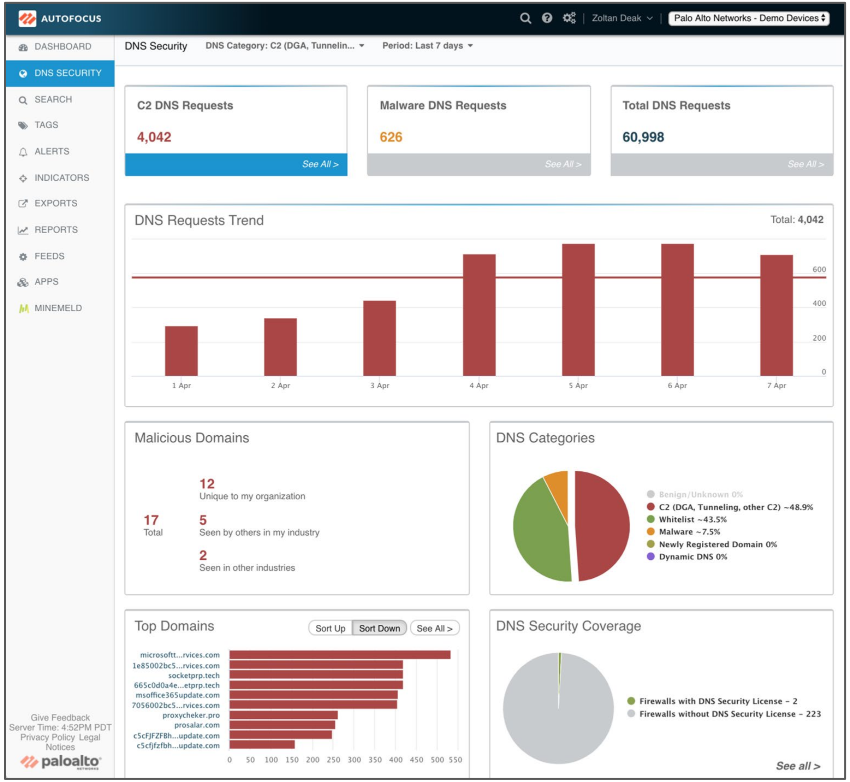
- Complete visibility across all DNS traffic and trends
- Filter based on DNS categories and timeframes
- Abuse of DNS (malware, C2, tunneling, DGA)

DNS Intelligence Context

- Why a domain was blocked
- Pivot to related threat intel
- AutoFocus Tags
- Whois and passive DNS data

DNS Hygiene

- Quickly view which firewalls in your estate are covered by DNS Security



DNS Security
DNS Category: C2 (DGA, Tunnelin...
Period: Last 7 days

Server Time: 4:52PM PDT

C2 DNS Requests 4,042

Malware DNS Requests 626

Total DNS Requests 60,998

DNS Requests Trend Total: 4,042

Malicious Domains

17 Total

12 Unique to my organization

5 Seen by others in my industry

2 Seen in other industries

DNS Categories

- Benign/Unknown 0%
- C2 (DGA, Tunneling, other C2) ~48.9%
- Whitelist ~43.5%
- Malware ~7.5%
- Newly Registered Domain 0%
- Dynamic DNS 0%

