

ThreatSTOP DNS Firewall

～脅威インテリジェンス活用してクリーンなインフラを目指す～

脅威インテリジェンス活用の現状



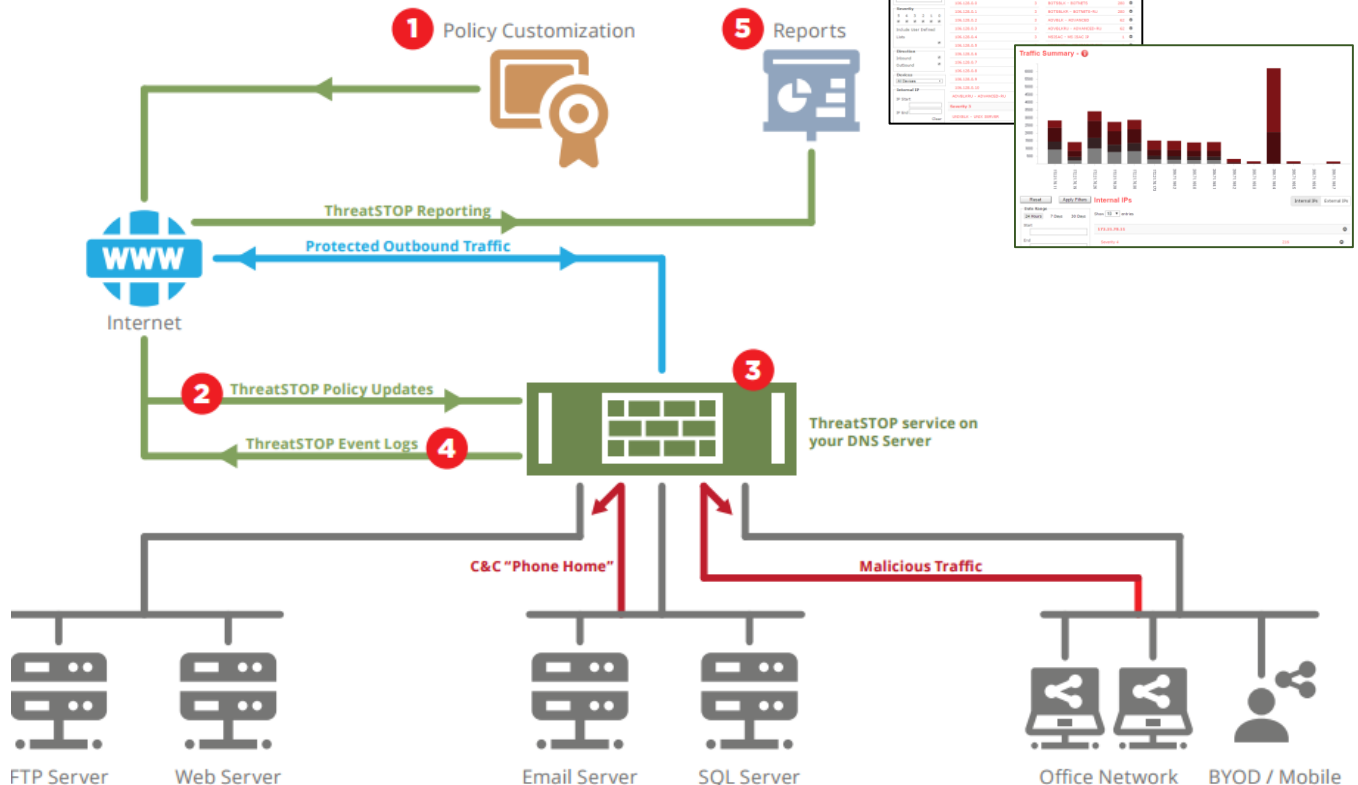
- ・ オペレーターが手動で危険な通信のあぶり出しをしている
 - ・ 脅威インテリジェンスの収集
 - ・ 脅威インテリジェンスの精査
 - ・ 脅威インテリジェンスとの照らし合わせ

せっかくのセキュリティ人材をもっと有効に使えるように、脅威インテリジェンスの活用はシステム化しませんか？

アウトバンド通信の要、DNSで危険な通信を遮断/隔離する

ThreatSTOPが危険なIPアドレス、ドメインの情報を集め精査したリストを自動でDNSサーバーに配信。DNSサーバーでの名前解決の際に、ThreatSTOPが持つ危険なIPアドレスもしくはドメイン名のリストと参照します。このときに、リストに該当する通信があれば、DNSサーバーへのクエリの無視もしくは通信の安全地帯への隔離を行います。

- ① ポータル画面でポリシーと、アクションを選択
- ② 自動で最新のポリシーがDNSサーバーにアップデート
- ③ 悪意を持ったアウトバンド通信をブロック
- ④ ブロックされた通信のログをThreatSTOPへ送信
- ⑤ ログをもとに、レポートを作成



精度の高い脅威インテリジェンス

サービスプロバイダーが脅威インテリジェンスの採用を検討するときに最も重要な要素はインテリジェンスの精度です。

ThreatSTOP社では、世界各国50以上の情報ソースから脅威インテリジェンスの情報を集めています。ソースはDShieldのように一般に公開されているものから、創業者およびThreatSTOPの多くのセキュリティ専門家が共有する軍事機関でのセキュリティ担当者の経験から得られるプライベートな情報ソースまで幅広く情報を集めています。

