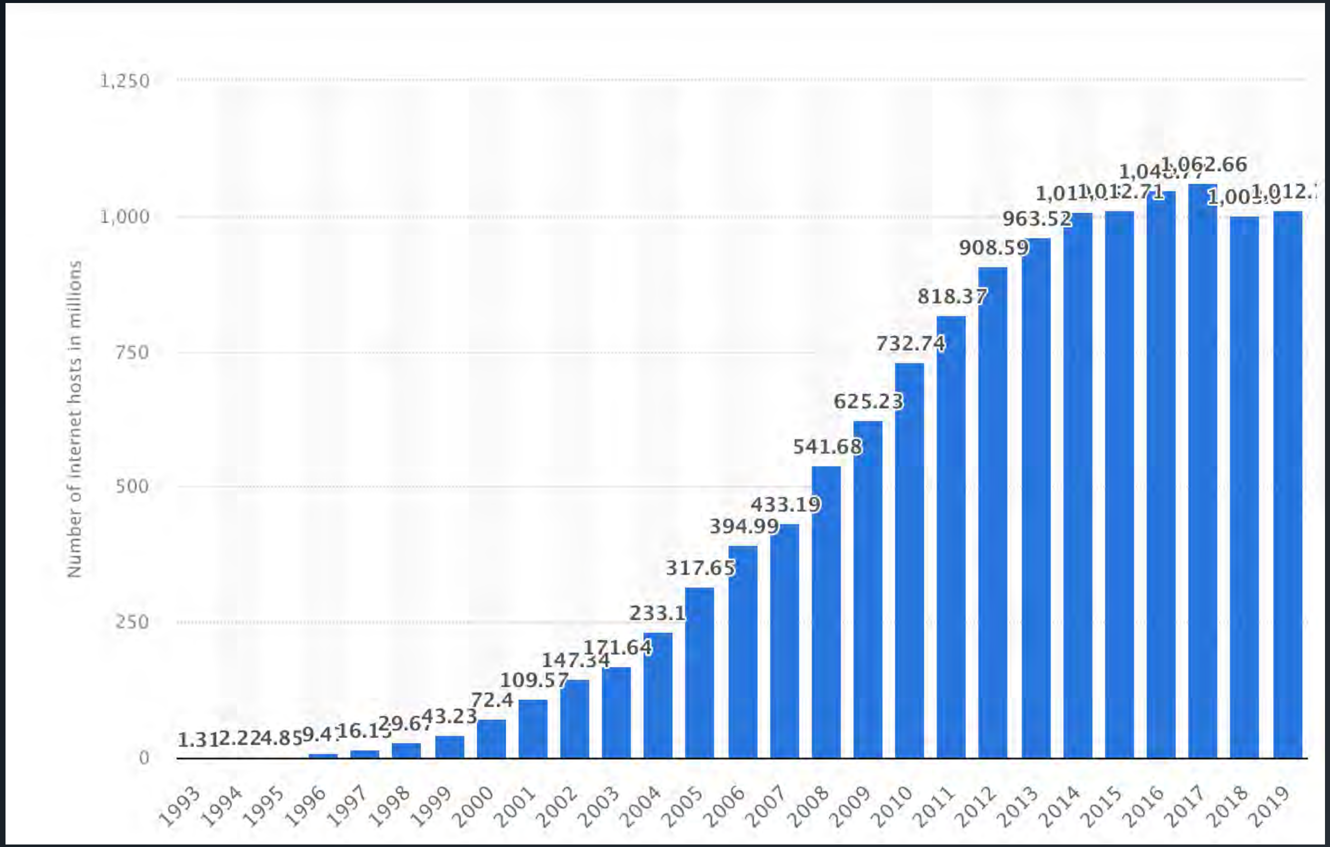
infoblox®

The Weaponization of DNS

Chad Hurt

DNS Volume



Over 1B domains inside of DNS

174 million domain names ending in .com a nd .net

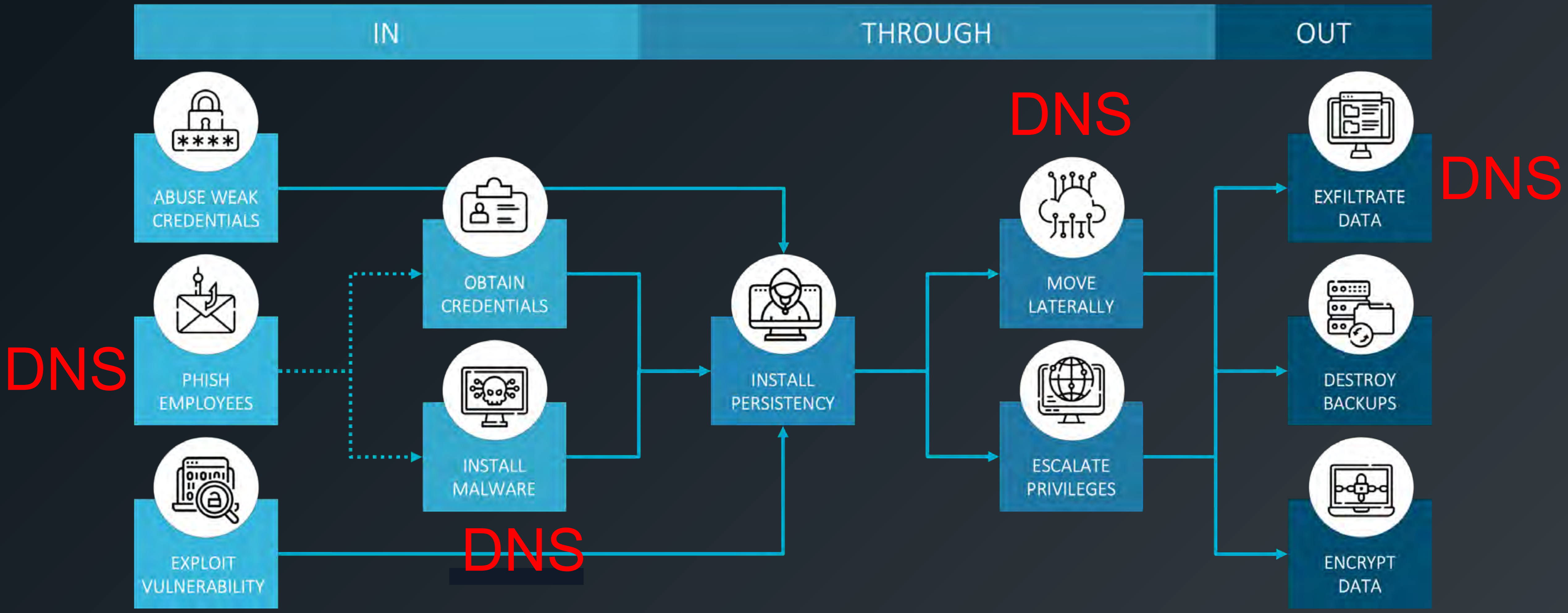
200,000 new domains created every day

Verisign processes 226 billion DNS queries per day and Google does 400 billion

The average PC does around 15,000 DNS queries per day

Let’s Encrypt issues around 600,000 digital certs per day

DNS in Cyber Attacks



IN

THROUGH

OUT

ABUSE WEAK CREDENTIALS

PHISH EMPLOYEES

DNS

EXPLOIT VULNERABILITY

OBTAIN CREDENTIALS

INSTALL MALWARE

DNS

INSTALL PERSISTENCY

DNS

MOVE LATERALLY

ESCALATE PRIVILEGES

EXFILTRATE DATA

DNS

DESTROY BACKUPS

ENCRYPT DATA

WHAT IS PROTECTIVE DNS?

