



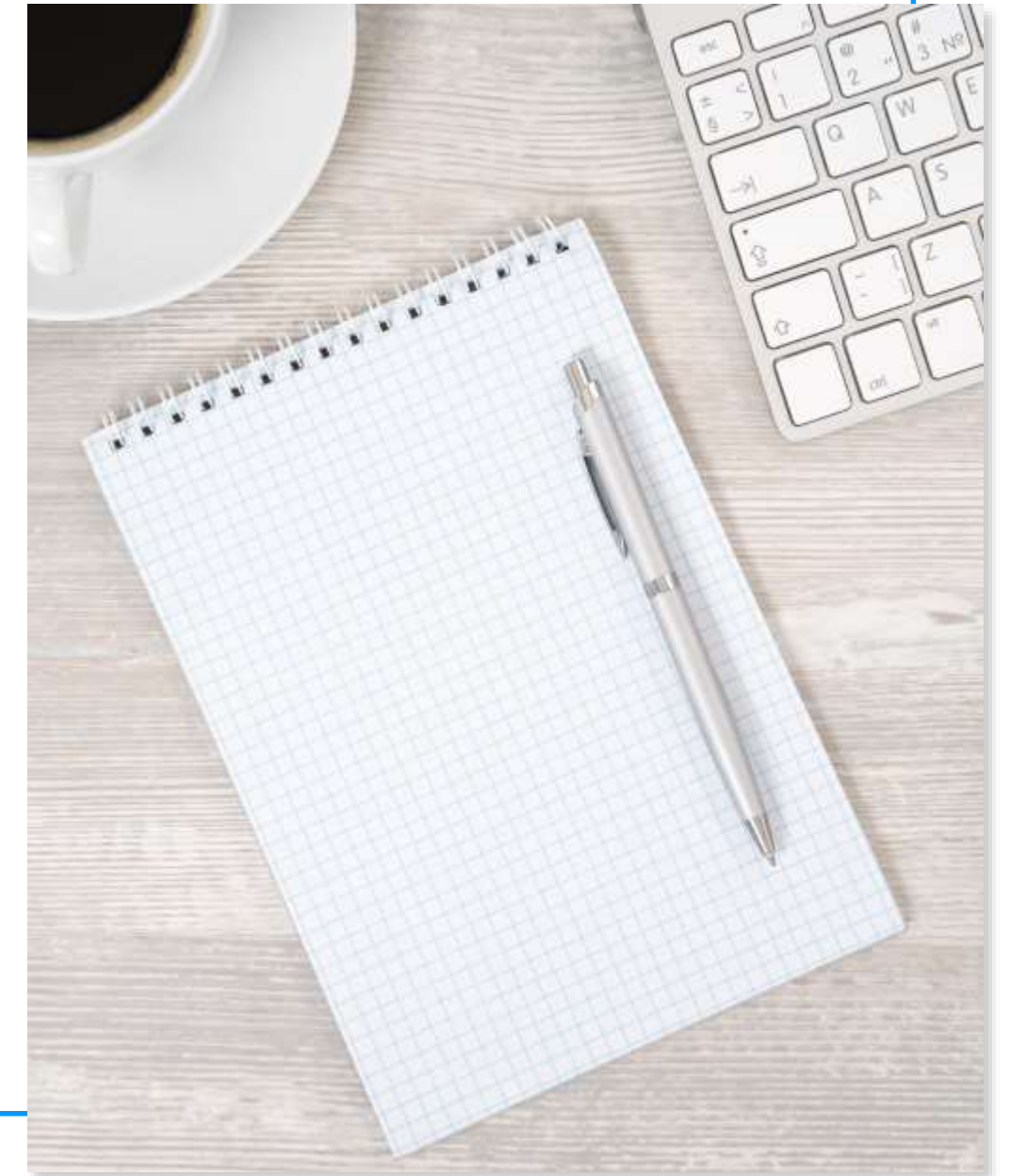
Shadow IT Control

How to Make it Simple with DNS

Bernd Wilhelm
Customer Solutions Architect

Agenda

- 1. State of Shadow IT Today**
- 2. How DNS Provides a Simple Way to Jump-start Detection and Control**
- 3. Key Takeaways**