集められたインテリジェンスは、相関分析にかけます。分析によって作成されたリストで確認がないものは更にThreatSTOPのセキュリティ専門家たちが手動で調査を行い、真偽を判断します。

一度脅威リストに入った情報も、リストに残しておくべきか、外すべきか定期的にセキュリティ専門家が調査を行い、判断します。

この収集→分析→専門家による調査→定期的な調査のサイクルをまわすことによって、常に最新の脅威状況を反映した、精度の高いリストを提供することができます。

データソース例

- Dshield
- Farsight
- MS-ISAC
- ShadowServer
- AlienVault
- PhishTank
- DenyHosts
- AutoShun
- Team Cymru
- Spamhaus

などなど

脅威が脅威である裏づけ情報の提示

The screenshot displays a network log table with columns for Time, Device, Source IP, Destination IP, Action, Direction, and Targets. Below the log, there are sections for 'Positive DNS' and 'Media Data'. The 'Positive DNS' section shows a list of IP addresses and their associated domain names, with columns for Record ID, Record Type, Count, Last Time, and First Time. The 'Media Data' section shows details for a specific IP address, including its location (London, UK) and associated media data.

何故この通信はとめるべきなのか、を知らずに通信を止めるべきではありません。ThreatSTOPのレポート機能では、何故この通信の宛先は脅威と判断されたのか、という情報を示すことができます。

例えば、図1では同じIPアドレス宛に秒単位で通信が発生しています。通常人間がアクセスしようとしているだけなら、このように短い間隔で通信をすることはできません。ボット化していると考えられます。

図2では、止められたIPアドレスに連なるドメイン情報を表示しています。1つのIPアドレスに約1万のドメインが作られています。通常悪意を持たない人物がこれだけのドメインを使用するとは考えにくいです。

このほかにも、レポート画面には、SANSやWatchGuardなど他のセキュリティ調査機関、ベンダーが提供する情報へ飛べるリンクを設定しているため、第三者機関でそのIPアドレスがどのように判断されているのか確認することもできます。

世界1200社以上が採用！

2011年の製品販売開始以降、ThreatSTOPはアメリカ軍やイスラエル軍でのサイバーセキュリティの経験を持つセキュリティの専門家たちが、高い精度を持つ脅威インテリジェンスを提供してきました。2016年にはDNSの生みの親Dr. Paul MockapetrisをChief Scientistに向かえ、DNSの名前解決の時点で脅威をとめるDNS Firewallに力をいれています。世界で1200社以上がThreatSTOPの脅威インテリジェンスを採用していること、またセキュリティの専門家であるVerizonやアメリカ政府関係機関での採用していることが、ThreatSTOPが提供する脅威インテリジェンスの優位性の証です。



株式会社ネットワークバリューコンポネンツ

〒144-0035 東京都大田区南蒲田2-16-2

電話 03-5714-2050 Mail sales@nvc.co.jp Web http://www.nvc.co.jp/



ThreatSTOP

Weaponize Your Threat Intelligence

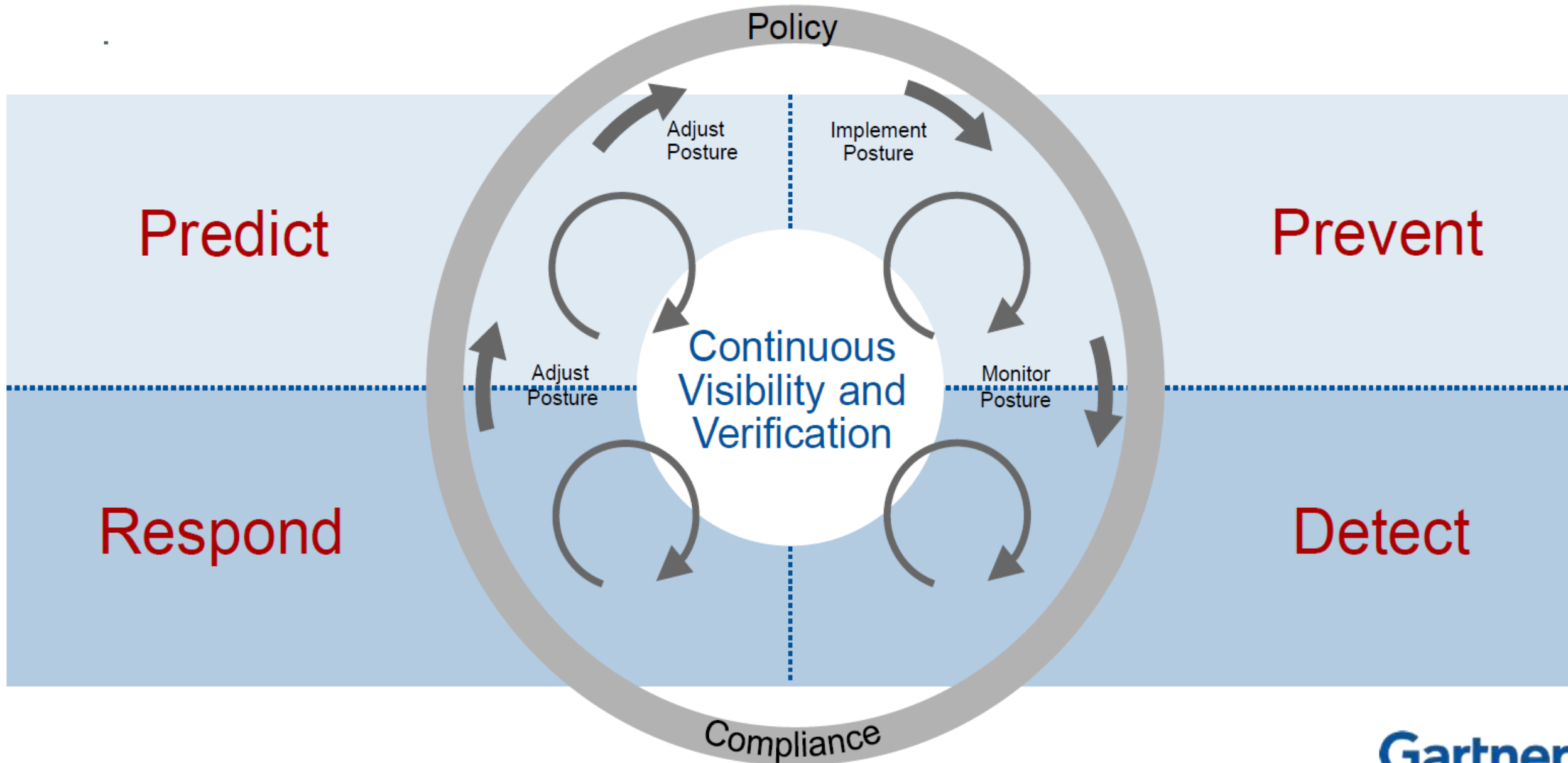
Threat **STOP**[®]