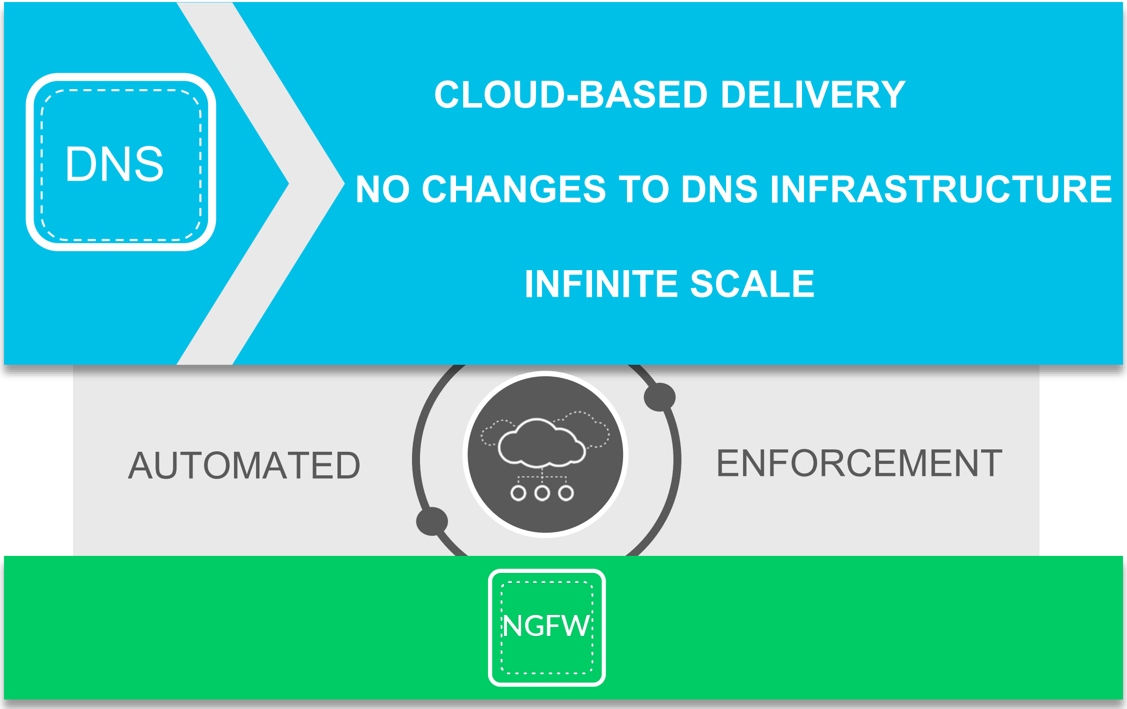
Top Domains

microsoftt...rvices.com
1e85002bc5...rvices.com
socketprp.tech
665c0d0a4e...etprp.tech
msoffice365update.com
7056002bc5...rvices.com
proxycheker.pro
prosalar.com
c5cFJFZFBh...update.com
c5cfjfzfbh...update.com

DNS Security Coverage

- Firewalls with DNS Security License – 2
- Firewalls without DNS Security License – 223