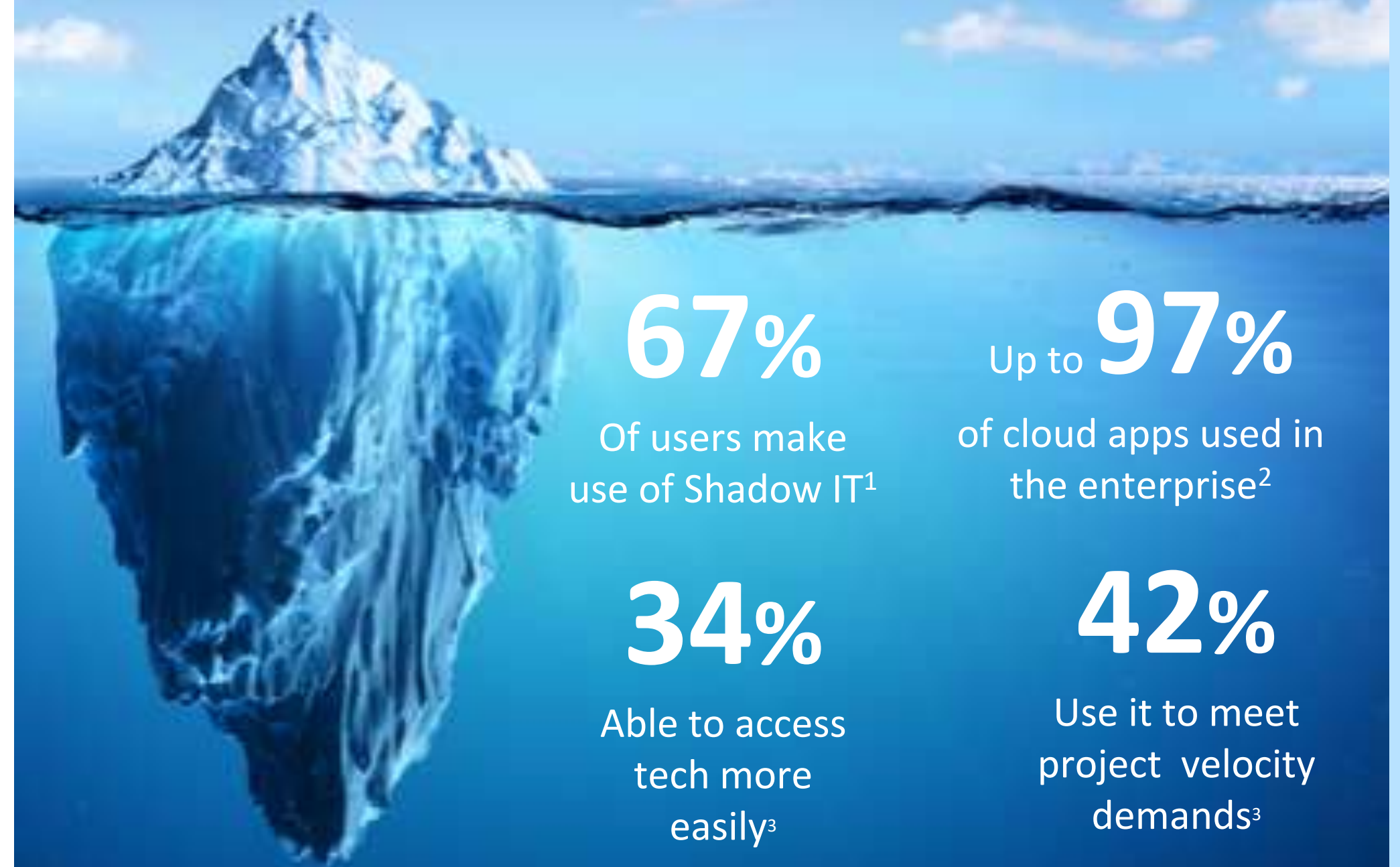
State of Shadow IT

Shadow IT Snapshot

“IT-related hardware, software and services outside the ownership or control of IT organizations”