“Interesting” Times

- “EternalBlue”: NSA Exploit from “The Equation Group”.
- CVE 2017-0144
 - <https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144>
- Patched by MS on 14 March 2017 in MS17-010
 - <https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>
- Wannacry hits 12 May 2017
 - We got lucky with the kill switch.
- Petya/GoldenEye hits today, using same vector
 - Initial vector was compromised update host for Ukrainian accounting SW using PHP vuln.
 - Then spreads using EternalBlue Vulnerability
- New ShadowBrokers Dump coming over next 2 weeks
 - “Between 07/01/2017 and 07/17/2017 a “mass email” will be send to the “delivery email address” of all ‘confirmed subscribers’ ”




Adaptive Security Architecture Continues to Evolve



The Problem

Adding layers to a defense-in-depth strategy has become increasingly complex and costly



Often requires adding expensive new software and hardware that needs to be managed by skilled resources

Rarely delivers synergy with other existing security solutions

Security solutions are becoming specialized to protect against only certain threat types or vectors

Automating security usually requires sacrificing control



So What Are These Simple Things

- Vulnerability Management
 - Internal Network Segmentation
 - Central Log Management
 - Application Whitelisting
 - Identity and Access Management
 - DNS Filtering/Monitoring
 - Good Systems Administration
- Backups
 - System Hardening
 - ...

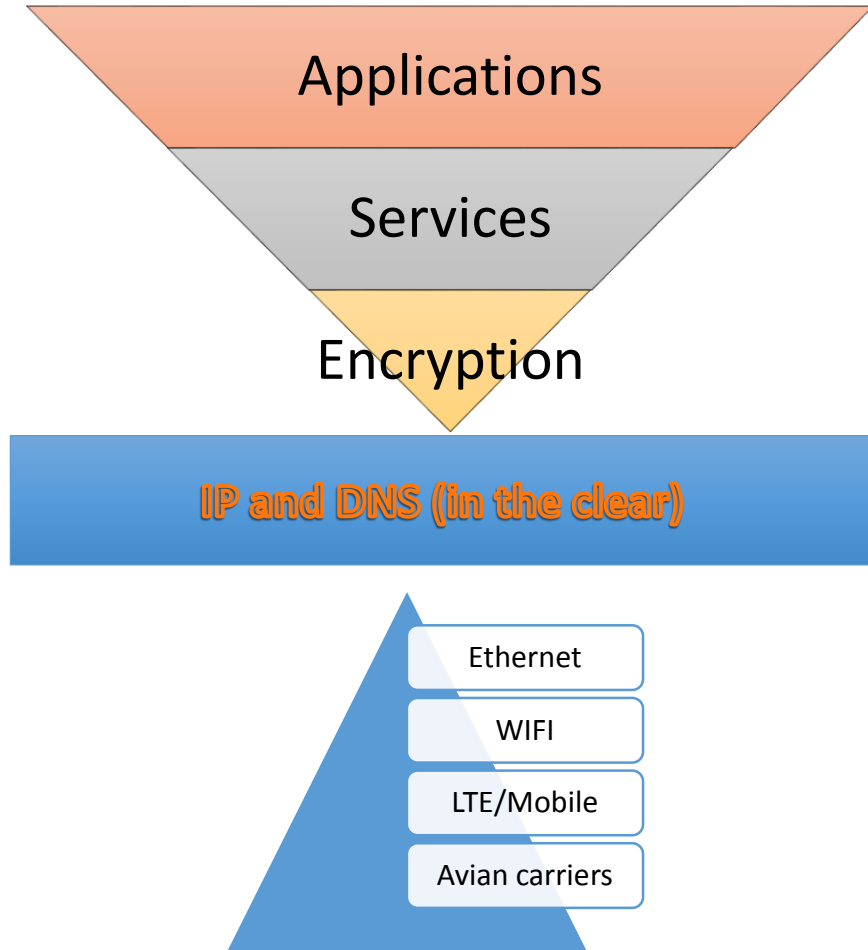


(Yes, the list is bigger than this, but notice there is no "Advanced Persistent ..." or "Machine Learning" in here)