The DNS Security Difference



DNS

CLOUD-BASED DELIVERY

NO CHANGES TO DNS INFRASTRUCTURE

INFINITE SCALE

AUTOMATED

ENFORCEMENT

NGFW

IoT Security

IoT is a Business Necessity that Introduces Risk

Massive Increase in Connected devices

30% of devices on enterprise networks today are IoT

Pose a Huge Security Risk

Shipped with vulnerabilities and difficult to patch, yet have unfettered access

Securing IoT Devices is Hard

Incredibly diverse devices; traditional IT security controls do not work

Why Current Solutions Fail

Limited Visibility

Cannot identify previously unseen IoT devices, accuracy requires constant effort

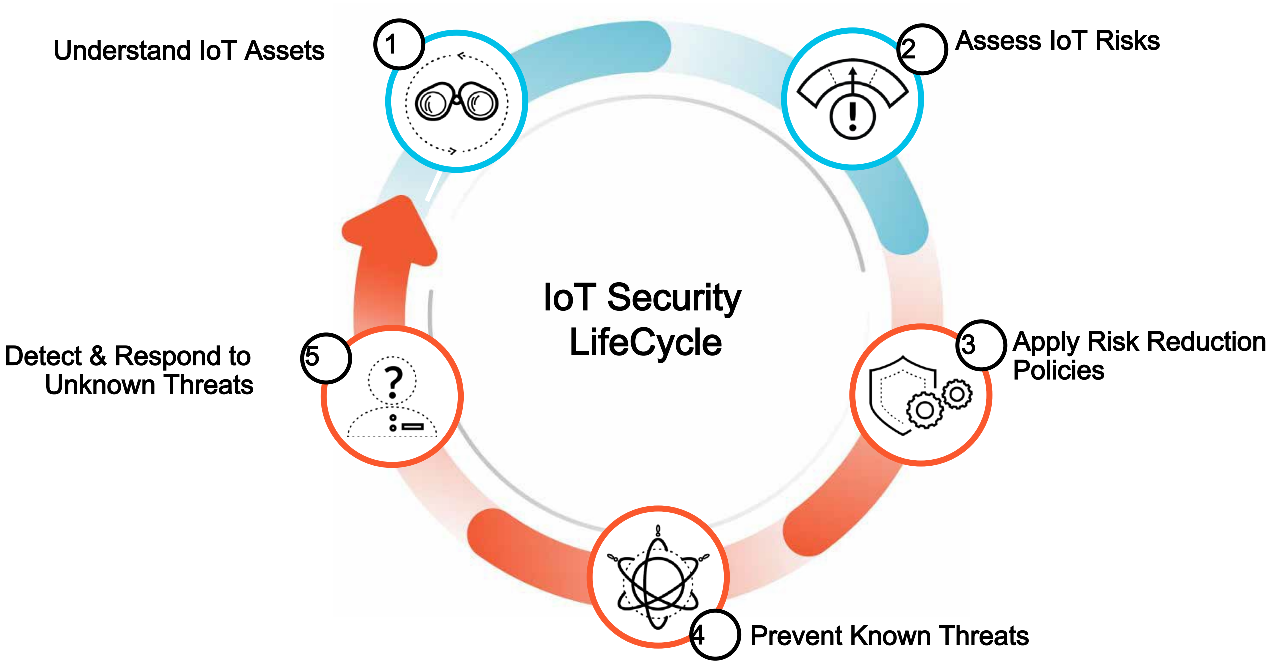
No Protection

Existing visibility-centric solutions do not offer native prevention or enforcement

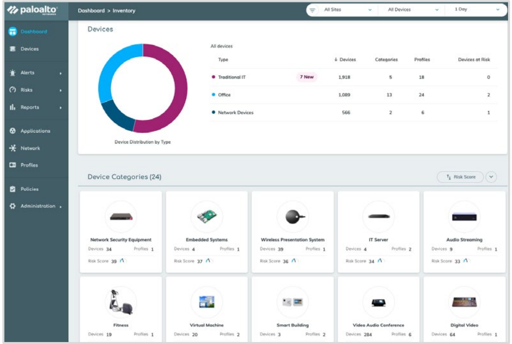
Hard to Implement

Require changes to network infrastructure, security team workflows and integrations

A New Methodology to Secure IoT Devices



Introducing IoT Security



Devices

All devices

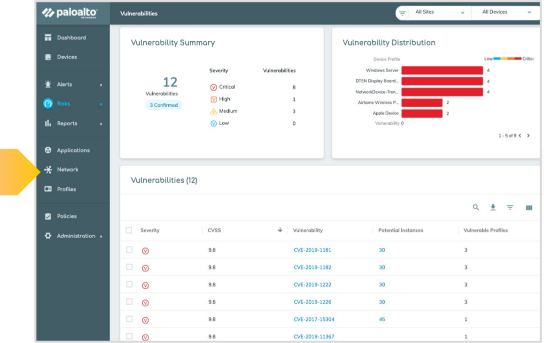
Type	↓ Devices	Categories	Profiles	Devices at Risk
● Traditional IT 7 New	1,918	5	18	0
● Office	1,089	13	24	2
● Network Devices	566	2	6	1

Device Categories (24)

Category	Devices	Profiles	Risk Score
Network Security Equipment	34	1	39
Embedded Systems	4	1	37
Wireless Presentation System	39	1	36
IT Server	4	2	34
Audio Streaming	9	1	33
Fitness	19	1	
Virtual Machine	20	2	
Smart Building	3	2	
Video Audio Conference	284	6	
Digital Video	64	1	

Complete Visibility

Accurately identify and classify all devices with ML, including those never seen before



