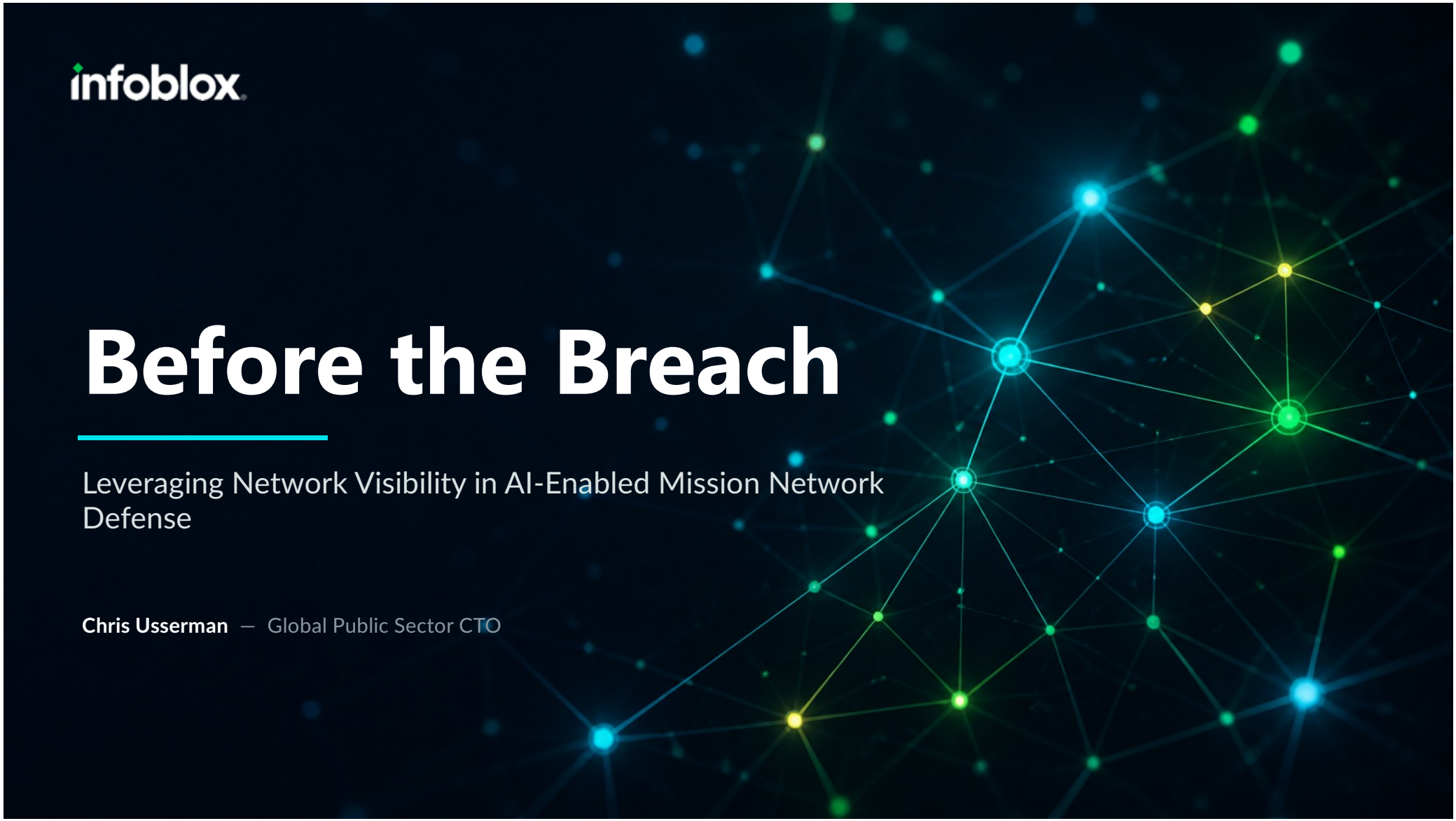
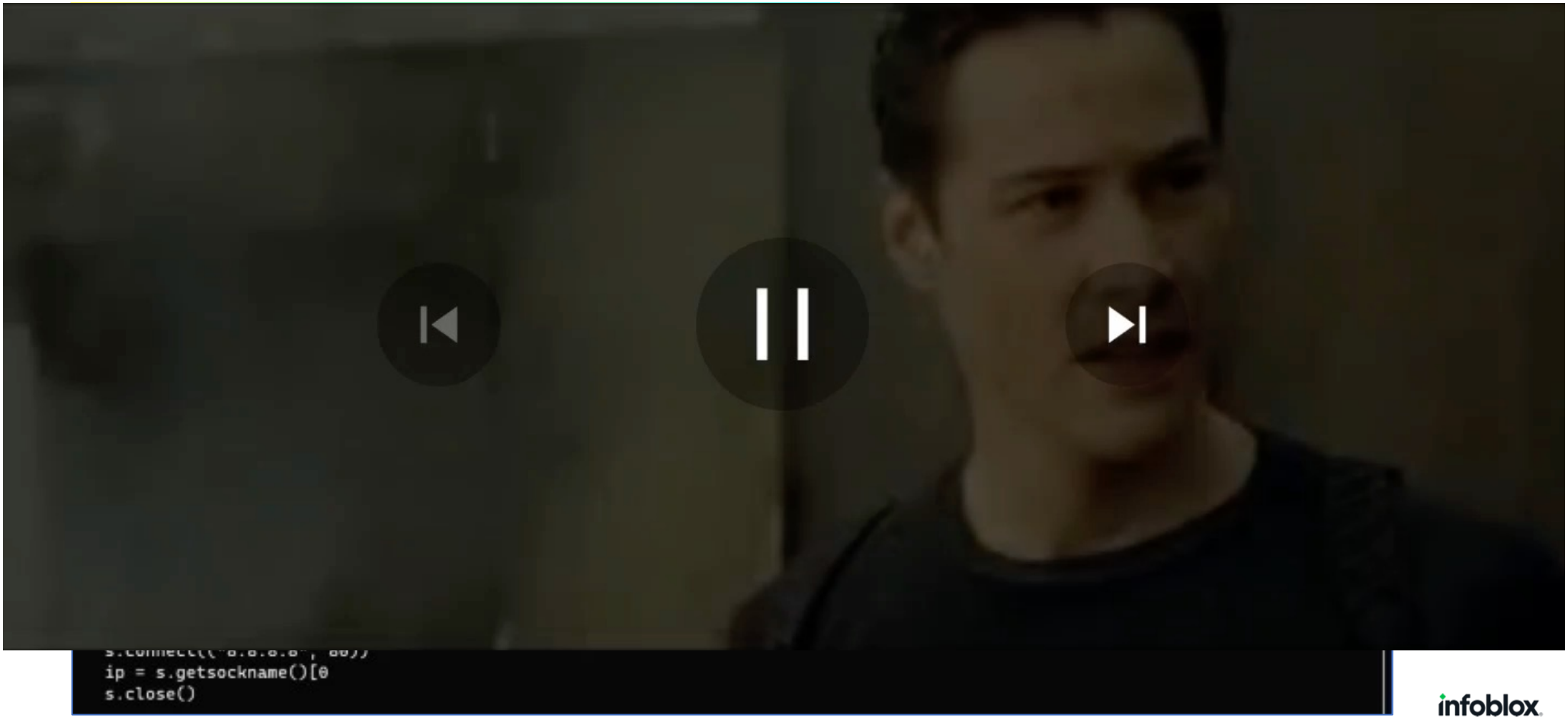
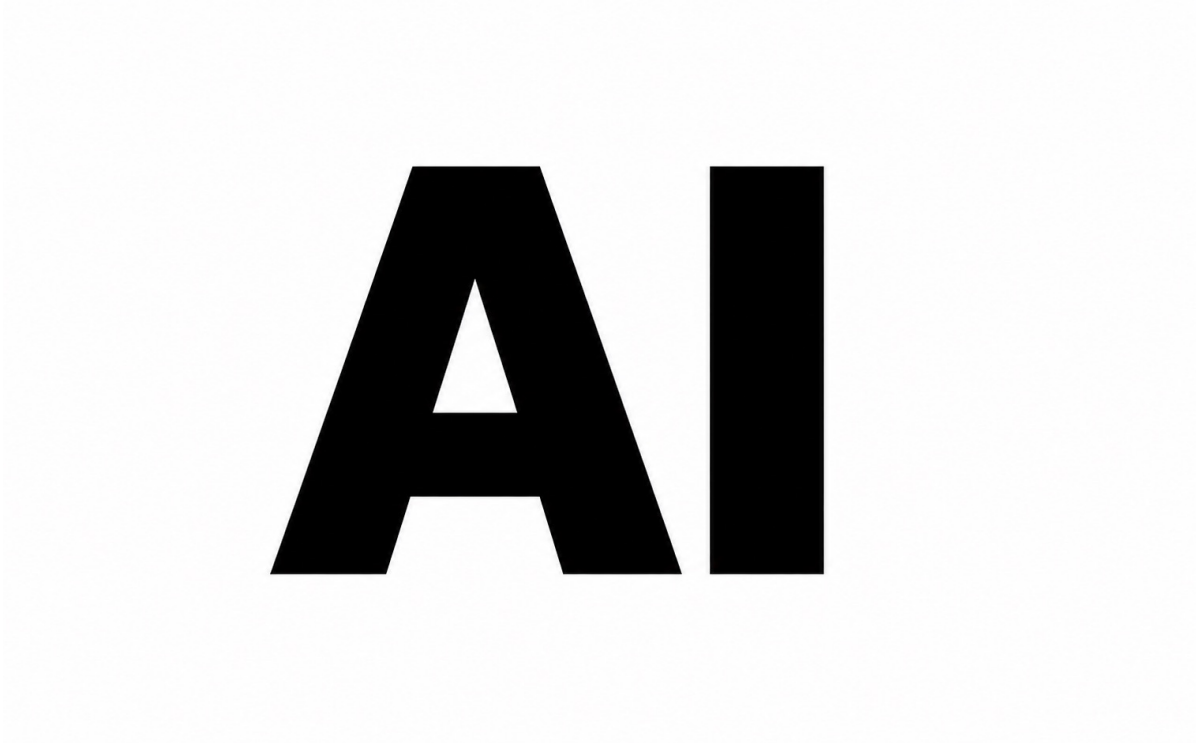