An Opportunity

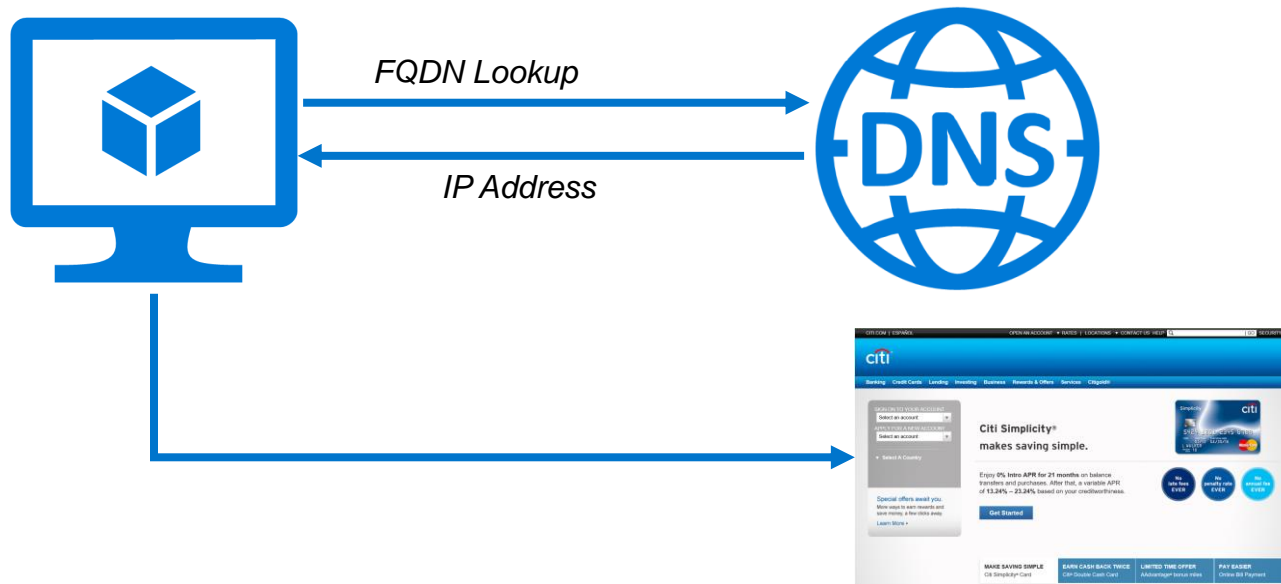
Threat **STOP**



- Everything converges at IP and DNS
- The only things that CANNOT be encrypted and still have connections complete.
- Used regardless of how the user connects, or what they are doing.
- Ubiquitous, well understood, and supported on all platforms and networks.
- The correct foundation to enforce policy throughout the network