Vulnerability Summary

12 Vulnerabilities

3 Confirmed

Severity	Vulnerabilities
Critical	8
High	1
Medium	3
Low	0

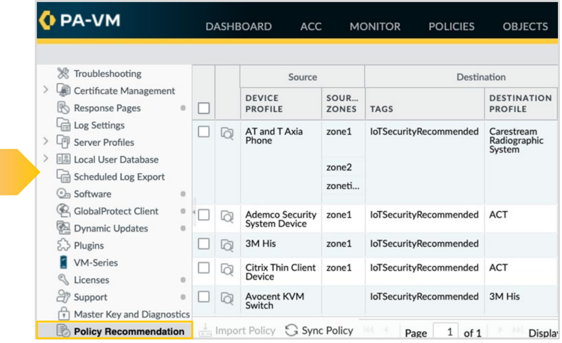
Vulnerability Distribution

Vulnerabilities (12)

Severity	CVSS ↓	Vulnerability	Potential Instances	Vulnerable Profiles
ⓥ	9.8	CVE-2019-1181	30	3
ⓥ	9.8	CVE-2019-1182	30	3
ⓥ	9.8	CVE-2019-1222	30	3
ⓥ	9.8	CVE-2019-1226	30	3
ⓥ	9.8	CVE-2017-15304	45	1
ⓥ	9.8	CVE-2019-11367		1

In-depth Risk Analysis

Quickly understand anomalies, vulnerabilities and severity to make confident decisions



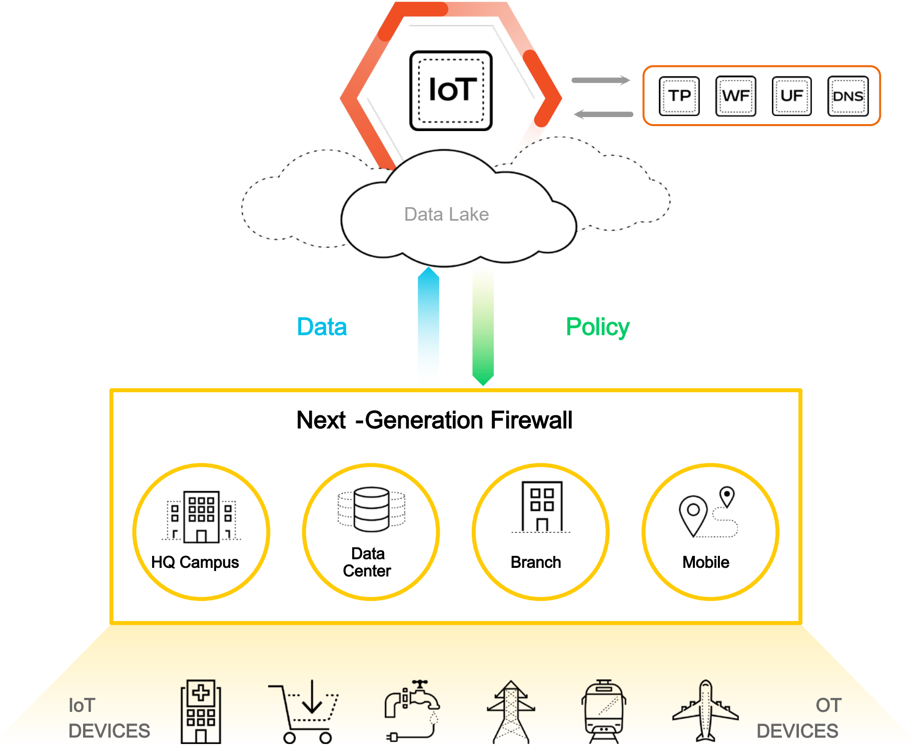
	Source		Destination	
□	DEVICE PROFILE	SOUR... ZONES	TAGS	DESTINATION PROFILE
□	AT and T Axia Phone	zone1 zone2 zoneti...	IoTSecurityRecommended	Carestream Radiographic System
□	Ademco Security System Device	zone1	IoTSecurityRecommended	ACT
□	3M His	zone1	IoTSecurityRecommended	
□	Citrix Thin Client Device	zone1	IoTSecurityRecommended	ACT
□	Avocent KVM Switch		IoTSecurityRecommended	3M His

