OpenDNS

Tech update

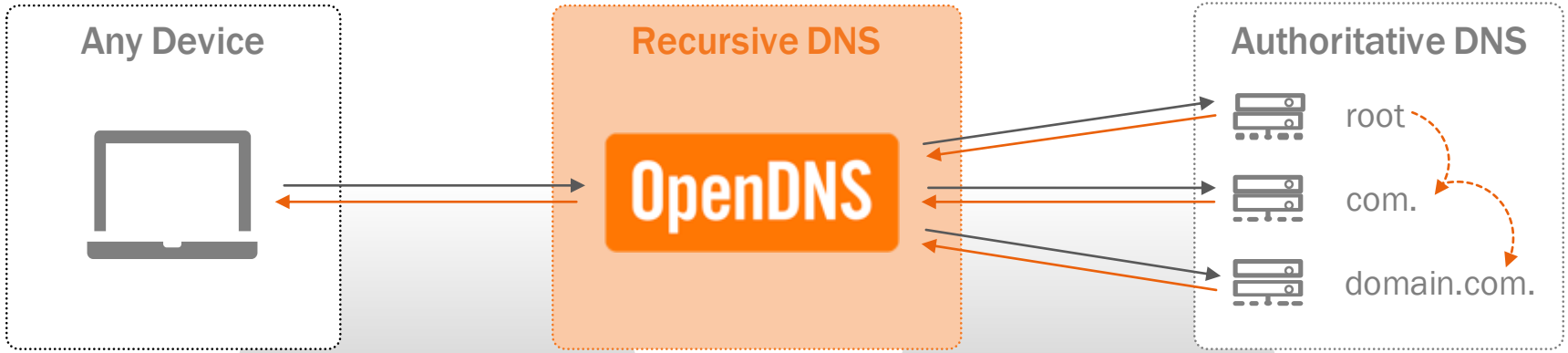
Mikael Grotrian, CISSP, CISM, CCSK, GISF, ITIL, PRINCE2, TOGAF Certified

Consulting Systems Engineer, Cyber Security, Denmark

OpenDNS is
now part of Cisco.

CISCO

Through DNS Resolution We Make Many Discoveries



Request Patterns

Used to detect:

- Compromised systems
- Command & control callbacks
- Malware & phishing attempts
- Algorithm-generated domains
- Domain co-occurrences
- Newly registered domains

Authoritative Logs

Used to find:

- Newly staged infrastructures
- Malicious domains, IPs, ASNs
- DNS hijacking
- Fast flux domains
- Related domains