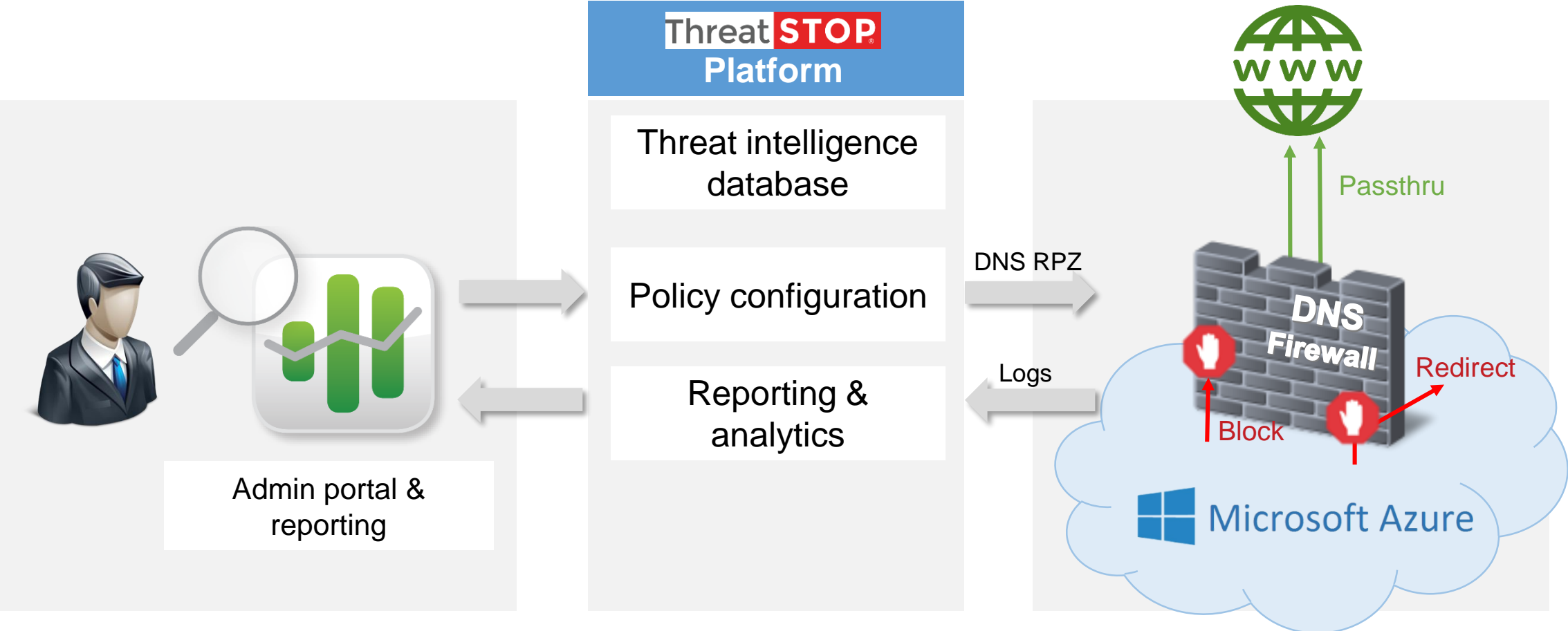


Every System Uses DNS...and Increasingly, so Does Malware **ThreatSTOP**

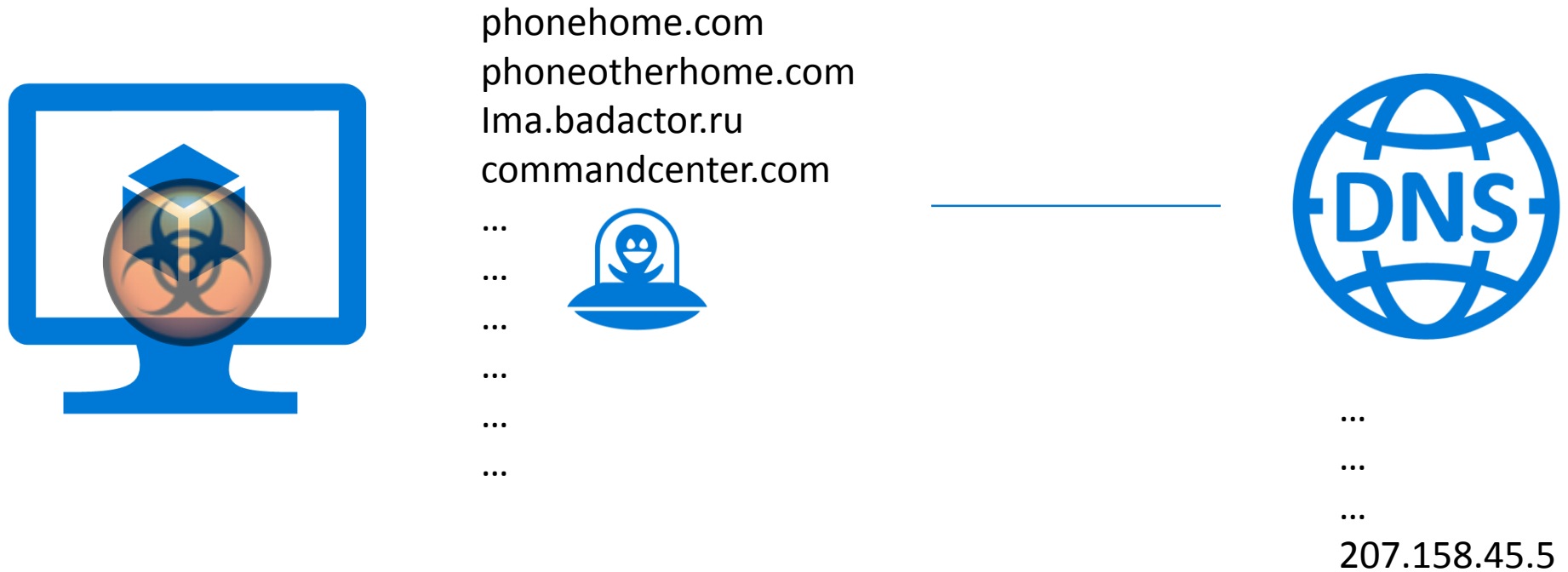


- Every device / application relies on DNS infrastructure
- Most DNS servers do little or no filtering to determine whether the domain or IP is malicious
- Cybercriminals use DNS to create more sophisticated threats and for command & control infrastructure

ThreatSTOP DNS Firewall: Solution Overview



Use Case: Compromised Host in the Network
Malware relies on DNS to establish communication channels



ThreatSTOP DNS Firewall prevents malware from communicating with its command and control infrastructure