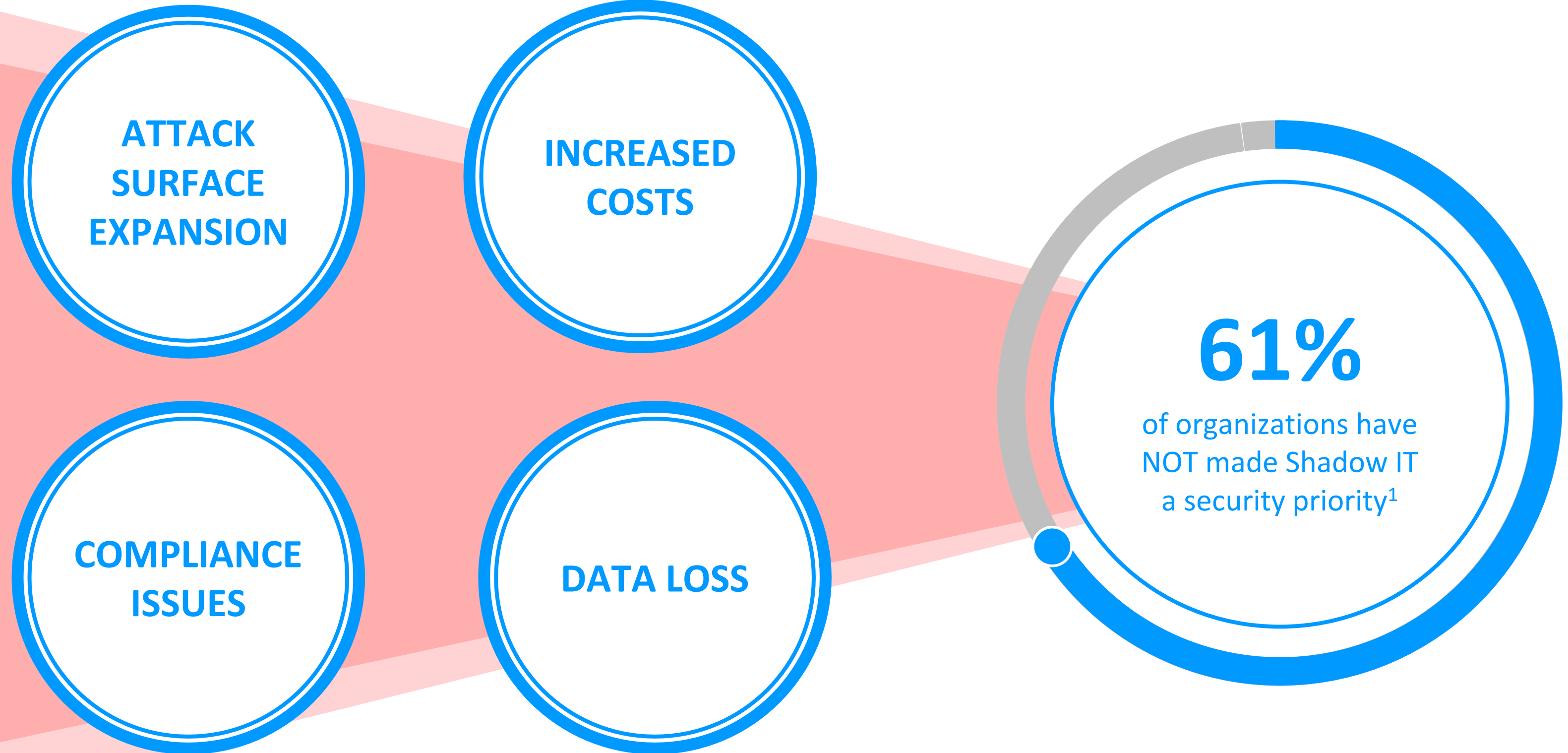
Gartner

Digital Transformation Amplifies Shadow IT Usage



¹ TNW, Why Shadow IT is the next looming cybersecurity threat, April 2019 - ² 2021-07-Cloud and Threat Report-RR-474-1 - ³ IDC Summit 2021: What Drives Shadow IT