infoblox
Before the Breach
Leveraging Network Visibility in AI-Enabled Mission Network Defense
Chris Usserman — Global Public Sector CTO

Science Follows Sci-Fi

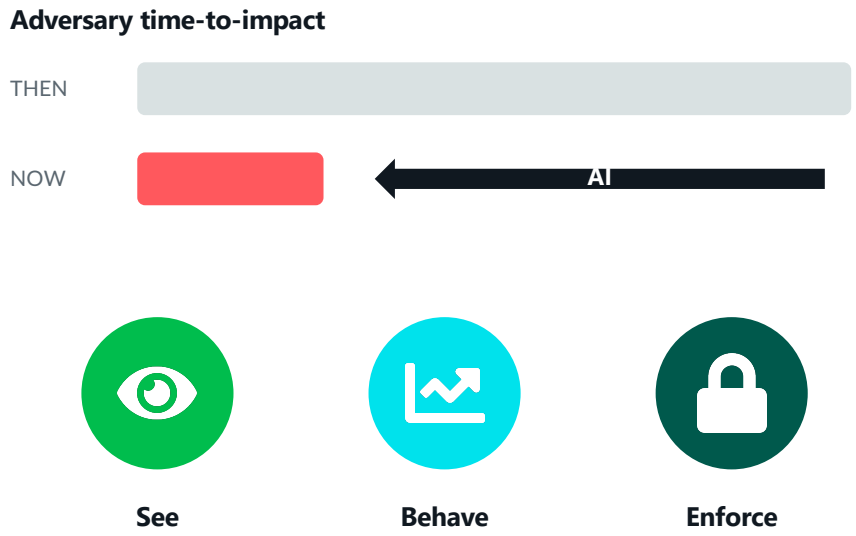


infoblox.


AI

BLUF: seeing risk earlier at the network layer scales with AI-era speed

- AI collapsed the time between an adversary showing up and doing damage.
- The advantage that scales with that speed is seeing risk earlier — at the network layer.
- Know what's connected, watch how it behaves, enforce where it's allowed to go.
- No new sensor, no new agent — the signal already exists. What most networks lack is a layer built to see it, decide, and enforce — the gap Zero Trust and C2C exist to close.



WHERE WE'RE GOING

1 WHY	**2 PROOF**	**3 CAPABILITY**	**4 MANDATES**	**5 SO WHAT**
the problem changed	three real cases	four things that repeat the save	Zero Trust · C2C · MPE	See → Decide → Assure

infoblox.

Where do most breach investigations start?