Protective DNS

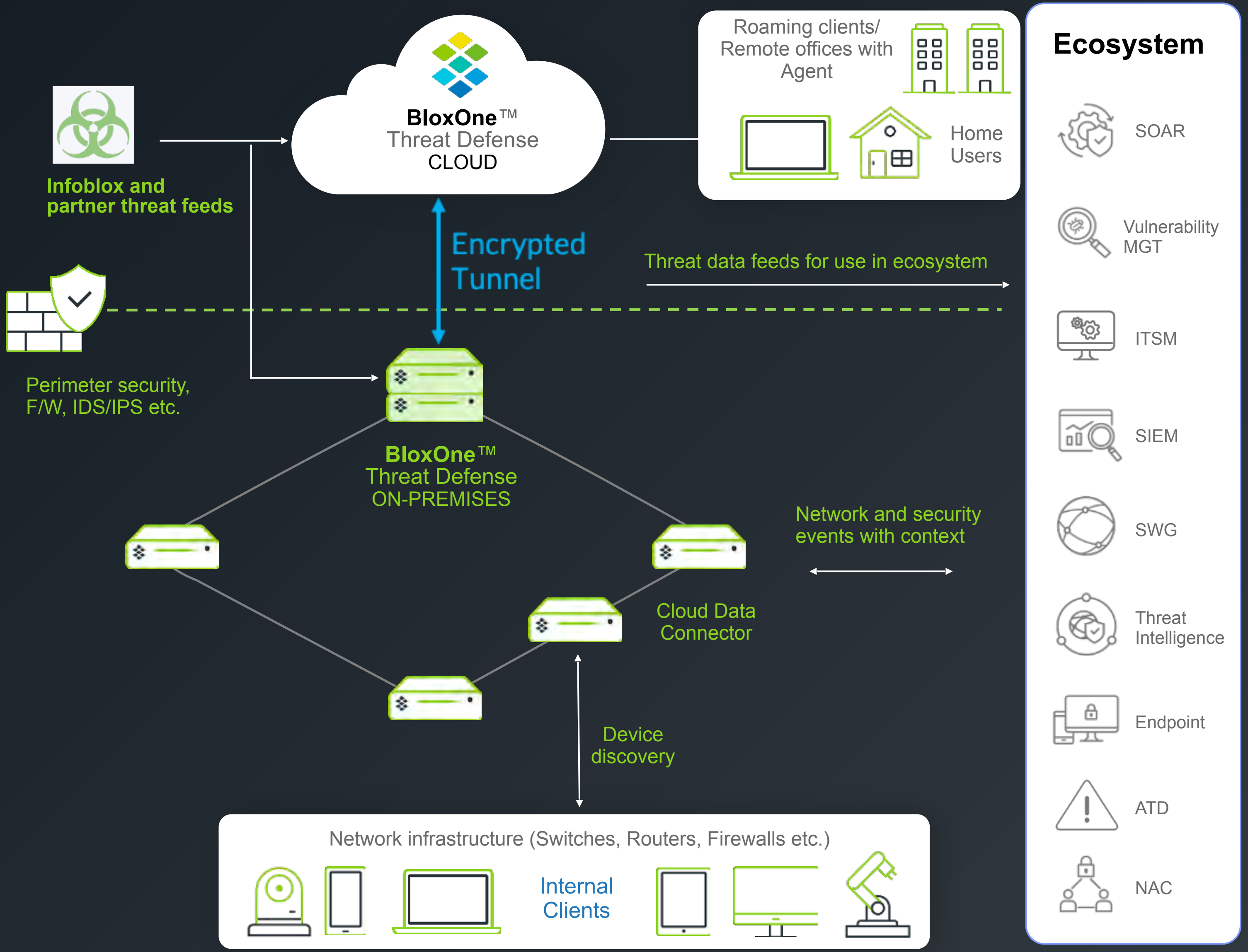
- DNS Server
- DNS Threat Intelligence
- DNS-based AI/ Machine Learning Engine
- DNS Policy Engine

EVOLVING YOUR DNS TO PROTECTIVE DNS

BloxOne®
Threat Defense

Complete, Hybrid Security

- Detect and block modern threats while closing gaps (Data exfil, DGAs)
- Optimized threat intelligence use across the ecosystem
- Improve SOC efficiency through automation and ecosystem integrations
- Realize ROI across the security stack