Built-in Enforcement

Safely automate enforcement on your next-gen firewall with a new Device-ID policy construct

|

Best -in -Class Enterprise IoT Security Deployed Effortlessly



- ✓ Available on NGFW form factors - Hardware & Software
- ✓ Start with your existing NGFW or expand for coverage
- ✓ Scale linearly with multi -tenant cloud infrastructure
- ✓ Leverage leading prevention from other Security Services

Trust Every Device On Your Network

Use Your Infrastructure

Deploy within minutes, no siloed sensors or enforcement products required

Leverage Existing Talent

Maintain current operations and empower your existing Network Security team to protect IoT

Get Complete IoT Security

Discover, secure and prevent threats on every IoT device in your network with one solution

Unit 42

DON‘T FORGET A TOWEL

UNIT 42

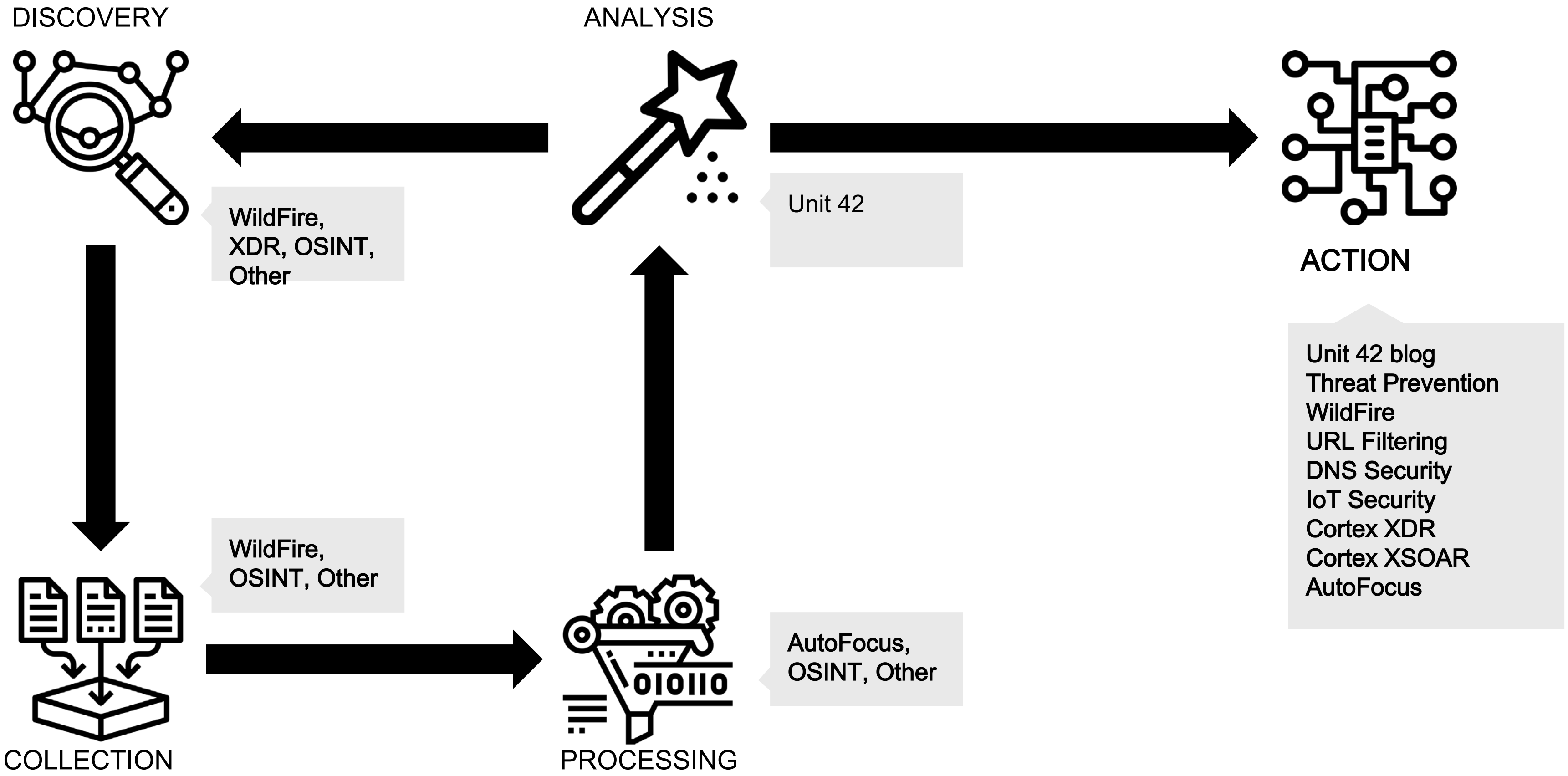
The ultimate question of life, the universe and everything