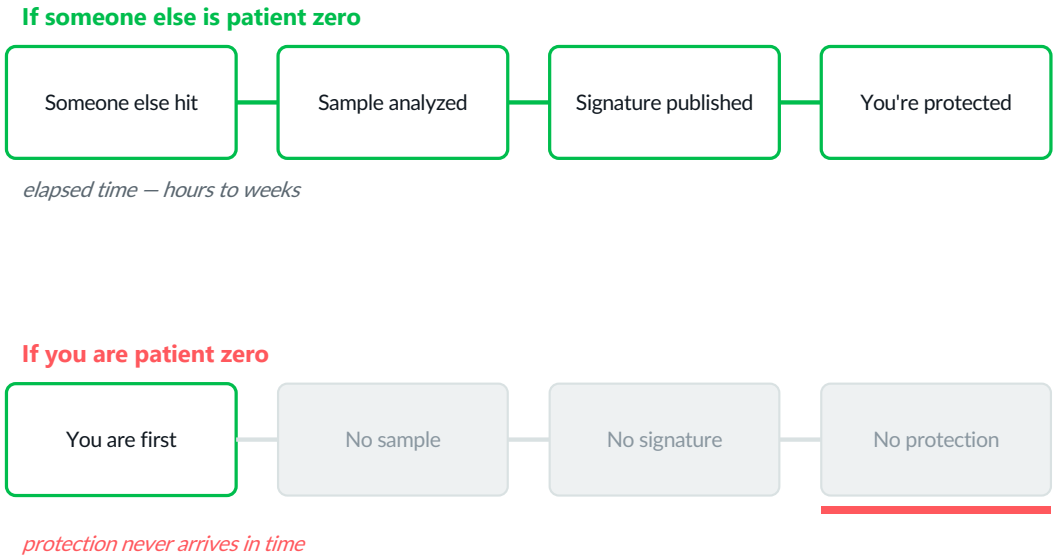


infoblox.

"Detect and respond" quietly assumes someone else was patient zero

THE ECONOMICS FLIPPED	One-time-use domains	Registered DGAs expiring inside 24 hours	Tailored phishing across tens of thousands of ephemeral hostnames

- Signature and reputation models depend on somebody being hit first.
- AI-crafted, single-use attacks make your mission network patient zero.
- Waiting for a known-bad verdict is waiting too long.
- Every hour of dwell time = more exfiltration, lateral movement, mission impact.



infoblox.

You can't defend what you can't see — and mission networks multiply the blind spots

79%

of organizations admit a substantial asset-visibility gap

3x

more incidents correlated with that gap

60–70%

is all scan-based discovery typically finds

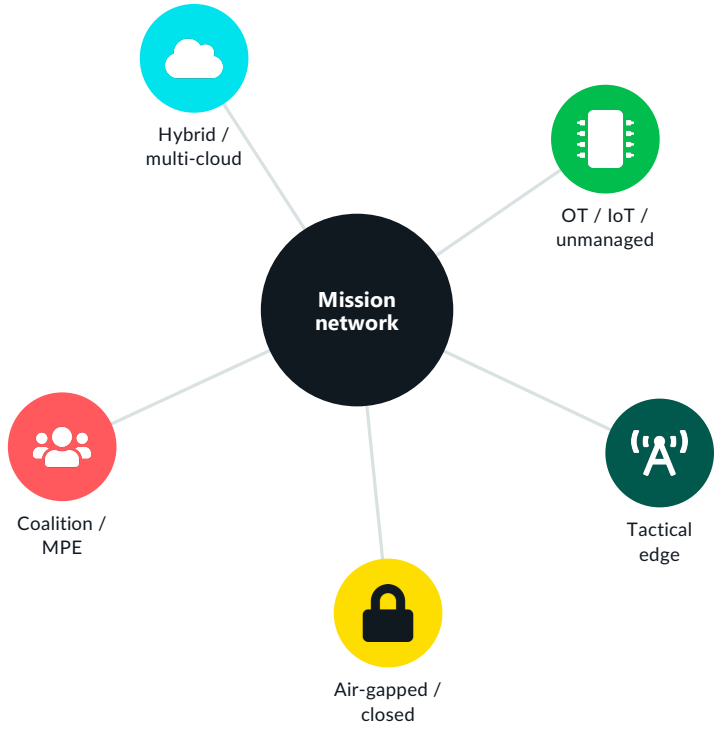
What you think you see

known & managed	UNKNOWN

what's actually connected

If the inventory is 60–70% right, every downstream control inherits that error — including Comply to Connect.

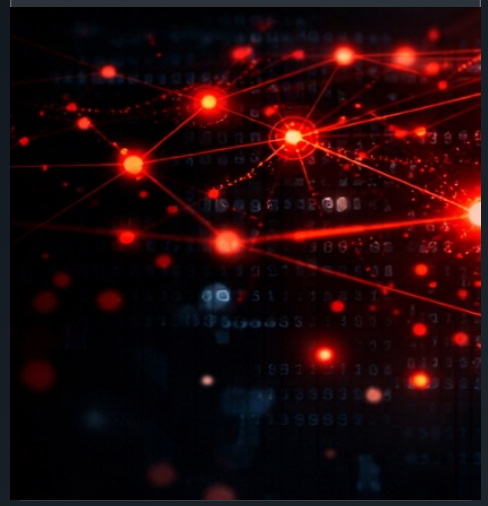
Every environment with no agent to install



infoblox.

DNS REVEALS A CONNECTED INFRASTRUCTURE

Phishing/Smishing/ Quishing



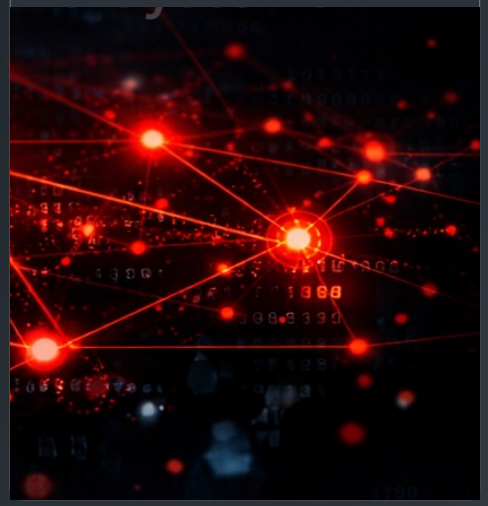
Command and Control



Data Exfiltration



Prompt Injection



Public

Nearly every attack stage generates a DNS query

92%

of malware attacks reducible from a C2 perspective with Protective DNS (NSA)

4B+

DNS queries analyzed in the DoD Protective DNS pilot — blocking millions of malicious connections



Phishing click · C2 callback · malware retrieval · data exfiltration — each one resolves a name first. DNS is the first observable step and the last one an adversary can avoid.

Tracking adversary infrastructure is watching the clouds roll in—not waiting until it rains. The infrastructure exists before the attack does.

infoblox.

Three real cases. One lesson.

- All three publicly documented. None of them requires you to take my word for it.
- I'll walk each one onto a mission network: the tradecraft as reported, then what it would look like on yours.



Case A

Decoy Dog

2022–2023 · found solely in DNS

Proof the method works — confirmed independently by a competitor's own telemetry.



Case B

Screening Serpens

2026 · endpoint-evasion tradecraft

Proof it's still the game today — engineered specifically to beat the endpoint.



Case C

Residential proxies

2026 · already inside gov networks

Proof it's already measurable in government networks — with no phishing and no malware.

one lesson

infoblox.

Decoy Dog was found in DNS, and only in DNS — nothing else saw it

- Nation-state DNS command-and-control toolkit — an advanced variant of the Pupy RAT.
- The first C2 malware ever discovered and characterized solely from DNS.
- Operating since at least April 2022 — undetected by the industry for over a year.
- Found by anomaly detection, not by reverse-engineering a sample.