Infoblox and partner threat feeds
BloxOne™ Threat Defense CLOUD
Roaming clients/ Remote offices with Agent
Home Users
Encrypted Tunnel
Threat data feeds for use in ecosystem
Perimeter security, F/W, IDS/IPS etc.
BloxOne™ Threat Defense ON-PREMISES
Network and security events with context
Cloud Data Connector
Device discovery
Network infrastructure (Switches, Routers, Firewalls etc.)
Internal Clients
Ecosystem
SOAR
Vulnerability MGT
ITSM
SIEM
SWG
Threat Intelligence
Endpoint
ATD
NAC

PROTECTIVE DNS DESIGN GOALS

- IPAM data as single Source of Truth

AUTHORITATIVE IP ADDRESS MANAGEMENT (IPAM)

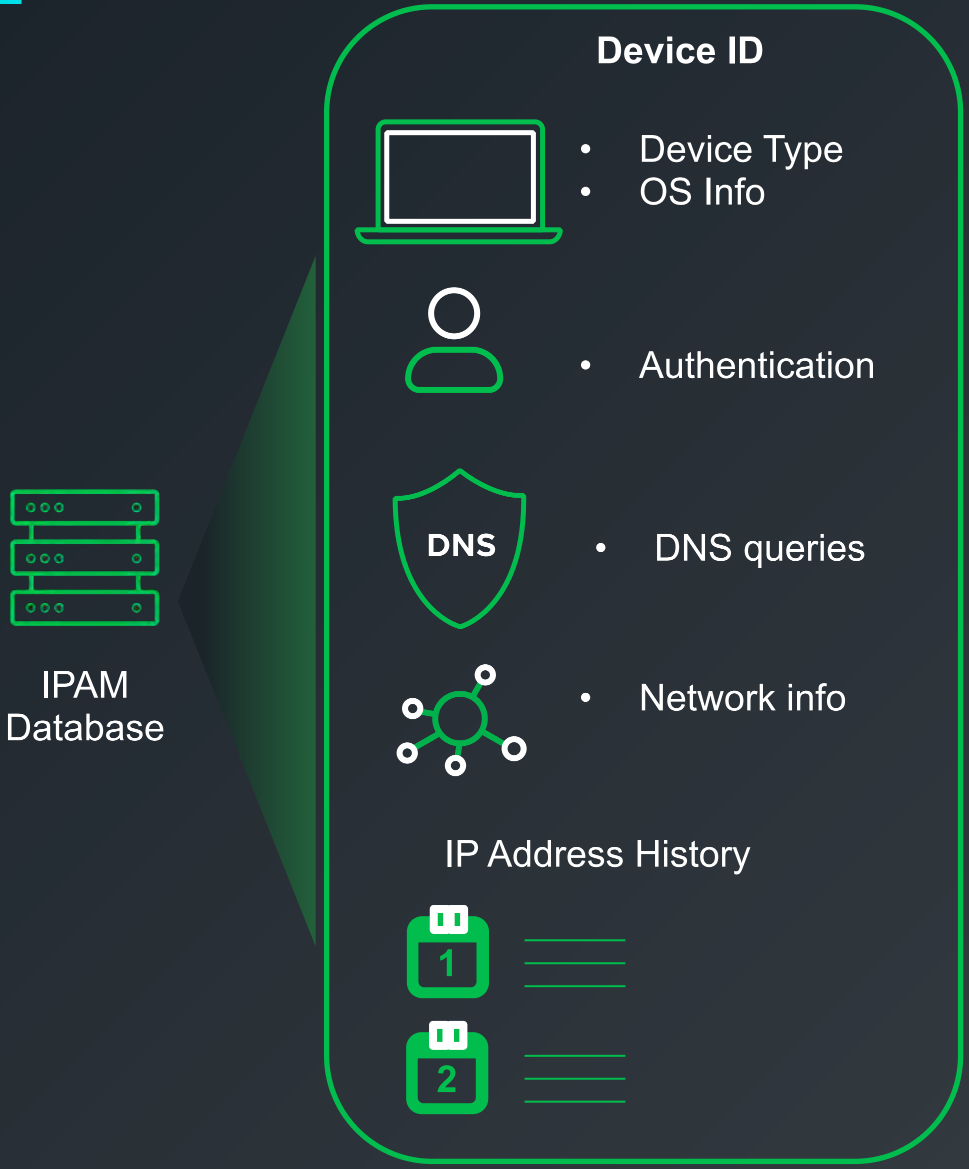
SINGLE SOURCE OF TRUTH

“Living” database of **everything** on your network

Leverage **DHCP** and discovery to inventory all devices that get an IP address.