A New Layer of Breach Protection

UMBRELLA
Enforcement

Threat Prevention
Not just threat detection

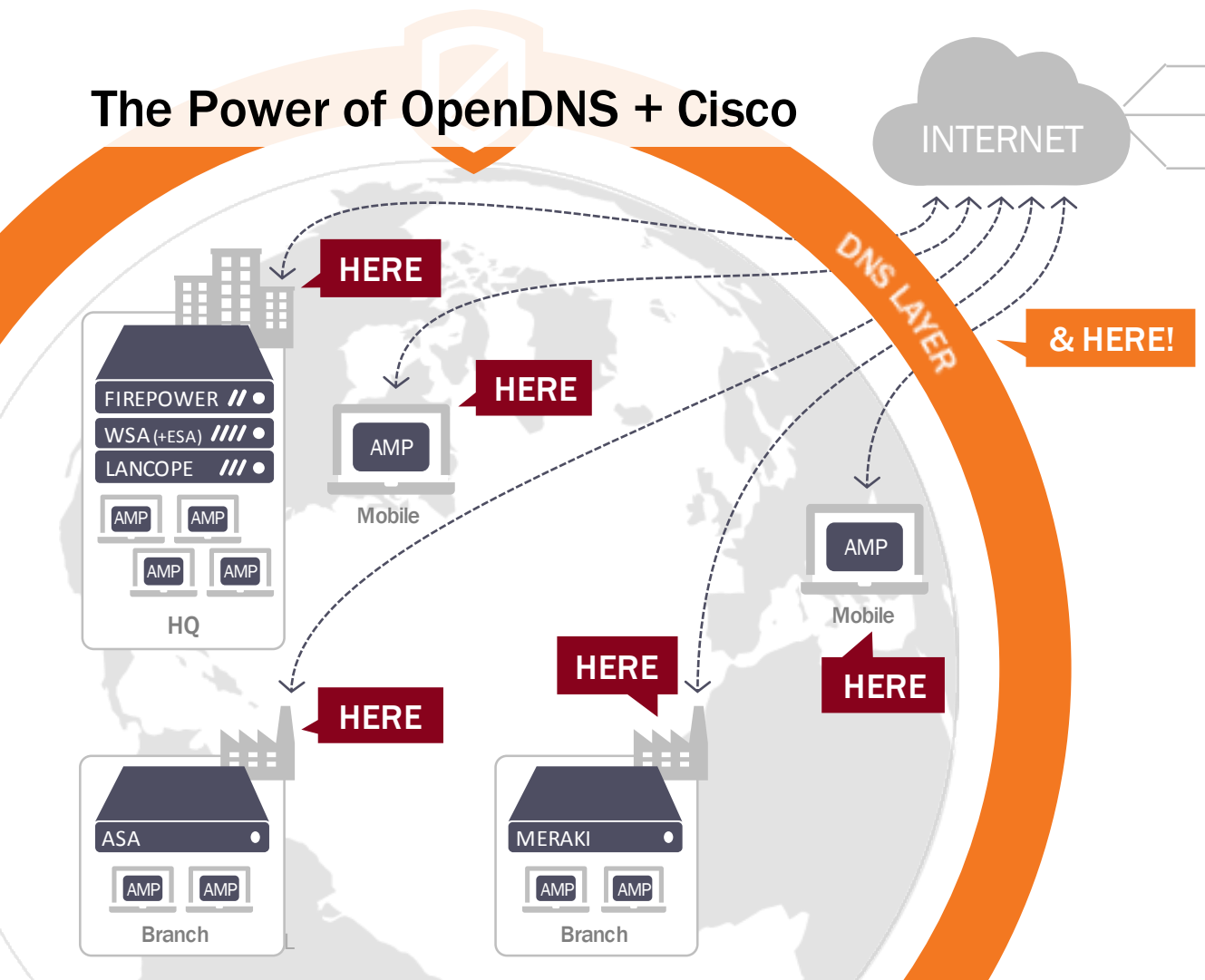
Protects On & Off Network
Not limited to devices forwarding traffic through on-prem appliances

Always Up to Date
No need for device to VPN back to an on-prem server for updates

Block by Domains for All Ports
Not just IP addresses or domains only over ports 80/443

Partner & Custom Integrations
Does not require professional services to setup

The Power of OpenDNS + Cisco



BENEFITS

Alerts Reduced 2x; Improves Your SIEM

Block malware before it hits the enterprise;