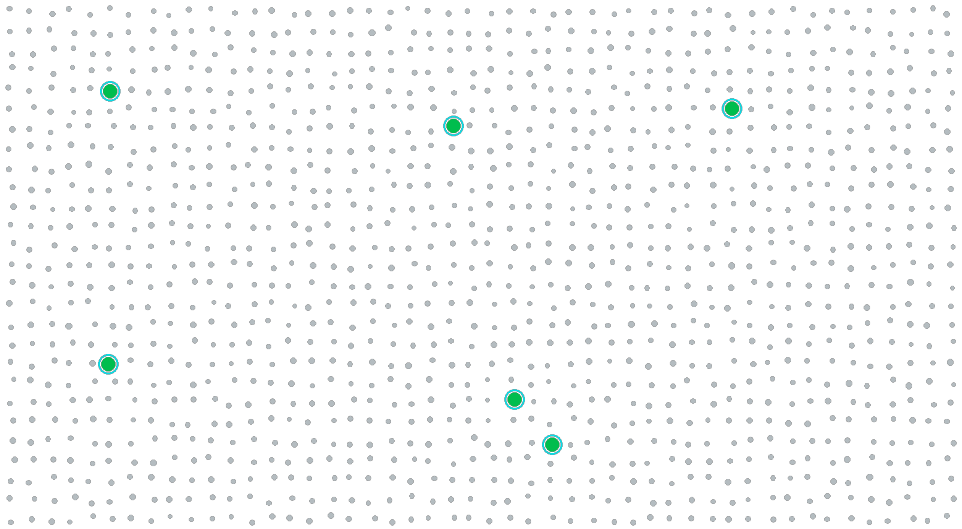
WHY NOTHING ELSE SAW IT

Fileless Pupy runs in memory with slow encrypted C2 and long persistence

Wrong vantage point the beaconing queries came from network appliances — firewalls, not user laptops

No agent to run devices that frequently have no endpoint agent in the first place

This exploits an inherent weakness of the malware-centric intelligence ecosystem that dominates the industry.

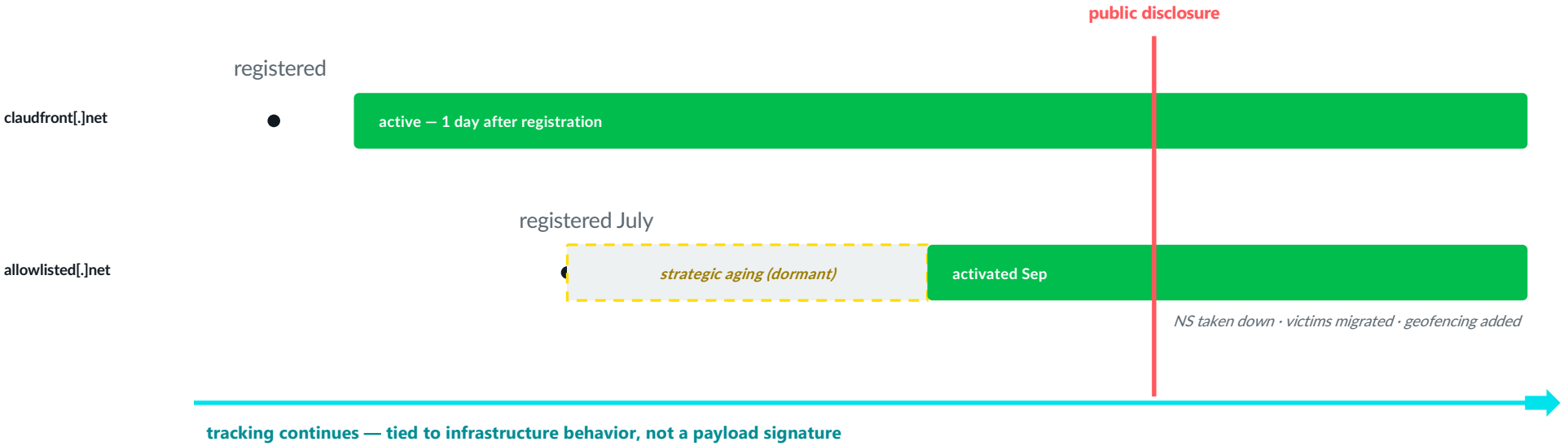


18 of 370 million domains matched the signature

~70B	1+ yr	Apr 2022
DNS queries analyzed daily	some victims talked to a controller	operating since at least

infoblox.

The controllers were staged and aged deliberately — and tracking held



Strategic aging defeats "newly registered domain" heuristics.

Adversary adapted after disclosure: response behavior changed.

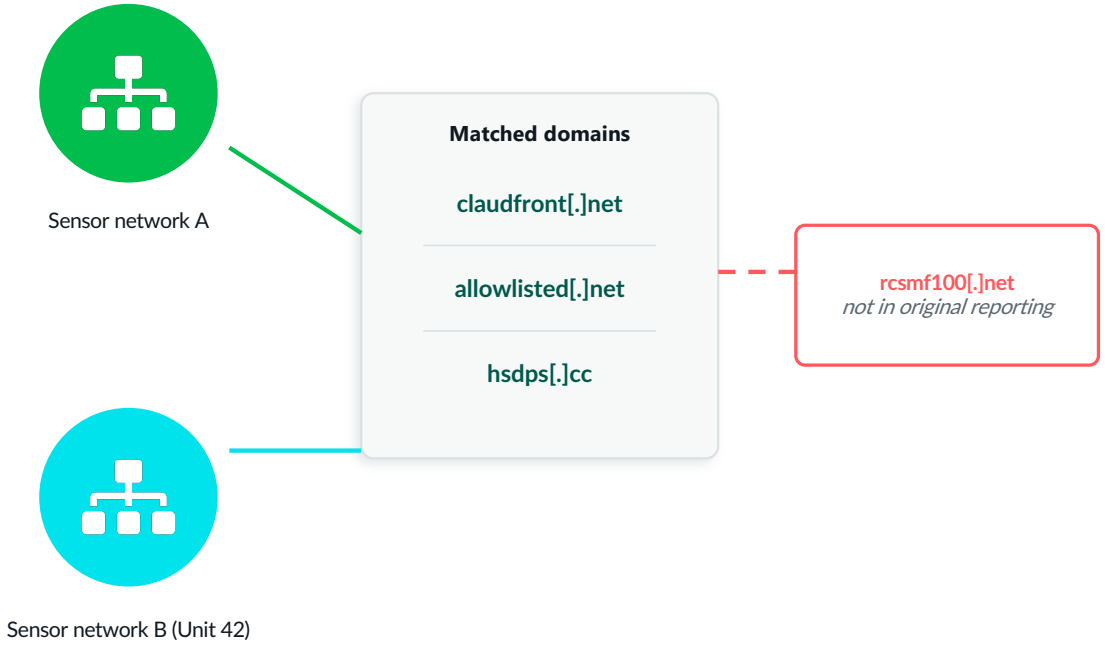
Tracking held infrastructure-centric visibility does not break.

infoblox.