Shadow IT Risks

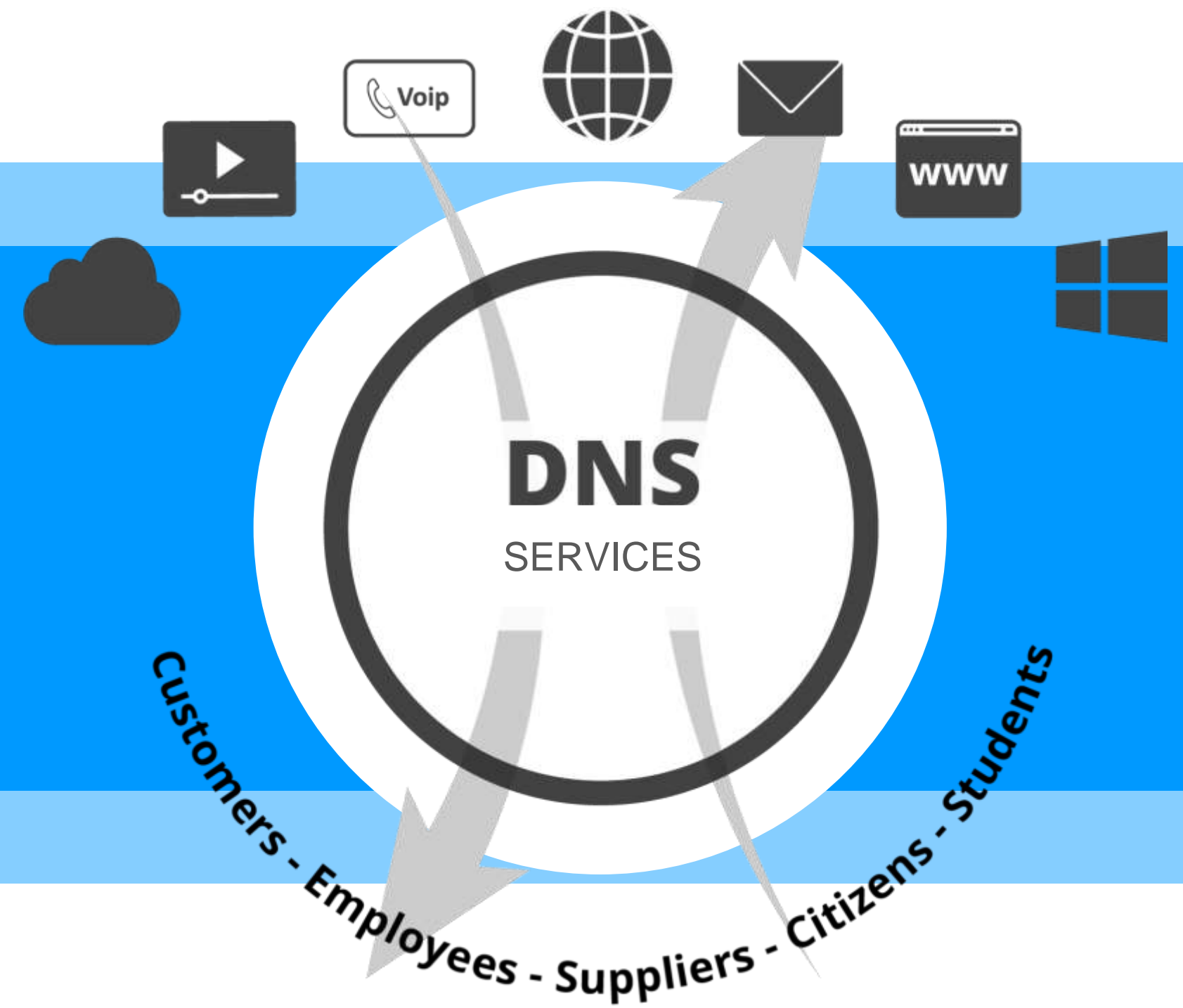


IDC DNS Threat Report 2022

How DNS Provides a Simple Way to Jump-Start Detection and Control

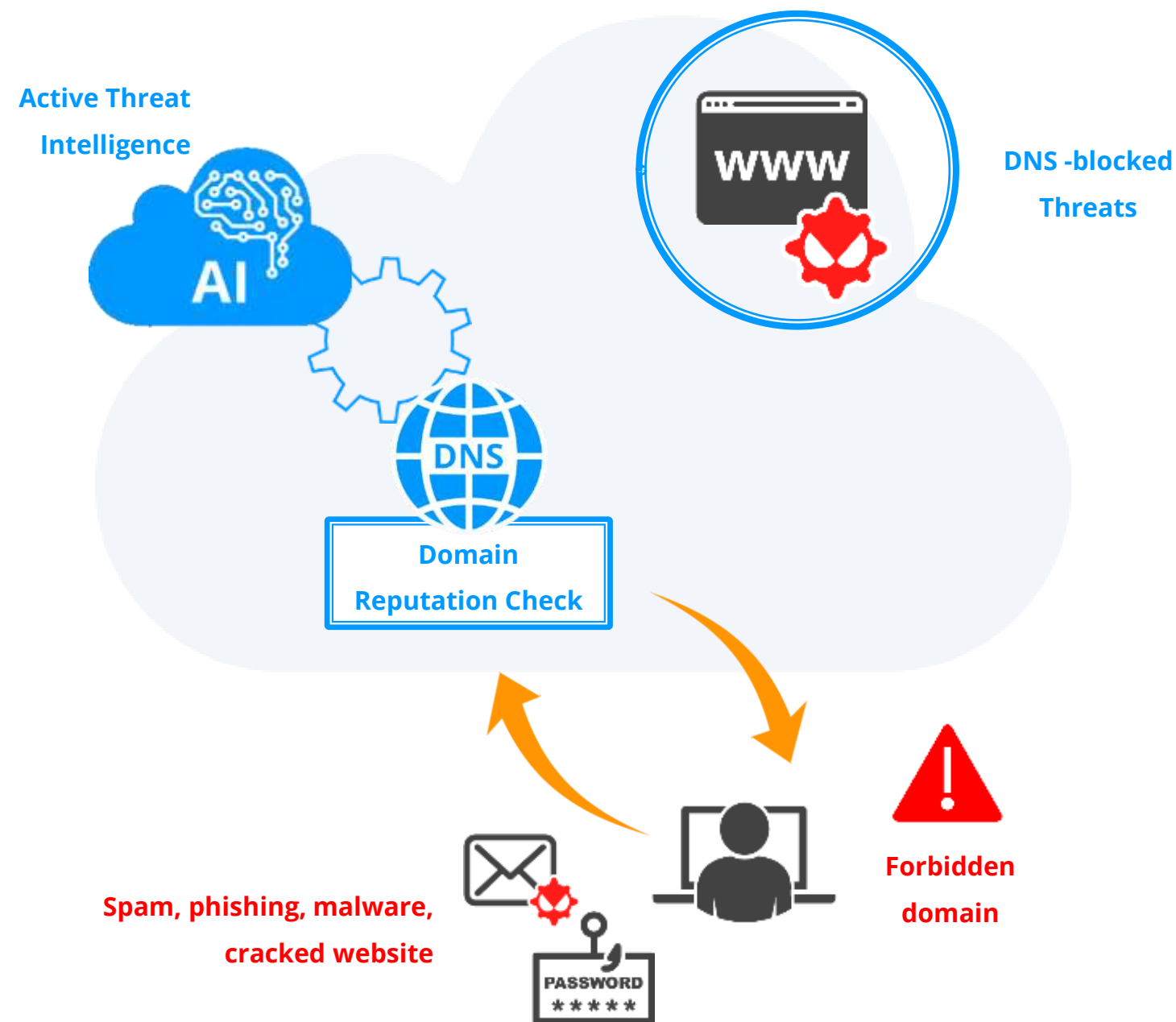
Why DNS Can Help in Fighting Shadow IT?

1. At the intent of all IP communications
2. Route internal and external traffic between users and apps.
3. Visibility over network traffic at the user level



How DNS Can Help Fighting Shadow IT? (1)