Instantly track changes as IP addresses change/expire/renew.

Leverage IPAM for Incident response/investigations.



IPAM Database

Device ID

- Device Type
- OS Info

- Authentication

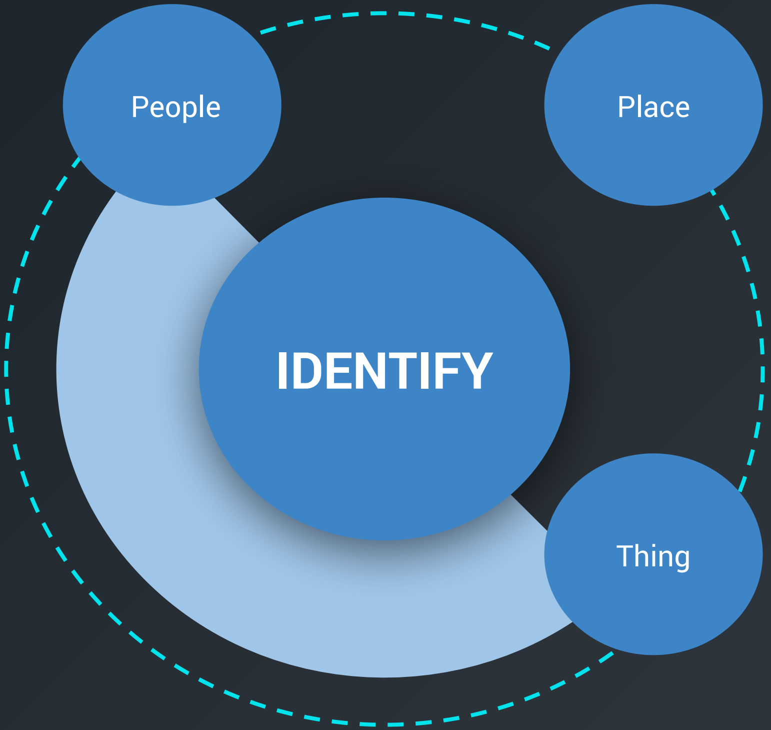
- DNS queries

- Network info

IP Address History

WHY AUTHORITATIVE IPAM

MATTERS TO A SOC



Asset

When did this happen?	Date stamp
Who is operating this asset?	Username
What type of asset is this?	OS Type, DHCP Fingerprint
What asset is this?	IP Address, Hostname, MAC address

Alert

What was the alert from?	Query, Response, IOC
What is the nature of the threat?	Domain Category, Threat Class, Property
How do I pivot ?	Links to other investigative tools

PROTECTIVE DNS DESIGN GOALS

- IPAM data as single Source of Truth
- Leverage Threat Intel across the enterprise

INFOBLOX INTELLIGENCE IS DESIGNED FOR DNS

We Detect, Track, and Block Persistent Threats via DNS

- **“Suspicious Domains”:** We know they are bad, we just don’t know how yet
- They share common “DNA” with other known threats
  - Uses a DNS server with poor reputation
  - Uses a registrar with poor reputation
  - Common network, common IP addresses, Common owners
- **“Suspicious Lookalikes”** can be identified and blocked, even before they resolve to a host

PROTECTIVE DNS DESIGN GOALS

- IPAM data as single Source of Truth
- Leverage Threat Intel across the enterprise
- Lookalike domain detection and brand protection
  - Custom domain lookalike detector
  - Top 100 common domains automatic detection
  - CISA-recommended takedown and remediation service

WHAT ARE LOOKALIKE DOMAINS?