Contains malware if already inside

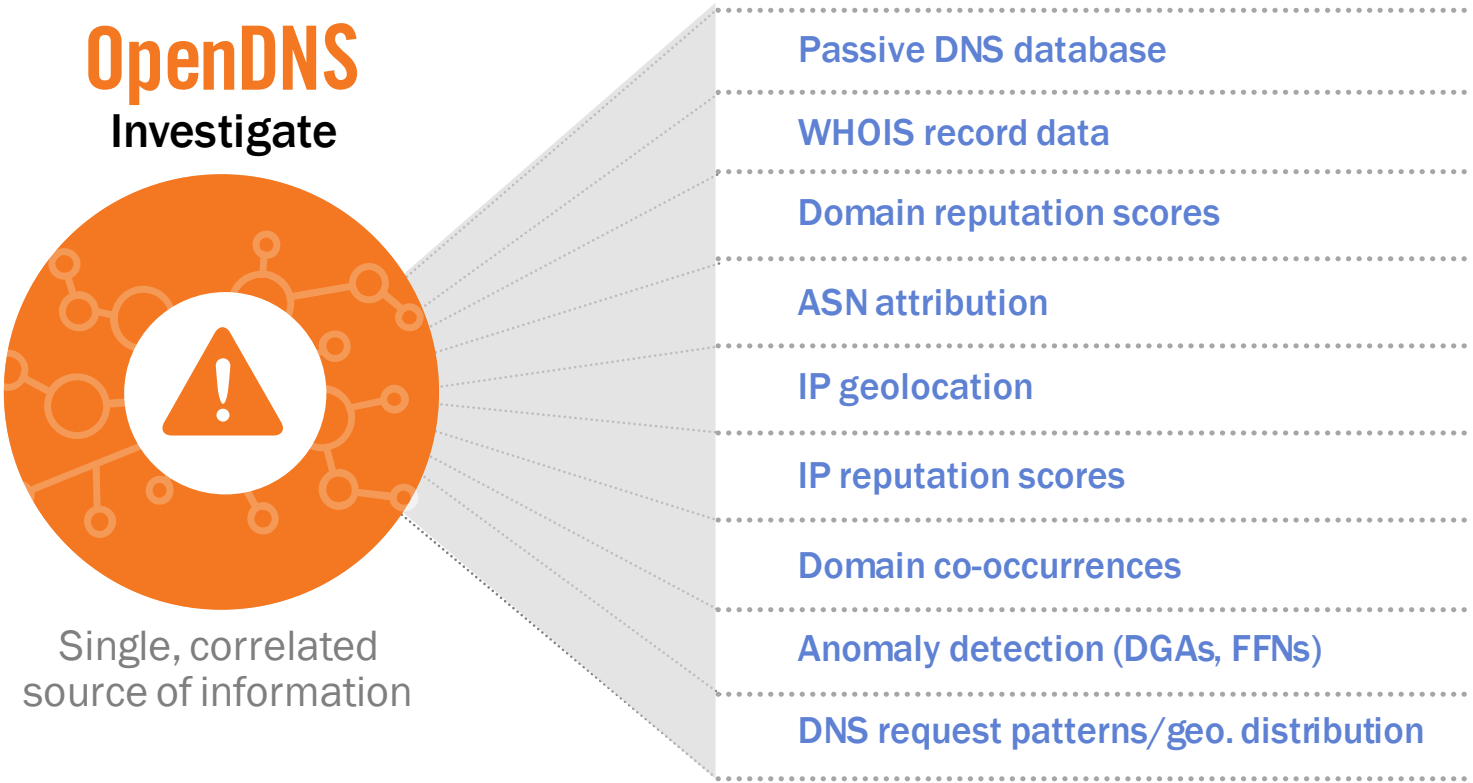
Internet Access Is Faster; Not Slower

Provision Globally in Under 30 Minutes

OpenDNS

We see where attacks are staged

Types of Threat Information Provided



Use Our Global Intelligence To…

You Know
One IOC

We Know All Its
Relationships

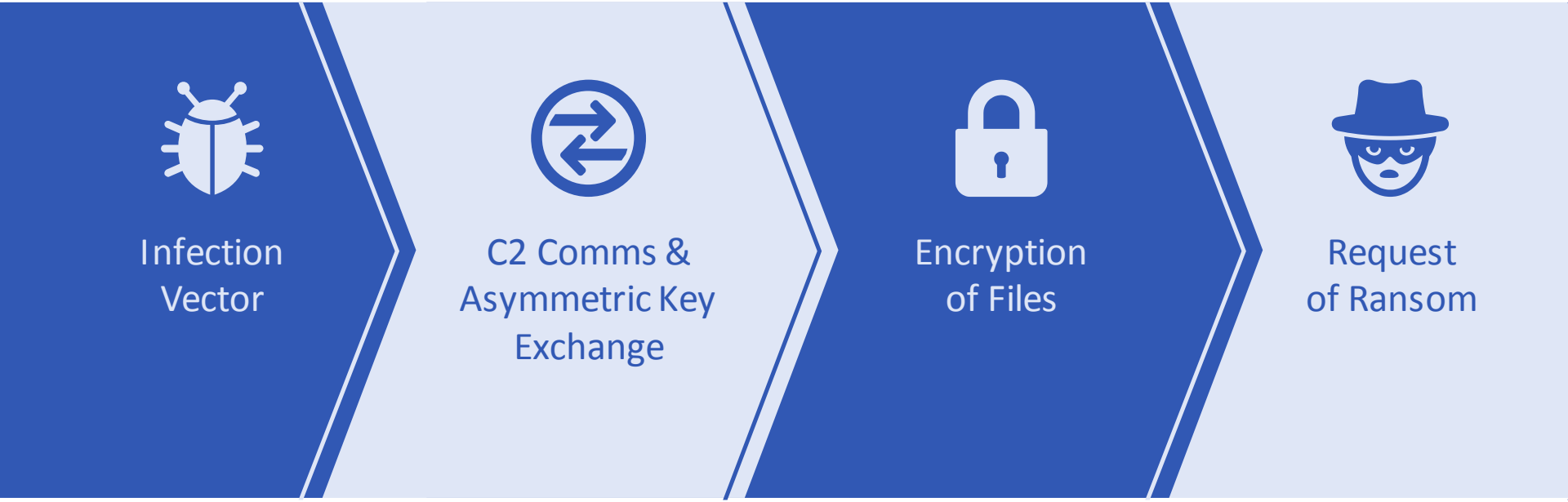
Your Local
Intelligence

Our Global
Context

- Speed up investigations
- Stay ahead of attacks
- Prioritize investigations & response