Outgoing Traffic Control



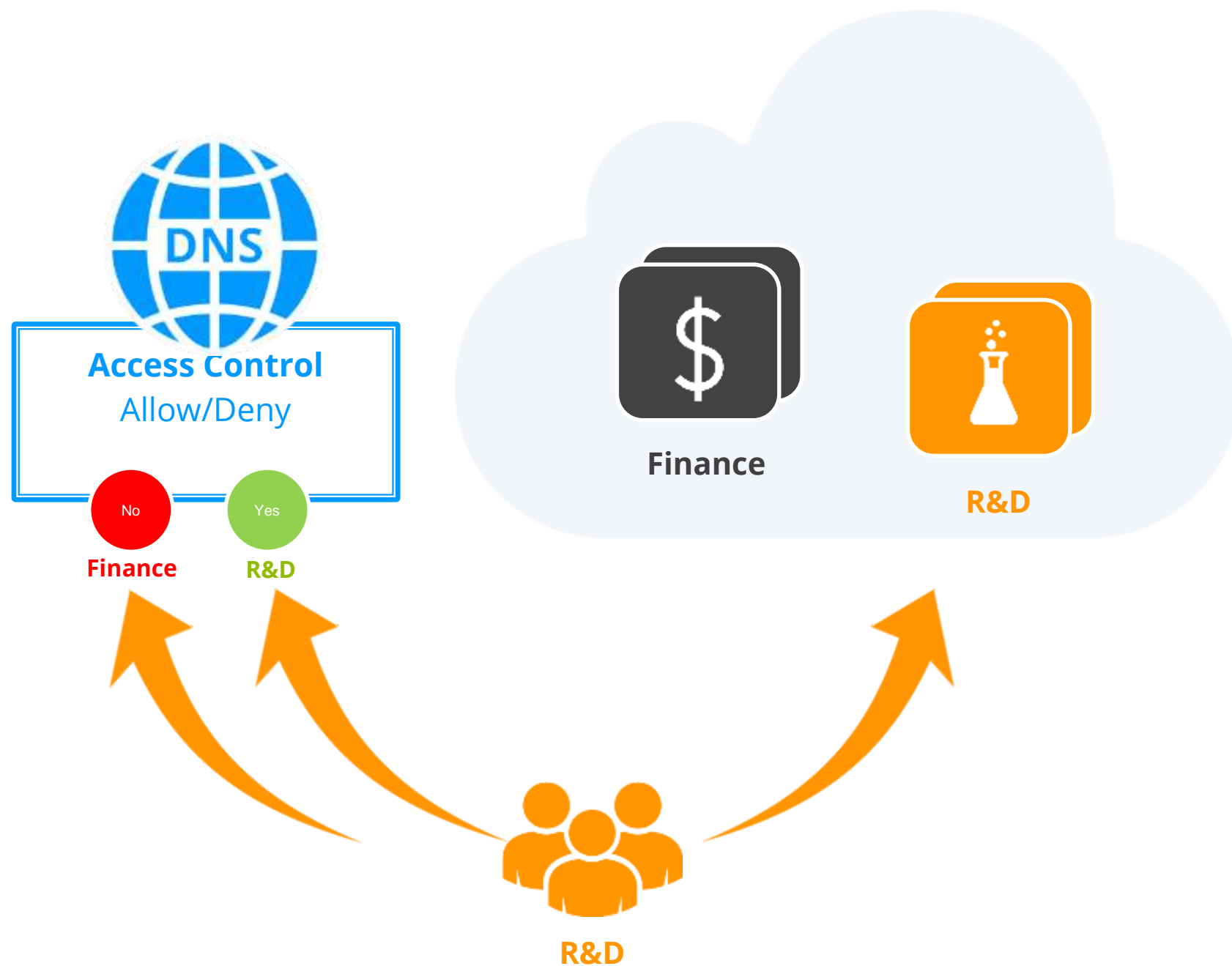
Identify and Block DNS Resolution for Known Malicious Destination

BENEFITS

- ✓ Prevent Initial infection
- ✓ Block Malware activity
- ✓ Adapt Protection

How DNS Can Help Fighting Shadow IT? (2)