- **Traditional** - Using prefixes and suffixes to alter the existing domain. Example: **infoblox-benefits.com**

- **Homographs / Homoglyphs** - Using similar looking characters to fool the eye. Example: **g00gle.com**

- **Typosquats** - Using replacement characters close on the keyboard. Example: **facebooj.com**

PROTECTIVE DNS DESIGN GOALS (con't)

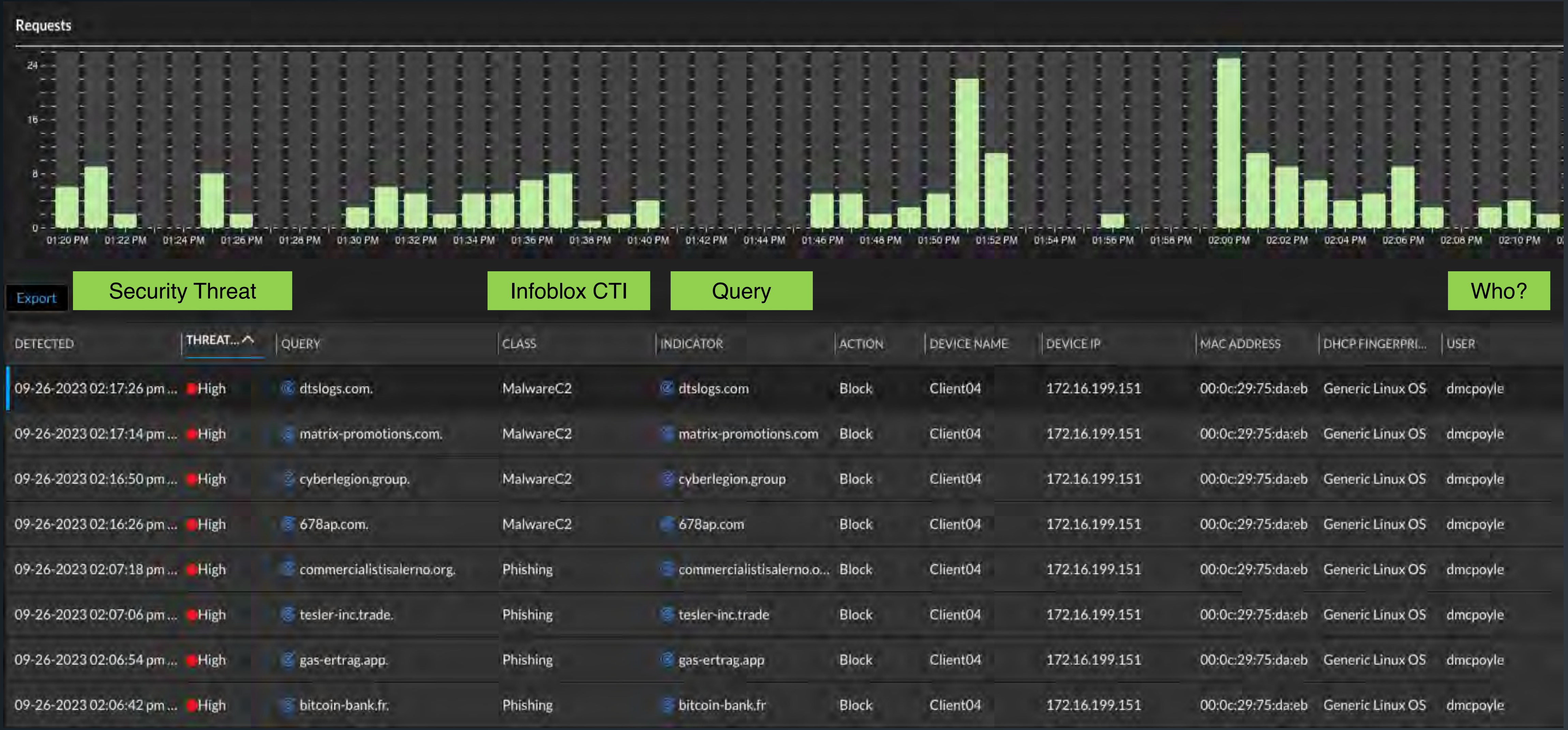
- Block malicious DNS responses using DNS infrastructure, not point solutions
  - Foundational and built into the underlying infrastructure
  - Used by all devices, from corporate users, to servers and IOT