- Enrich security systems with real-time data

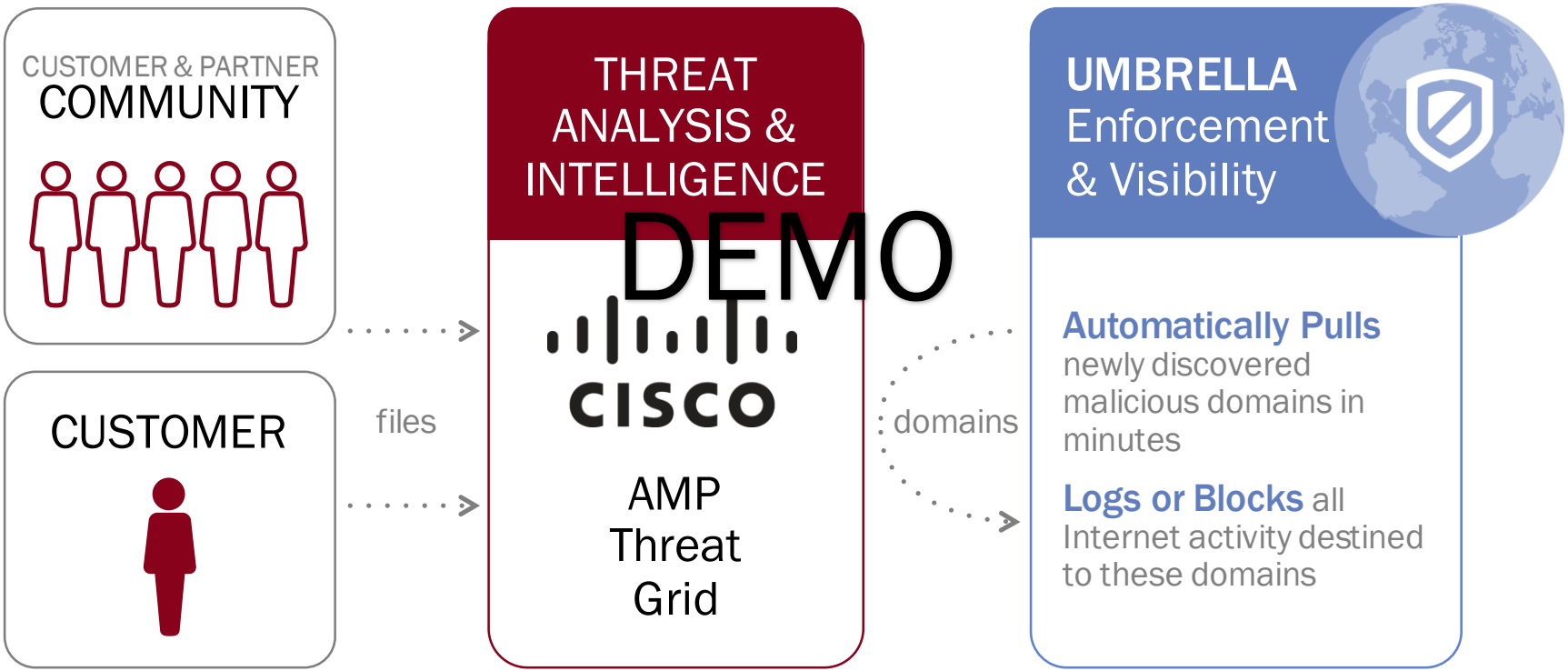

Your personal files are encrypted by CTB-Locker.
Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.
Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.
You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.
Press 'View' to view the list of files that have been encrypted.
Press 'Next' for the next page.
WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.
View
95:59:29
Next >>