The Three Things to Get Right to Do Threat Intelligence Well



Acquire

- Commercial
- Open Source
- End-User-Led
- Community-Driven
- Industry-Led



Aggregate

- Threat Intelligence Platforms (TIP)
- SIEM
- Existing Controls

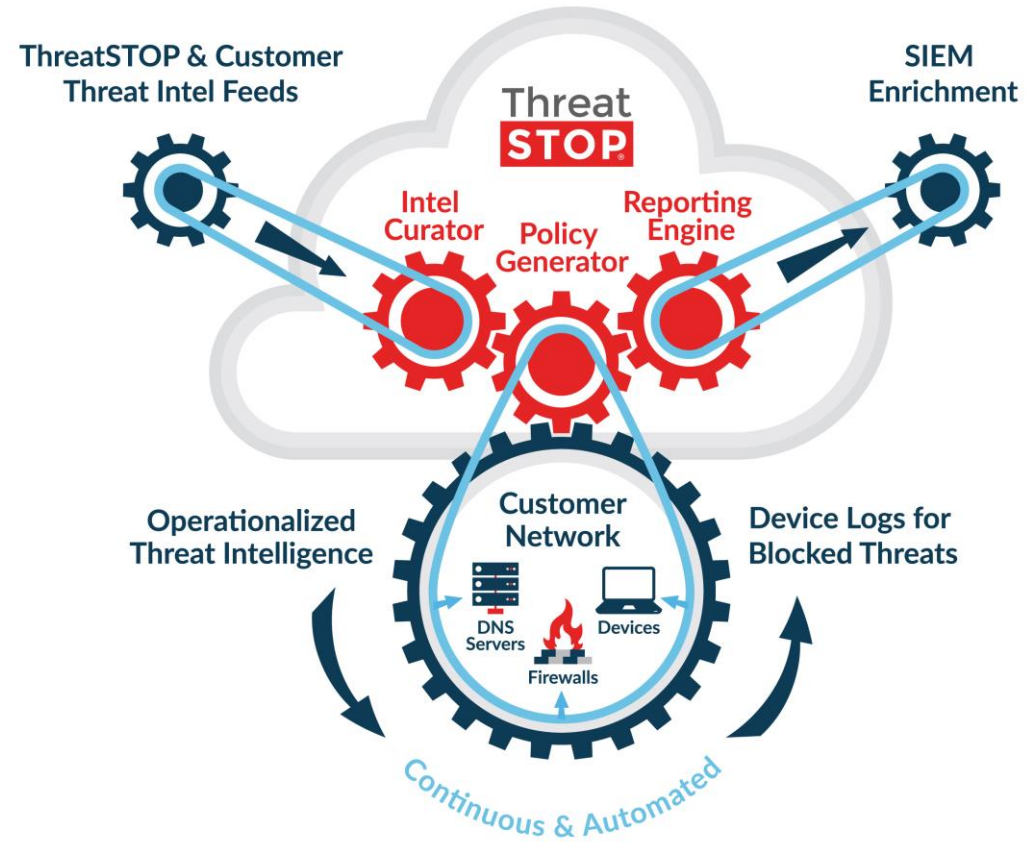


Action

- Predict
- Prevent
- Detect
- Respond



How It Works



How ThreatSTOP Delivers



DNS Firewall Service

- Compatible with BIND and Microsoft (2016) DNS Servers
- Block malicious domain requests and IP responses at the DNS-layer
- Choose to block, redirect, or pass-thru based on domain or IP

IP Firewall Service

- Compatible with Firewalls, Routers, Switches and Load Balancers
- Block malicious connections, inbound or out, at the TCP/IP-layer
- Choose to block or allow by IP

Roaming Endpoint Service

- Block or redirect malicious DNS queries in real-time
- Local DNS resolution, no VPN or 3rd party DNS servers needed
- Compatible with Windows and Mac OSX devices

Shared Functionality

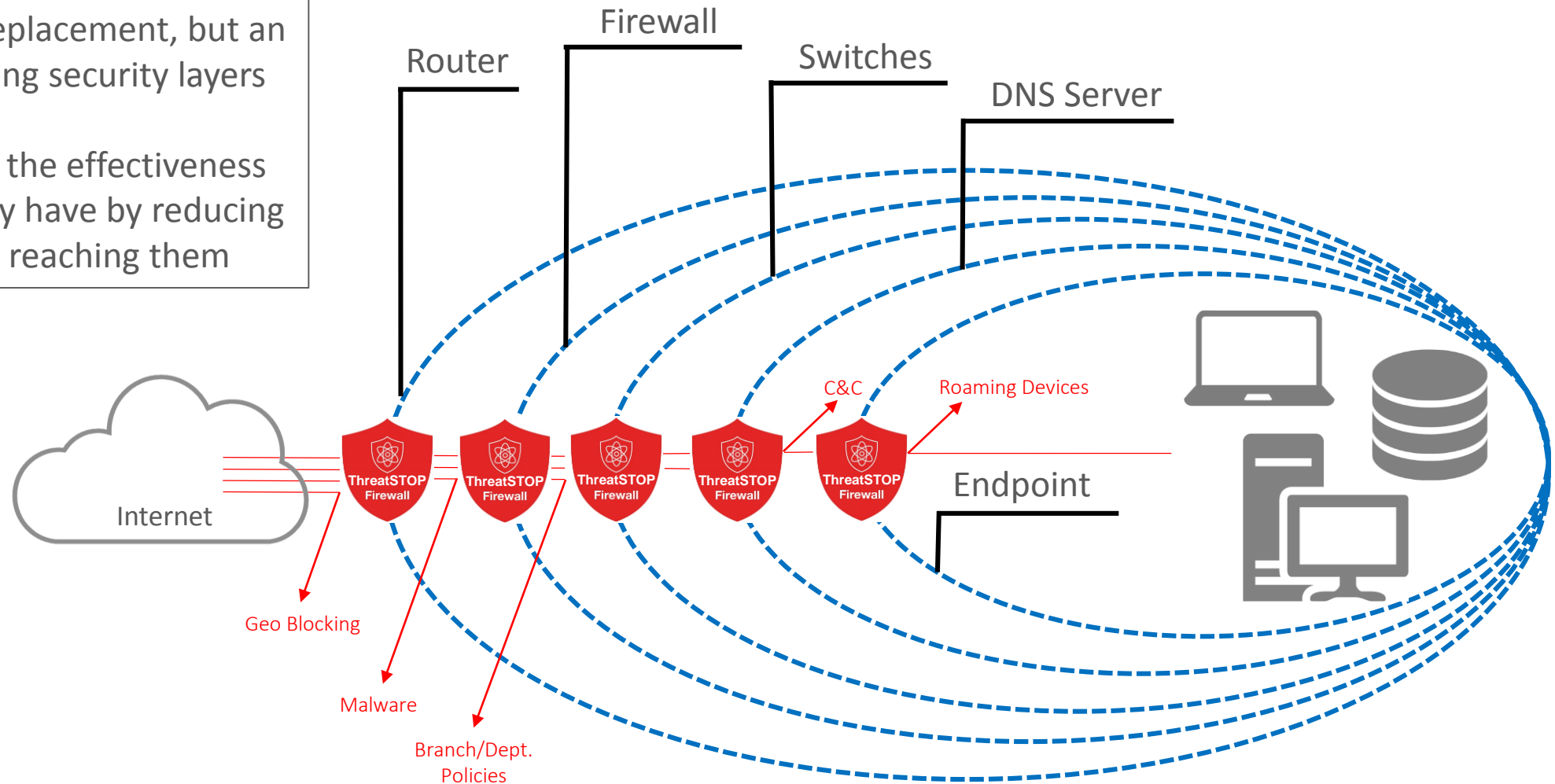
- Customize security policies by selecting from 185+ threat categories, plus your own feeds and user-defined lists. Centrally manage all policies and devices.
- Includes web-based reporting of blocked threats across all devices, *Check IoC* security research tools, and easy-to-use email alerts and notifications