GLOBAL THREAT INTELLIGENCE TEAM

COLLABORATION

DON’T PANIC

Powerful Threat Intelligence Lifecycle Directly Benefits Customers



DISCOVERY

WildFire,
XDR, OSINT,
Other

COLLECTION

WildFire,
OSINT, Other

PROCESSING

AutoFocus,
OSINT, Other

ANALYSIS

Unit 42

ACTION

Unit 42 blog
Threat Prevention
WildFire
URL Filtering
DNS Security
IoT Security
Cortex XDR
Cortex XSOAR
AutoFocus

Tap into the Latest Research from Unit 42

Highlights

- Over 550 detailed threat blogs published
- Average of 80,000 unique monthly visitors
- Spotlight reports including Unit 42 2020 IoT Threat Report
- More than 21 Adversary Playbooks provide contextual insights across the entire attack lifecycle
- Threat intelligence research directly implemented into products (385+ actors and campaigns tagged)

unit42.paloaltonetworks.com

Muhstik Botnet Attacks Tomato Routers to Harvest New IoT Devices

Unit 42 discovered a new variant of the Muhstik botnet that now adds a scanner to attack Tomato routers for the first time by web authentication brute-forcing.

Unit 42 is the global threat intelligence team at Palo Alto Networks. Experts in hunting and collecting unknown threats, Unit 42 has been internationally recognized for key research on threats and campaigns. This interactive explores some of Unit 42's biggest contributions to threat intelligence research.

UNIT 42

HOW TO SPOT SPEAR PHISHING IN BEC SCHEMES

Spear phishing is a common social engineering tactic among threat actors, particularly as part of business email compromise (BEC) attacks.

What Is Spear Phishing?

Traditional phishing campaigns send generic email messages to a broad audience. Spear phishing is targeted and requires knowing some details about the victim.

47% of spear phishing attacks last less than 24 hours[1]

42% of IT security pros consider spear phishing one of the top three cyberattack concerns[1]

91% of email scams use spear phishing techniques[2]

The Spear Phishing Approach

1. Attacker chooses and researches a target
2. Attacker crafts malicious email that appears to come from an internal source ... current/potential business associate ... ically brief and specific ... nse of urgency