A competitor independently reproduced the finding from its own telemetry

- October 2023: Unit 42 published its own in-the-wild DNS tunneling study.
- Built on four years of its own detection data plus third-party passive DNS.
- Detected tunneling on the same reported domains — confirming the shared Pupy encoding.
- Then went further: flagged a new domain by pivoting on a shared name server IP.

Two vendors. Two separate sensor networks. Same conclusion — and the pivot was a name server, not a malware sample.



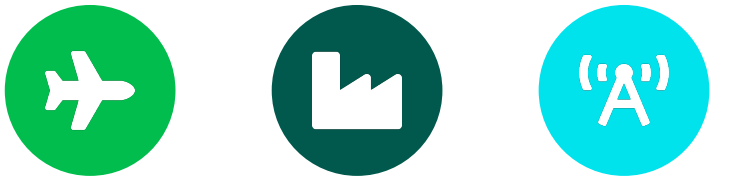
infoblox.

The fair objection: that was 2023. Here is 2026.

Reasonable question: does a 2022–2023 case still describe the threat you face now?

Screening Serpens — and its target set is this room

- Iran-nexus APT active since at least 2022; also tracked as UNC1549, Smoke Sandstorm, and "Iranian Dream Job."
- Unit 42 observed campaigns through March–April 2026 against entities in the U.S., Israel, and the UAE.
- Heavily targeting aerospace, defense manufacturing, and telecommunications.

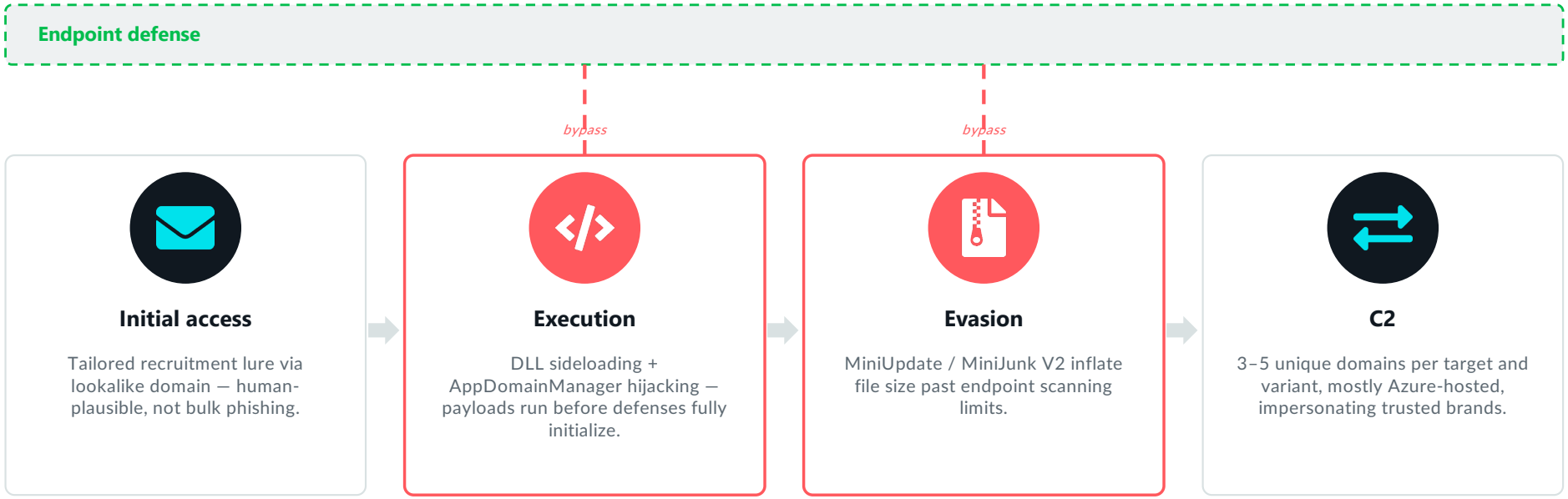




Answer: yes. Same class of adversary, same dependency — and the tradecraft is now purpose-built to beat the control you just invested in.

infoblox

Engineered to defeat the endpoint — and the C2 still has to resolve



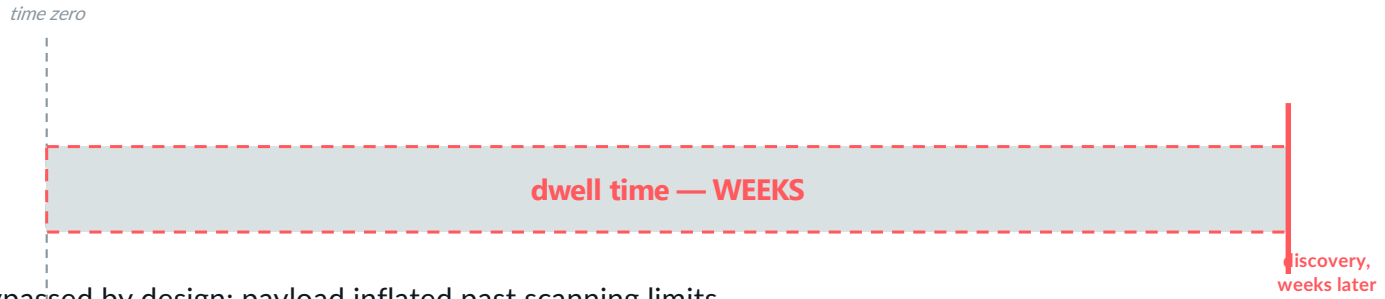
Every one of those evasions targets the endpoint. They invest there because that's where they expect you to be looking. Compartmented, rotating, cloud-hosted C2 still requires name resolution — the one step the adversary cannot engineer away.

Name resolution

the one gate every path must pass through — and exactly where Decoy Dog was found

infoblox.

Same intrusion, two outcomes: weeks versus minutes



- Endpoint telemetry bypassed by design; payload inflated past scanning limits.
- Each C2 domain fresh, victim-unique, reputable cloud host — reputation says nothing.
- Discovery weeks later via correlation or external tip; scope and owner unknown.



- Device identified the moment it connects.
- First C2 lookup evaluated at the DNS layer against infrastructure intel gathered while domains were being staged.
- Alert arrives pre-enriched with user, device, VLAN, location, and mission system.
- Automated policy segments the device and pushes the indicator to the ecosystem.

infoblox.

Residential proxies: no phishing, no malware — already inside government networks

- Residential proxy networks enroll ordinary consumer devices as traffic exit nodes — routers, gateways, set-top boxes, phones.
- An adversary rents that access and operates from a real, residential, in-country IP that no reputation list ever flagged.
- No longer a fraud-and-scraping story. This is general-purpose attack infrastructure.