- Monitor 100% of DNS traffic - Exclusive query path for all queries
  - Block 3rd party DNS, including DoT and DoH

- Improve telemetry across security stack
  - Query logging to SIEM/SOAR
  - User and device attribution data for secops in real-time

- Leverage security ecosystem integrations with your existing toolset

IPAM + USER + SECURITY POSTURE IN CLOUD PORTAL



Security Threat

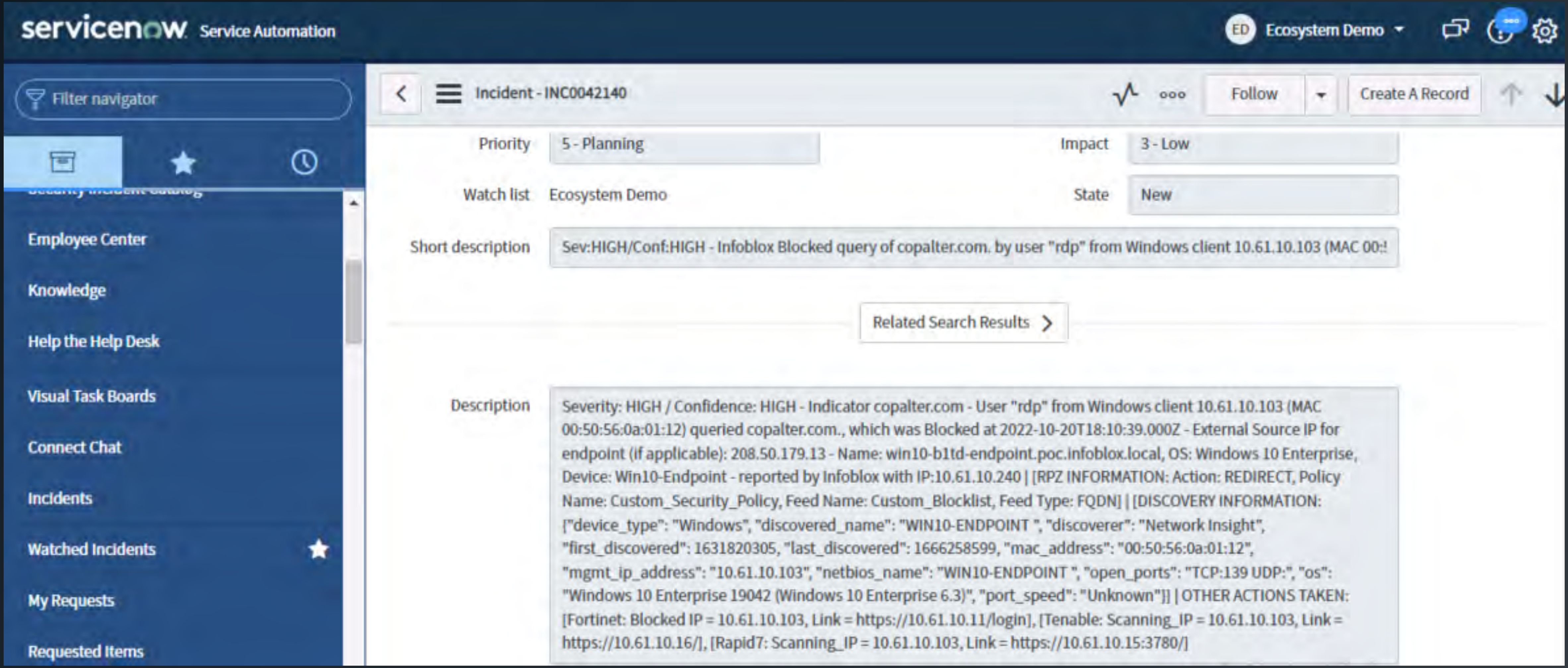
Infoblox CTI

Query

Who?