Micro-segmentation & Application Zoning



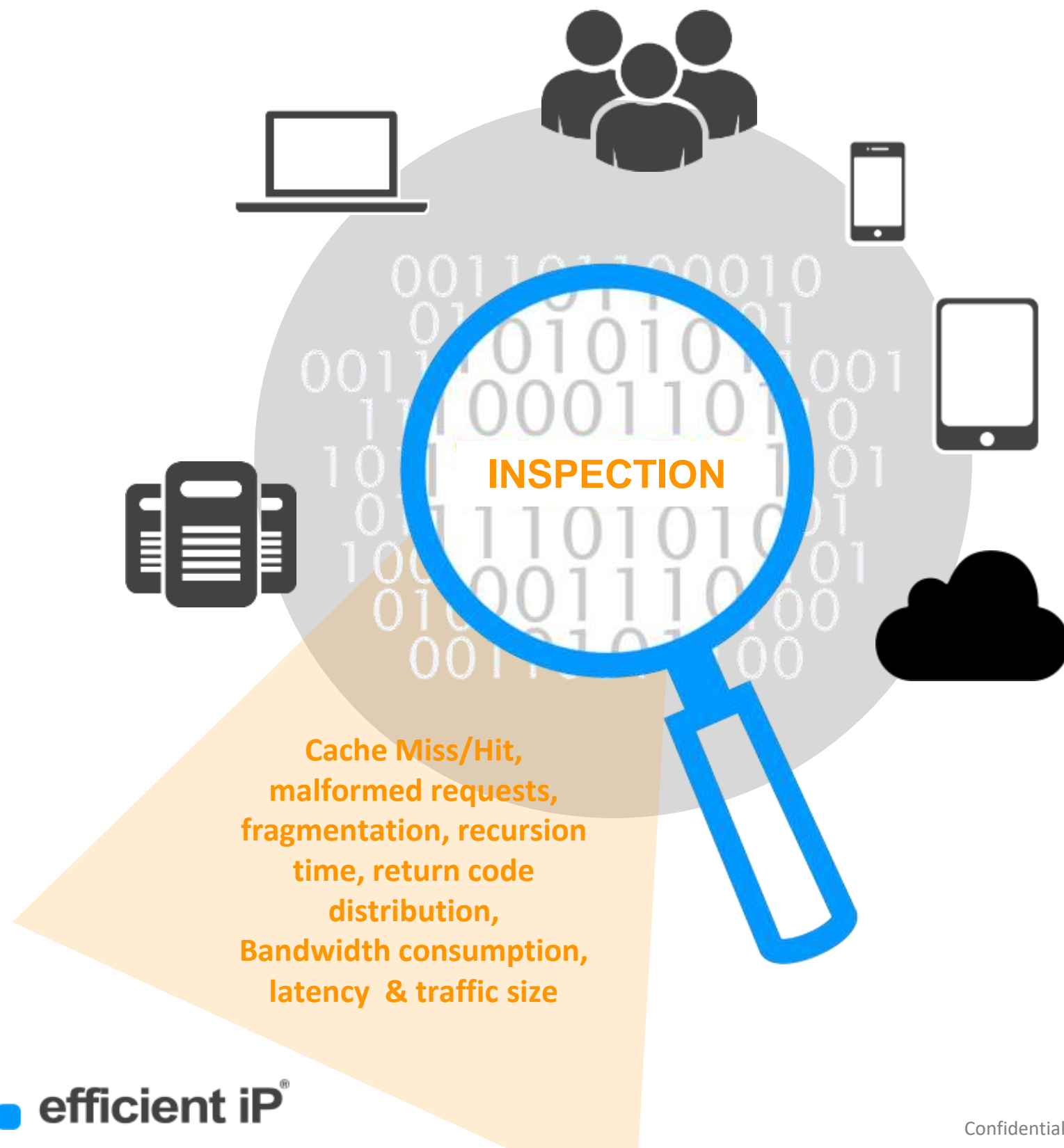
Control Internal and Ext. App Access
with User-Based Filtering Policies

BENEFITS

- ✓ Reduce attack surface
- ✓ Mitigate lateral move
- ✓ Improve breach containment

How DNS Can Help Fighting Shadow IT? (3)