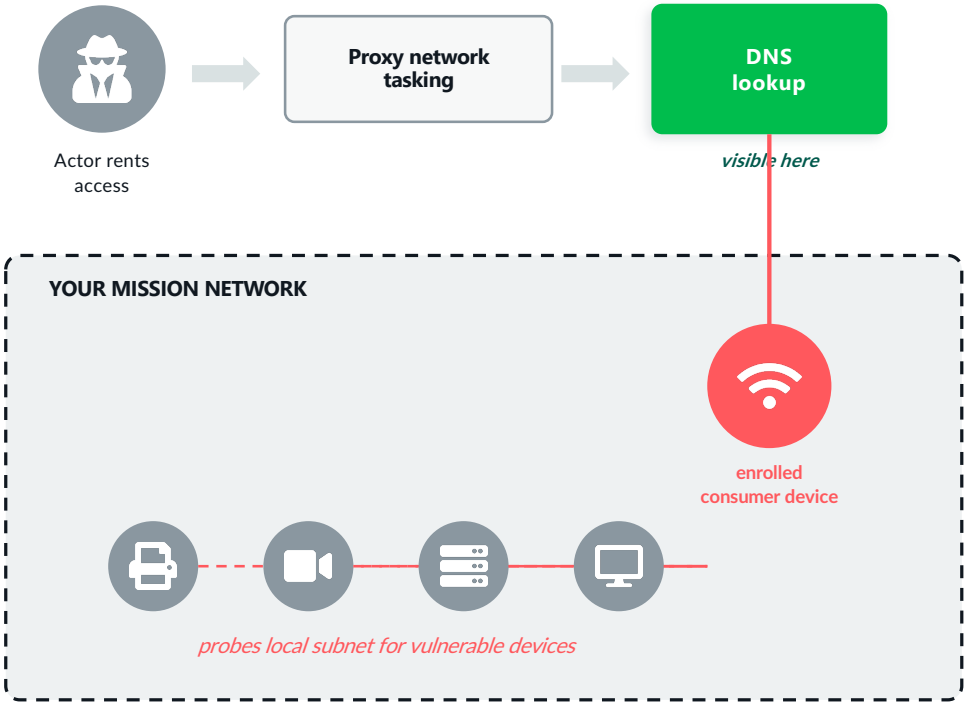
65%+
of Threat Defense Cloud customers queried residential proxy domains in 2026

60%+
of government customers queried these indicators

~25%
of cloud customers queried Kimwolf domains specifically

"...without any phishing, endpoint malware, or obvious signs of compromise."

Not a forecast — measured traffic, in 2026, from government networks. On peak days, 8% of customers were probed in a single day.



Attribution liability: a third party's incident response would correctly identify your IP space as the source.

infoblox.

Every IP-centric control fails here — and the FBI says so in writing

Controls that stop working

- ✖ **Rate limiting** thousands of rotating real home IPs
- ✖ **Geo-blocking** exit nodes chosen inside your own country
- ✖ **IP reputation** those homes were never on a list
- ✖ **ASN blocking** consumer ISP space you cannot block

DON'T TAKE OUR WORD FOR IT

FBI FLASH · 21 May 2026 · anonymization service used by ransomware actors

"Do not rely solely on IP-based blocking" — addresses are dynamically and ephemerally assigned.

The durable indicators the FBI publishes are domains — 1vpns[.]com / .org / .net, 1jabber[.]com — with an explicit caveat that the IPs get reassigned.

Who is operating on it

APT28 / GRU Unit 26165

Russian military intelligence compromising consumer CPE at scale to build proxy infrastructure — subscriber unaware, ISP blind at the IP layer. DoJ and FBI ran a court-authorized takedown of the U.S. portion.

IPIDEA

9–11 million daily active proxies used by 550+ distinct threat groups, including state-sponsored actors from China, DPRK, Iran, and Russia.

NetNut

2M+ hijacked consumer devices serving 316 threat clusters in a single week — including nation-state espionage masking origin IPs for password-spray attacks.

Every operator shares one dependency: enrollment, tasking, and persistence all run on DNS.

infoblox.

Three different problems. Same conclusion: the endpoint is not a reliable chokepoint.

Decoy Dog

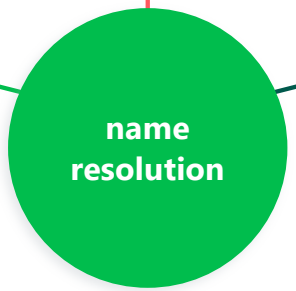
no file, no agent — the endpoint was never going to see it

Screening Serpens

has a file, engineered to beat the agent that is there

Residential proxies

no malware at all — an unmanaged device doing reconnaissance



The one behavior all three share, and none of them could avoid.

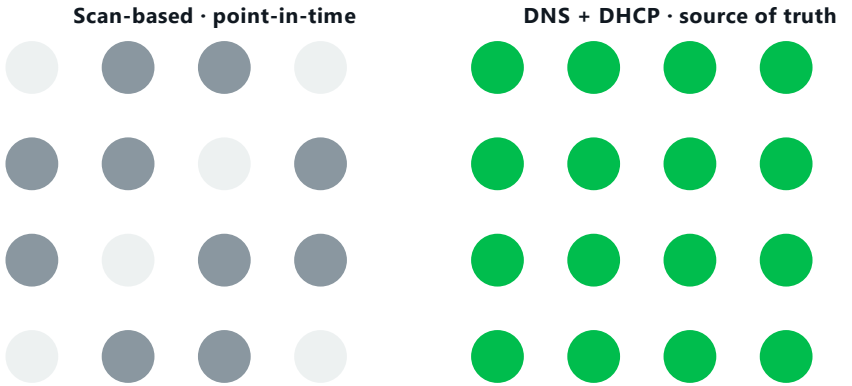
Detection here is independent of endpoint device or attack vector — which is what gives it maximal coverage.

"Are we really securing our network if we're not monitoring our DNS?"

infoblox.

See what's connected and how it behaves

- Need: a continuously validated, authoritative inventory across on-prem, cloud, OT/IoT, and unmanaged assets.
- Every device must use DNS and DHCP to connect — making those services a universal source of truth.
- DHCP leases, DNS registrations, and discovery yield real-time visibility into endpoints, subnets, VLANs, and zones.



faded / missing nodes

VLAN · subnet · zone context

~100% vs **60–70%**

coverage of network-connected assets vs scan-based discovery

infoblox.

Detect earlier at the DNS and network layer

Three tiers of detection — only one of them is early

Behavioral detection

Data science across domain metadata — registrar, TLD, SSL certificate, name server, registration behavior — to flag emergent and suspicious infrastructure while it is still being staged.

Independent of endpoint device or attack vector, for maximal coverage.

Reputational detection blocks what is already burned and listed

Signature detection needs a sample first — so it is always after the fact



This is the AI-era half of the defense: anomaly detection at query scale — exactly how Decoy Dog was found, with no malware sample in hand.