DETECTED	THREAT...	QUERY	CLASS	INDICATOR	ACTION	DEVICE NAME	DEVICE IP	MAC ADDRESS	DHCP FINGERPRI...	USER
09-26-2023 02:17:26 pm ...	High	dtslogs.com.	MalwareC2	dtslogs.com	Block	Client04	172.16.199.151	00:0c:29:75:da:eb	Generic Linux OS	dmcpoyle
09-26-2023 02:17:14 pm ...	High	matrix-promotions.com.	MalwareC2	matrix-promotions.com	Block	Client04	172.16.199.151	00:0c:29:75:da:eb	Generic Linux OS	dmcpoyle
09-26-2023 02:16:50 pm ...	High	cyberlegion.group.	MalwareC2	cyberlegion.group	Block	Client04	172.16.199.151	00:0c:29:75:da:eb	Generic Linux OS	dmcpoyle
09-26-2023 02:16:26 pm ...	High	678ap.com.	MalwareC2	678ap.com	Block	Client04	172.16.199.151	00:0c:29:75:da:eb	Generic Linux OS	dmcpoyle
09-26-2023 02:07:18 pm ...	High	commercialistisalerno.org.	Phishing	commercialistisalerno.o...	Block	Client04	172.16.199.151	00:0c:29:75:da:eb	Generic Linux OS	dmcpoyle
09-26-2023 02:07:06 pm ...	High	tesler-inc.trade.	Phishing	tesler-inc.trade	Block	Client04	172.16.199.151	00:0c:29:75:da:eb	Generic Linux OS	dmcpoyle
09-26-2023 02:06:54 pm ...	High	gas-ertrag.app.	Phishing	gas-ertrag.app	Block	Client04	172.16.199.151	00:0c:29:75:da:eb	Generic Linux OS	dmcpoyle
09-26-2023 02:06:42 pm ...	High	bitcoin-bank.fr.	Phishing	bitcoin-bank.fr	Block	Client04	172.16.199.151	00:0c:29:75:da:eb	Generic Linux OS	dmcpoyle

WHAT CAN YOU DO WITH MORE IPAM DATA



Priority	5 - Planning	Impact	3 - Low
Watch list	Ecosystem Demo	State	New

Short description: Sev:HIGH/Conf:HIGH - Infoblox Blocked query of copalter.com. by user "rdp" from Windows client 10.61.10.103 (MAC 00:

Description: Severity: HIGH / Confidence: HIGH - Indicator copalter.com - User "rdp" from Windows client 10.61.10.103 (MAC 00:50:56:0a:01:12) queried copalter.com., which was Blocked at 2022-10-20T18:10:39.000Z - External Source IP for endpoint (if applicable): 208.50.179.13 - Name: win10-b1td-endpoint.poc.infoblox.local, OS: Windows 10 Enterprise, Device: Win10-Endpoint - reported by Infoblox with IP:10.61.10.240 | [RPZ INFORMATION: Action: REDIRECT, Policy Name: Custom_Security_Policy, Feed Name: Custom_Blocklist, Feed Type: FQDN] | [DISCOVERY INFORMATION: [{"device_type": "Windows", "discovered_name": "WIN10-ENDPOINT ", "discoverer": "Network Insight", "first_discovered": 1631820305, "last_discovered": 1666258599, "mac_address": "00:50:56:0a:01:12", "mgmt_ip_address": "10.61.10.103", "netbios_name": "WIN10-ENDPOINT ", "open_ports": "TCP:139 UDP:", "os": "Windows 10 Enterprise 19042 (Windows 10 Enterprise 6.3)", "port_speed": "Unknown"}] | OTHER ACTIONS TAKEN: [Fortinet: Blocked IP = 10.61.10.103, Link = https://10.61.10.11/login], [Tenable: Scanning_IP = 10.61.10.103, Link = https://10.61.10.16/], [Rapid7: Scanning_IP = 10.61.10.103, Link = https://10.61.10.15:3780/]

ありがとう

köszönjük

Cảm ơn

धन्यवाद

terima kasih

gracias

고마워요

teşekkür ederim

Σας ευχαριστώ

obrigado

grazie

THANK YOU!

merci

谢谢

takk

شكرا

ขอบคุณ

tack

danke

bedankt

kiitos