User-Based Behavioral Traffic Analysis



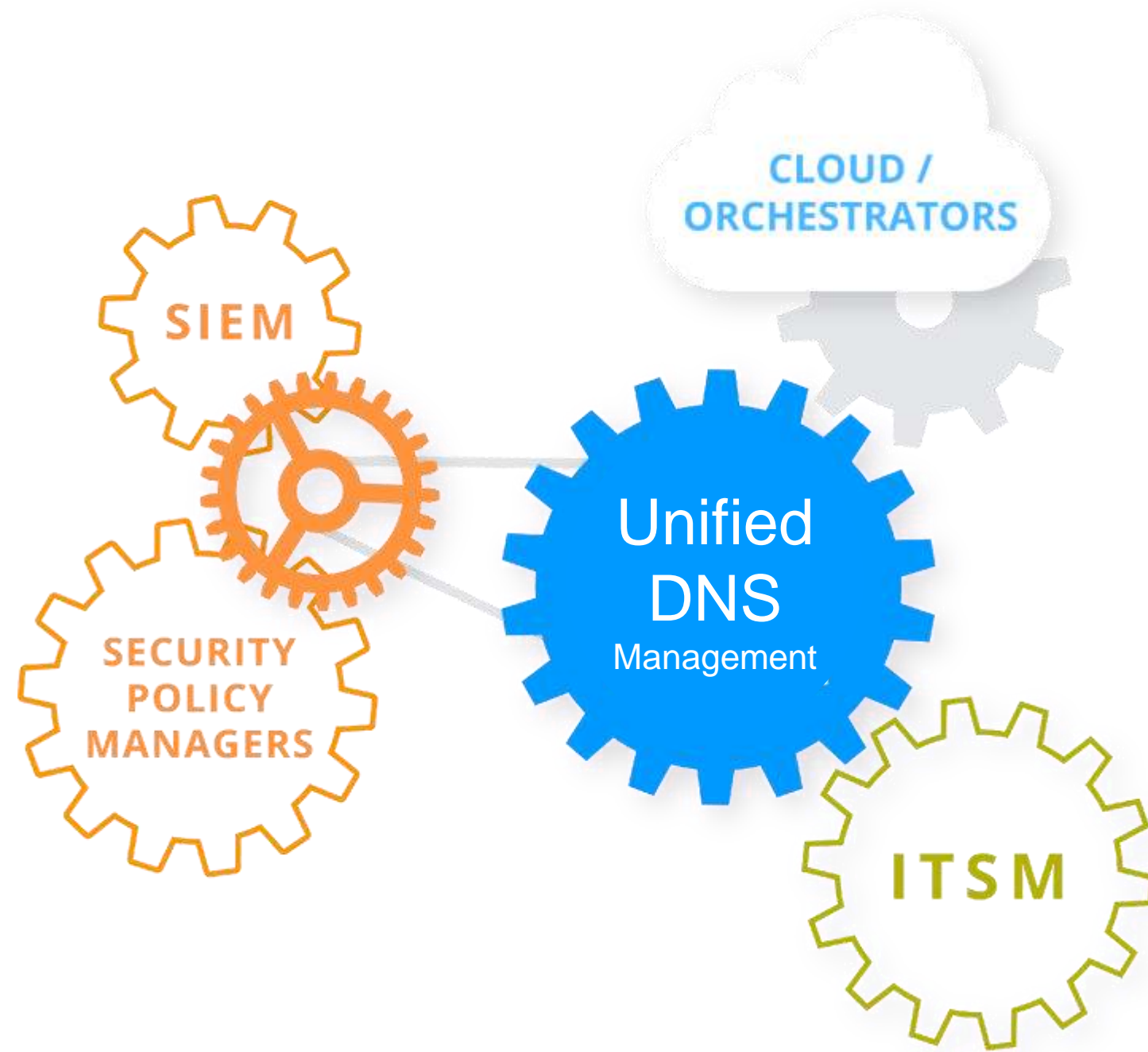
**Real-Time Advanced DNS Analytics
Enables Behavioral Threat Detection**

BENEFITS

- ✓ Detect threats beyond limited signature mechanisms
- ✓ Enable predictive security
- ✓ Simplify incident investigation

How DNS Can Help Fighting Shadow IT? (4)

Enforce DNS Security Posture Policies




Integrated and Centralized Management & Reporting, Enterprise-wide

BENEFITS

- ✓ Ensure consistent security policies
- ✓ Simplify regulatory compliance
- ✓ Accelerate security response

Three Key Takeaways

- 
- 1.** DNS sees all traffic intent, so is by design ideally placed to be your 1st line of defense
 - 2.** DNS can easily detect queries from unapproved apps or services
 - 3.** You already have a DNS, so is an obvious simple, cost-effective starting point for controlling Shadow IT

EfficientIP In Brief

DDI

Network Automation &
Security Company

110+
Countries

- App & infrastructure Life-Cycle Automation
- Intelligent App Traffic Steering
- Adaptive DNS security



Open
Ecosystem
Integration

Vision: Make Networking Simple & Secure Everywhere,
Deliver the Best User Experience at all Times

HQ
USA - Philadelphia
EMEA - Paris
APAC - Singapore

1000+
Customers in
All Industries



- Improve Efficiency
- Reduce Risks
- Lower Costs

1000+ Companies From All Industries & All Sizes Trust Us To Enable & Secure Their Business





Come and meet us on Stand 7-120