What DNS-layer theft actually looks like on the wire

```
ssn123-45-6789.baddomain.com

DOB01-01-82.baddomain.com

123PixieWay.baddomain.com

Fayettvile-AR.baddomain.com

----------------------------------------------------------

sdfarbixi4.18047.unkdomain.com
```

PII in the clear, then encoded tunnel traffic

Sensitive data walking out inside subdomain labels — no email attachment, no web upload, no blocked port, no file for an agent to scan. Phishing and lookalike domains, malware retrieval, C2, and tunneled exfiltration all surface at the same layer.

92% of cyber attacks use DNS at some stage — NSA

infoblox.

Strengthen Zero Trust and Comply to Connect

- Need: use asset and network context to enforce policy and validate what's allowed on the mission network.
- Deny or segment unknown and non-compliant devices by default — exactly the unmanaged population Case C exposed.
- DNS is a universal, protocol-agnostic policy and inspection point: prevention and attribution on every connection attempt.



Resolution request → Protective DNS enforcement point

prevention + attribution on every connection attempt

infoblox.

Automate response: turn an alert into an action

- Need: turn network activity into action without adding analyst burden.
- Pre-enriched alerts, automated containment, indicators pushed to SIEM, SOAR, NAC, and firewall.
- DNS logs preserved as forensic and audit evidence.

One picture from every resolver you already run

BIND	*on-prem · hybrid · multi-cloud*
Microsoft DNS	*on-prem · hybrid · multi-cloud*
Route 53	*on-prem · hybrid · multi-cloud*
Azure DNS	*on-prem · hybrid · multi-cloud*
Google Cloud DNS	*on-prem · hybrid · multi-cloud*

The same SIEM event, before and after attribution

BEFORE

```
Source IP address: 198.18.197.61
```

An analyst cannot act on this. IPs get reassigned.

AFTER

Security event: DATA EXFILTRATION

```
Threat level:  Medium
Private DNS name:  ip-10-0-0-254.us-west-2.compute.internal
Provider:  AWS
Account ID:  905418046272
Region:  us-west-1
Domain:  vpc
```

Same alert. Now it names the workload, the account, and the region — so it can be acted on, or acted on automatically.

Visibility feeds detection, detection sharpens enforcement, enforcement generates more visibility — a system, not a shopping list.

infoblox.

We inspect the vehicle before anyone drives it. We don't always inspect what connects.

- Before a vehicle moves, someone runs the inspection checklist — safe, serviceable, mission-ready.
- We do this rigorously for vehicles — inconsistently for the thousands of things joining networks daily.
- ***Comply-to-Connect*** is that checklist for the network.
- Netw eck possible at all.



ITEMS TO BE CHECKED
(Circle items applicable to your vehicle type only)

1 CLEANLINESS/DAMAGE/MISSING ITEMS (Interior/Exterior) UNUSUAL NOISE OR OCCURRENCE (During operation)
2 LEAKS/FLUID LEVELS (Visually check for any leaks/check oil/coolant/hydraulic/transmission/brake fluid)
3 SAFETY DEVICES (Warning lights/horn/warning devices/emergency/backup horns/seat belts)
4 BATTERIES (Fluid/charge/clean/hires/security / INSTRUMENTS/GAUGES (Operation & readings)
5 DRIVE BELTS (Fraying/cracking/tension) PULLY / MOTOR (Air / hydraulic / electrical)
6 STEERING SPRINGS/ SHACKLES (Free play/ excessive wear)
7 EXHAUST SYSTEM SPARK ARRESTORS (Damage/ leaks)
8 TIRES/ WHEELS (Lug nuts/ cracks) TRACKS
9 HEATER/ DEFROSTER/ AIR-CONDITIONER/AUXILLIARY GENERATORS/ AUXILLARY HEATERS
10 BRAKES (Servicing/Parking) CLUTCHES (Operate) ACCELERATOR/PEDAL (Damage/wear)
11 WINDSHIELD (Wipers/ washer fluid/ cracks)
12 HYDRAULIC HOSES (Damage/ hoses) CYLINDERS/ VALVES (Damage/leaks)
13 COLD WEATHER ADS (Ether/alcohol/ injector/battery heaters/oil-engine heater/coolant heater, etc.)
14 POWER TAKE-OFF (PTO)
15 WINCH/TOW CONNECTIONS
16 AIR TANKS (Drain daily or after operation)
17 MAST/ TINES/ROLLERS/ TINES
18 ROLLERS/POWER COVEYORS/RAILS/LADDERS/CAT WALKS/CARGO BED
19 BED (A LOAD) TOP/HALF/LOWEST ROLL SHIFT/TANK (check position)
20 LOWER LOBE CAB SHIFT (Operation)
21 EMERGENCY STAND-BY SYSTEM
22 WARNINGS-CHECK LEGIBILITY ("WATCH STEP" stencil AROUND 1-10")
23 CHUTES/ASSEMBLY/ PLAQUES/NAMEPLATES
24 DRUMS/CROWN/GEAR/ LEADS
25 BOOMS/OUTRIGGERS/BASKET/PLATFORM/TURNTABLE (Check for cracks and damage)
26 BROOMS/SPROCKETS/CHAINS
27 BLADES/REELS/SICKLE BARS/FLAILS
28 KETTLE / HOISTING MECHANISM / AGITATORS
29 SHEAVES / BLOCKS / CABLES
30 MOULDBOARDS / BOWLS / CUTTING EDGES / SKIDS
31 PUMPS / PIPING / DISCHARGE VALVES FOR LEAKS, CORROSION / SPARE BARS
32 FIREFIGHTING SPECIALIZED EQUIPMENT / SAFETY DEVICES (Axe, spanner wrench, power saw, ladder, pike pole, trouble light, mega phone, generator, resuscitator, rescue tools, winch/Buzzers, fire extinguishers, ropes, breathing apparatus, personal alert safety system, etc)
33 FIREFIGHTING SYSTEM OPERATION AND FOAM / WATER LEVELS
34 AUXILLARY FIREFIGHTING SYSTEM (Nitrogen tank pressure, agent levels, etc)
35 HOSE / REELS / HANDLINES / TURRETS (Operational functions)
36 OTHER (Specify)
37 OTHER (Specify)
38 OTHER (Specify)
39 OTHER (Specify)
40 OTHER (Specify)