UNIT 42

THREAT FORECAST

CLOUDY WITH A CHANCE OF ENTROP

Summer 2019 Unit 42 Cloud Threat R

Platform vs. Real World Attacks

Rocke Threat Group Campaign

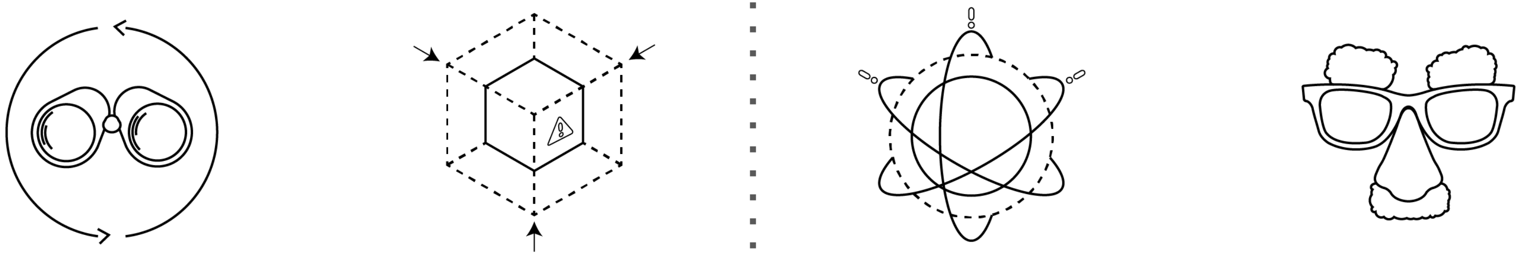
UNIT 42

PLAYBOOK VIEWER

Preventing Successful Attacks with Security Services

Delivered by NGFW

Powered by Security Services



Complete Visibility → Reduce Attack Surface → Prevent Known Threats → Prevent Unknown Threats

Consistent Across all Locations

Headquarters

Branch Offices

Data Center/ Private Cloud

IoT

Public Cloud

SaaS

Mobile Users

TP | WF | DLP | IoT

URL | DNS | SaaS

paloalto NETWORKS

Thank you

paloaltonetworks.com

Next Steps: Resources and Engaging with the Security Services Team

Security Services Loop Pages (Deep dive presentations, walkthroughs, collateral)

https://theloop.paloaltonetworks.com/loop/product-intel/strata/security-services

Office Hours:

- Every Two Weeks: Friday 10 AM-11AM PST | Link to add to Calendar
- Recent & Upcoming Features, Special Topics, Special Guests from Product Management, Customer Feedback, Sales and SE Q&A.

Slack Channels and Tek-Talk:

- #help-security-subscriptions
- #help-iot-security
- Tek-Talk

Leader in The Forrester Wave™: Enterprise Firewalls Q3'20 Report

Cloud-delivered services enable single security strategy across on-prem, cloud and endpoint

- **Ranked a LEADER** in The Forrester Wave™: Enterprise Firewalls Q3 2020 Report
- Received the **highest score in the Strategy and Cloud -Delivered components**
- Received the **highest possible score** in 17 criteria, including **IDS/IPS,** usability, threat intelligence, automated malware analysis, ICS/OT/IoT

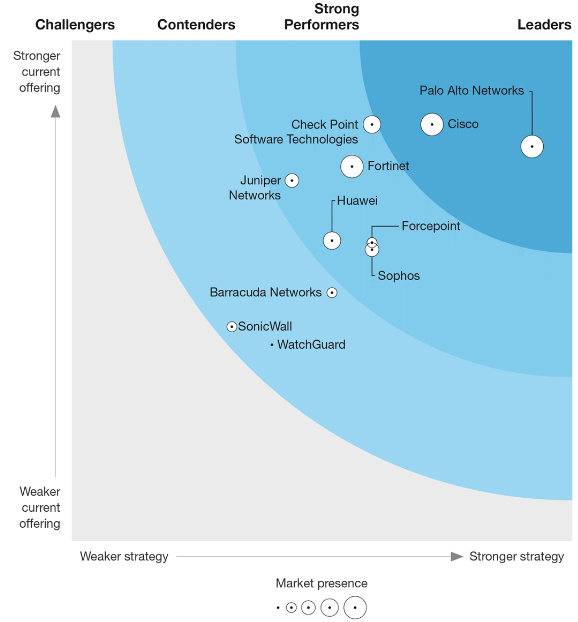
> *"Enterprise security buyers with a preference for a single solution vendor should look to Palo Alto Networks to enable their SOC staff and security program."*
>
> *-- The Forrester Wave™: Enterprise Firewalls Q3'20*

FORRESTER®

THE FORRESTER WAVE™

Enterprise Firewalls

Q3 2020



158796 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.