Add Security Layers

ThreatSTOP is not a replacement, but an addition to your existing security layers

ThreatSTOP increases the effectiveness of security you already have by reducing the volume of threats reaching them



Easy as 1, 2, 3

ThreatSTOP[®]

1

Customize a security policy, choosing from 180+ categories including your own lists or feeds

- ✓ Ransomware
- ✓ Botnets
- ✓ Phishing
- ✓ DGA Domains
- ✓ Russia
- ✓ China

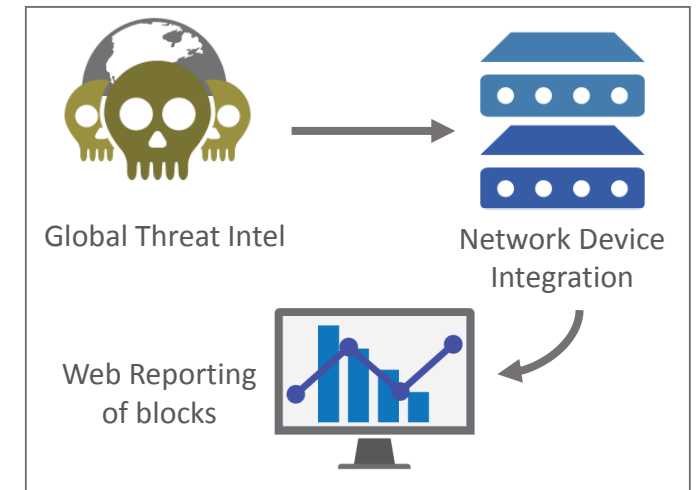
2

Run the ThreatSTOP service on your existing firewalls, routers, load balancers & DNS servers

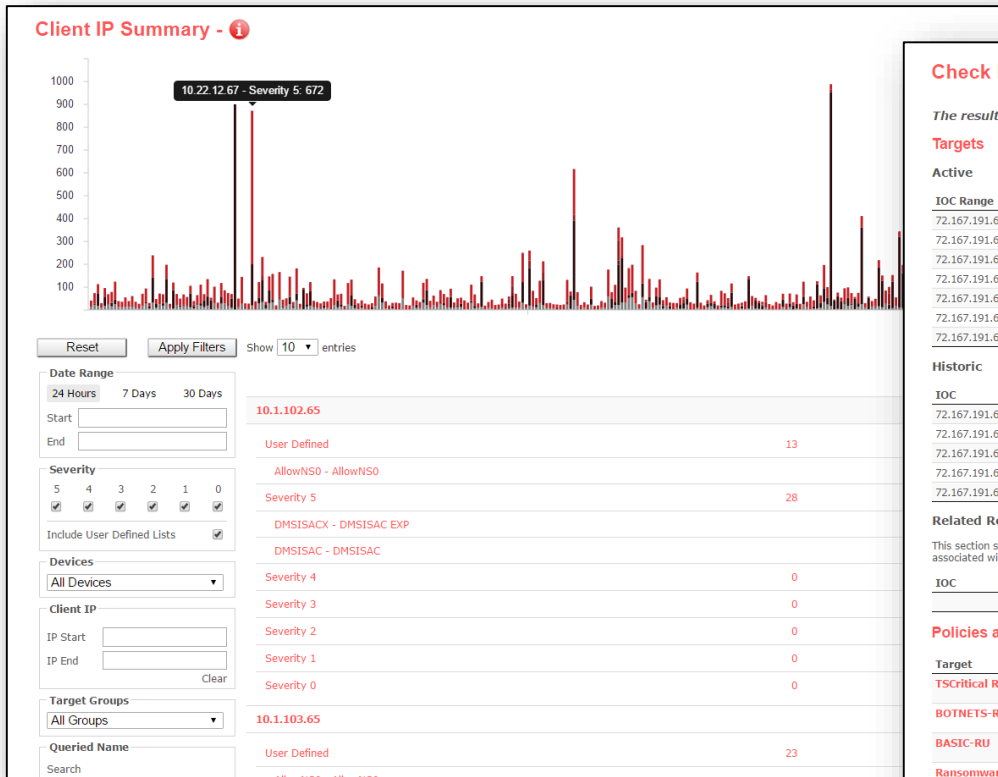


3

ThreatSTOP updates the IPs and domains in your policy automatically, using real-time threat intelligence



Complete Security Solution



Check IOC (Indicator Of Compromise) - 72.167.191.69 Copy Results to Clipboard

The resulting information cannot be reused for commercial purposes without permission.