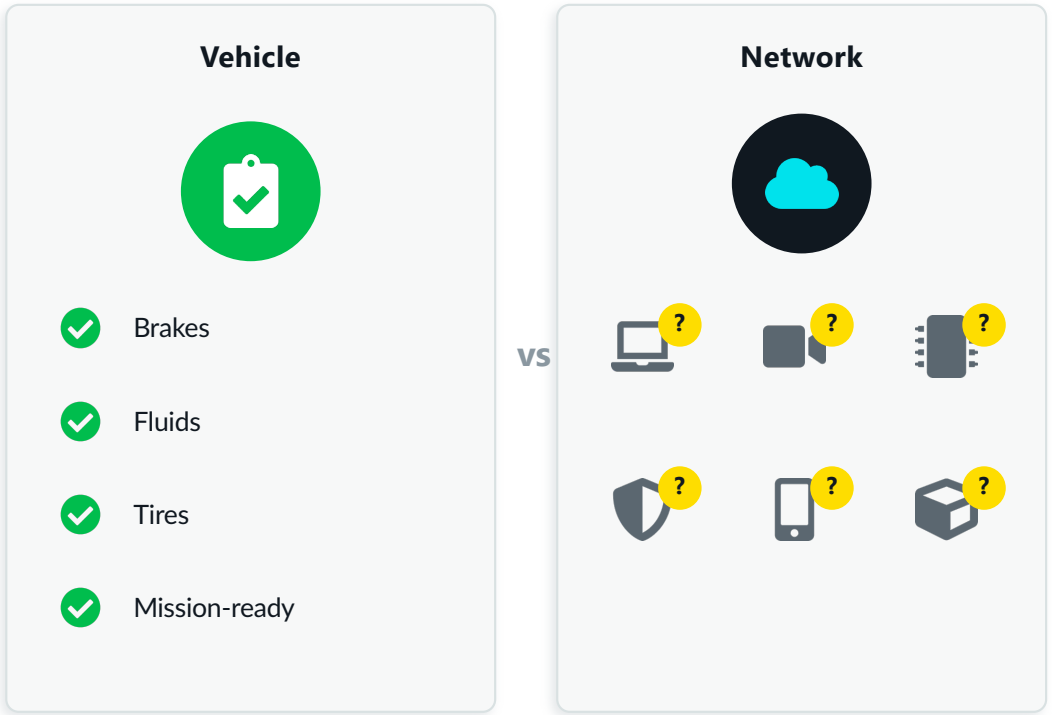
OPERATOR'S INSPECTION GUIDE AND TROUBLE REPORT (For use with all Registered Vehicle Equipment except Returning Vehicles and Equipment) MONTH/YEAR

VEHICLE TYPE | REGISTRATION NO.
ORGANIZATION | LOCATION/BASE | PHONE NO.
VEHICLE CONTROL OFFICER NAME | PHONE NO.

OPERATOR'S SIGNATURE SIGNIFIES ACCOMPLISHMENT OF CHECKS (LAST NAME ONLY REQUIRED)

DAY	SHIFT/SIGNATURE	DAY	SHIFT/SIGNATURE	DAY	SHIFT/SIGNATURE
1		11		21	
2		12		22	
3		13		23	
4		14		24	
5		15		25	
6		16		26	
7		17		27	
8		18		28	
9		19		29	
10		20		30	
				31	

AF FORM 1800, 20060901 Previous Editions Are Obsolete Page 1 of 2 Pages



infoblox

Comply to Connect and Zero Trust already require this — across every mission network

- C2C in one line: discover, identify, and assess every device before and while it connects — continuously determine whether it may connect, where, and to what.
- Impossible without authoritative visibility — so visibility is the foundation of C2C, not an accessory.
- Zero Trust removes implicit trust — but DNS is the most commonly overlooked implicitly-trusted service.

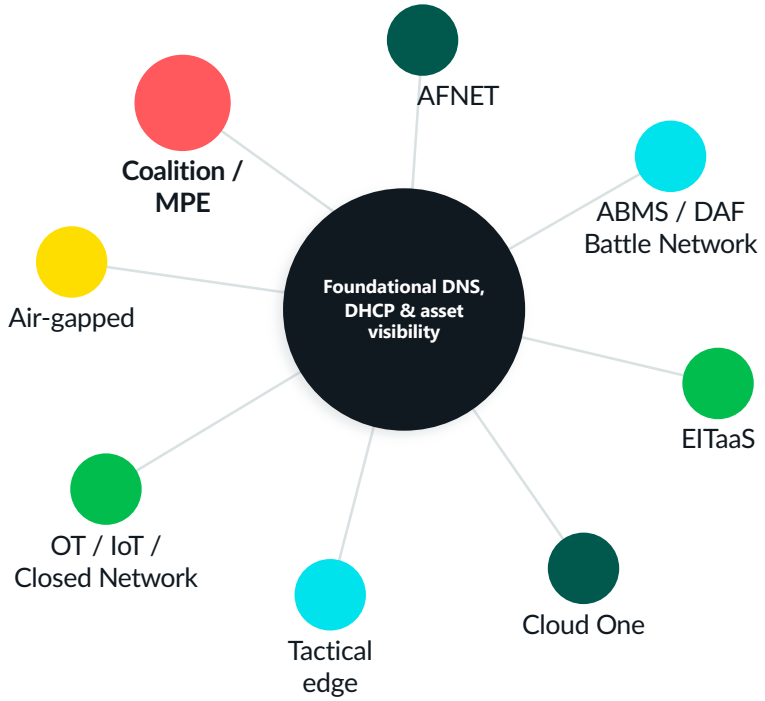
If you implicitly trust DNS, it isn't Zero Trust.

Policy backing

NIST SP 800-207	OMB M-22-09	NSA/CISA PDNS	NIST SP 800-81r3

Mission network specifics

- Hardened, STIG-mapped authoritative DNS; DNSSEC with FIPS-validated crypto; encrypted DNS (DoT/DoH).
- Automation to cut drift and manual error — cleaner ATO, CCRI, and RMF pathways.
- Air-gapped: Protective DNS with local resolution still enforces policy when the cloud is unreachable.



MPE is the sharpest case — more partners, enclaves, and classification boundaries than legacy DNS was built to serve.

infoblox.

See → Decide → Assure — what to do Monday, and how we do it

See — Establish authoritative, cross-environment asset and network visibility.

Decide — Instrument DNS as a high-fidelity, context-enriched detection and enforcement point.

Assure — Automate response and connect security, network, and operations data.

reactive → assured

Three things you can start Monday

1. **Ask the two questions.** What is connected to my network right now, and what is it trying to resolve? Note how long the answer takes.
2. **Find out whether anyone is looking at DNS.** Are internal resolver logs collected, retained, and searchable — or discarded at the resolver?
3. **Run the proxy check.** Query your own resolver logs against published residential proxy and anonymization indicators. Kimwolf and the FBI FLASH domains are a starting point.

AND THIS IS HOW WE DO IT

Infoblox tracks adversary infrastructure while it is being built — not after it is used.

68.4 **days earlier** blocking than the rest of the industry

90% **of threats detected** before the first DNS query

.0002% **false-positive rate** plus real-time protection for newly seen domains

Active threat count under track

>11.6M High risk domains
>10.9M Medium risk domains
>13.8M Low · log and watch risk domains

"It's like watching the threat actors — and the nation-state actors — who are watching you."

infoblox.