Targets

Active

IOC Range	First Identified	Last Time Present	Present in Targets
72.167.191.69	July 07, 2016	October 06, 2016	TSCritical Ransomware IP Addresses
72.167.191.69	July 07, 2016	October 06, 2016	BOTNETS-RU
72.167.191.69	July 07, 2016	October 06, 2016	BASIC-RU
72.167.191.69	July 07, 2016	October 06, 2016	Ransomware IP addresses
72.167.191.69	July 07, 2016	October 06, 2016	TSCritical General
72.167.191.69	July 07, 2016	October 06, 2016	BOTNETS
72.167.191.69	July 07, 2016	October 06, 2016	BASIC

Historic

IOC	First Identified	Last Time Present	Present in Targets
72.167.191.69	March 22, 2016	August 02, 2016	PhishTank
72.167.191.69	February 08, 2016	March 24, 2016	DShield Top 4000
72.167.191.69	April 17, 2015	May 14, 2015	ADVANCED-RU
72.167.191.69	April 17, 2015	May 14, 2015	ADVANCED
72.167.191.69	December 13, 2014	December 30, 2014	AlienvaultScanSpam

Related Records

This section shows IP addresses (A records) resolved for the requested domain. It does not perform a complete lookup of all DNS records associated with the domain.

IOC	Relationship	Address	Last Time Present	Present in Targets
72.167.191.69 does not have any related records				

Policies and Devices

Target	Present in Policies	
TSCritical Ransomware IP Addresses	SRX-EXP	configured on device SRX-IDS
BOTNETS-RU	SRX-EXP	configured on device SRX-IDS
BASIC-RU	SRX-EXP	configured on device SRX-IDS
Ransomware IP addresses	TSBasic	
	SRX-EXP	configured on device SRX-IDS
TSCritical General	TSBasic	

ThreatSTOP

ThreatSTOP Alert - TS Alert Test

[Click here to view more details about this alert in the portal](#)

You are receiving this alert because the number of log lines matching your filter criteria has exceeded your custom threshold.

Threshold	Matched Log Lines
0	1
Filter	Value
Start Date	2016-07-10 22:58:52
End Date	2016-08-09 22:58:52
Severities	5, 4, 3, 2, 1, 0, User Defined
Direction	Inbound, Outbound
Devices	Device1, Device2
Internal IP Start	216.73.241.61
Internal IP End	216.73.241.61
Actions	Allow, Block

Web-based Reporting

Threat Research Tools

Configurable Alerts



Deploy ThreatSTOP Everywhere



Protect every square inch
of your hybrid network



Fully Integrated

Threat **STOP**[®]

Trying to replicate ThreatSTOP's end-to-end solution is expensive and difficult to manage



Affordable, Easy to Implement

Threat **STOP**[®]

Focused on preventing infections and breaches

- Not content filtering, not a web proxy, not reactive security. Blocking by IP at the first packet, and DNS at the queried name, means no tearing apart or redirecting traffic.

Not Just Another Threat Intel Feed

- Our platform operationalizes threat intelligence data by automatically piping newest malicious IPs and Domains to existing enforcement devices that control the flow of DNS and TCP/IP traffic.


No Heavy Lifting Required

- SaaS platform deploys native as an RPZ (DNSFW) and via CLI or API (IPFW) as a cloud service. No new software or hardware to manage.





The Company




 Cloud-based SaaS: protect networks using live threat intelligence to block malicious connections in real-time

 1,200+ customers ranging from SMB to F10 across all industries

 Patents on using DNS for dissemination of network security policy data – scalable and reliable

 Funded by the two original investors in Google

 Seasoned management team & deep security expertise. Chief Scientist Paul Mockapetris invented DNS

 Partnerships with leading cloud, firewall, router, DNS server, switch and load balancer vendors



概要	製品名	ThreatStop DNS Firewall
	コンセプト	脅威情報をDNSサーバへ配信(RPZ形式)
	棲み分け/強み	日本のキャリアにも採用された情報の精度の高さ
	役割	キャッシュサーバ
	提供形態	クラウドサービス
性能	権威サーバ	
	キャッシュサーバ	
コスト	課金モデル	デバイス単位年間ライセンス
	初期コスト(最小構成)	450万円 (定価)
	継続コスト	
保守・移行	サポート体制	平日9時～17時(日本語対応)
	脆弱性対応	一斉メールアナウンス
	EOLポリシー	
	マイグレーション	設定への追加



ゾーンデータ保持形式			
ローカルゾーン保持		可	
水責め対策			
毒入れ対策			
DDoS対策			
サポートするRR Type		RPZ	
IPv6トランスポート対応			
管理	インターフェイス		
	統合管理		
	ロギング		
	クエリログ検索		
DNSSEC	権威	署名更新	
		鍵更新	
		鍵更新方式	
		HSM対応	
	キヤッチ	Validation	
		TA更新	
		NTA対応	