Typical Ransomware Infection



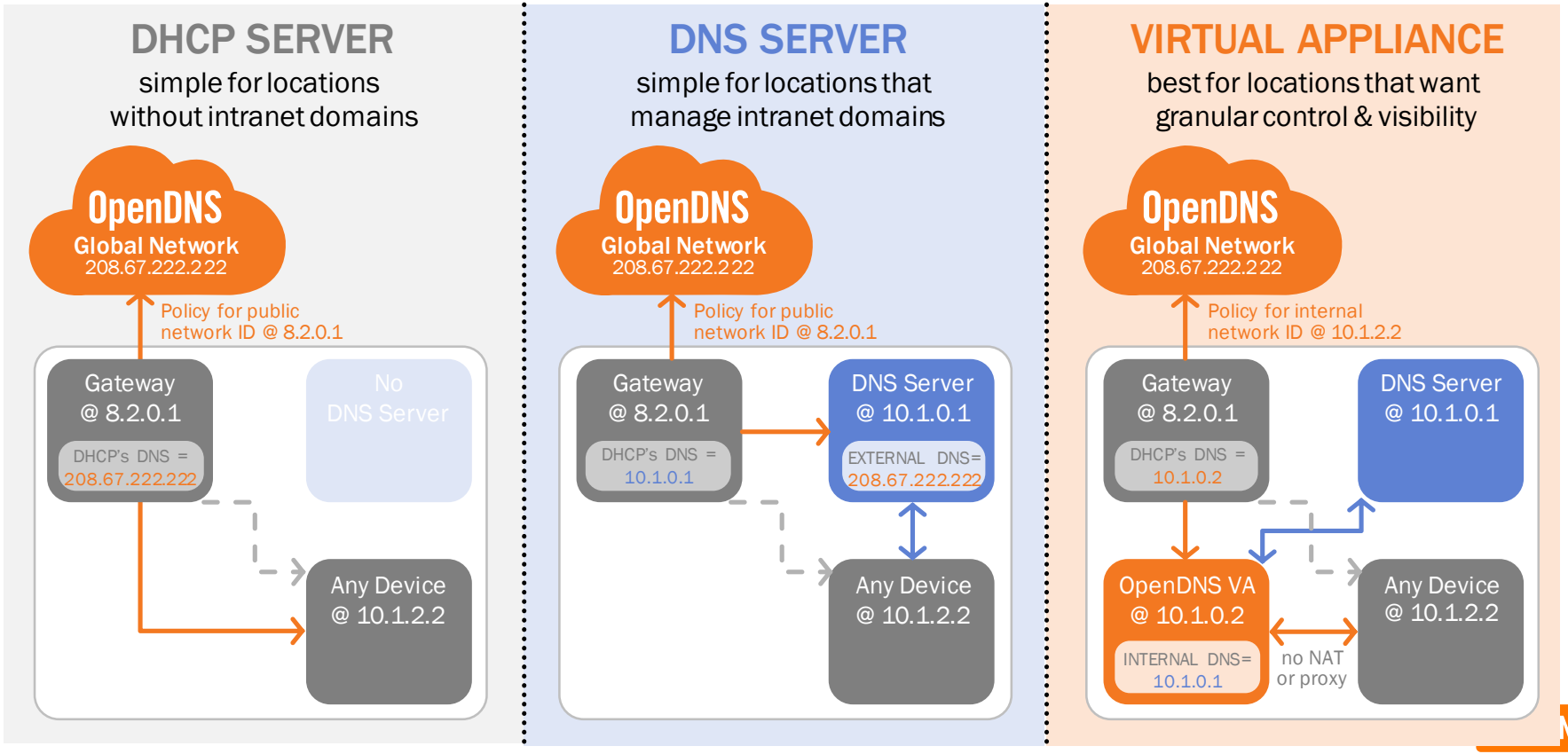
	Encryption C&C				Payment MSG
NAME	DNS	IP	NO C&C	TOR	PAYMENT
Locky	●	●			DNS
SamSam			●		DNS (TOR)
TeslaCrypt	●				DNS
CryptoWall	●				DNS
TorrentLocker	●				DNS
PadCrypt	●				DNS (TOR)
CTB-Locker	●			●	DNS
FAKBEN	●				DNS (TOR)
PayCrypt	●				DNS
KeyRanger	●			●	DNS

Automate Security to Reduce Attack Dwell Time

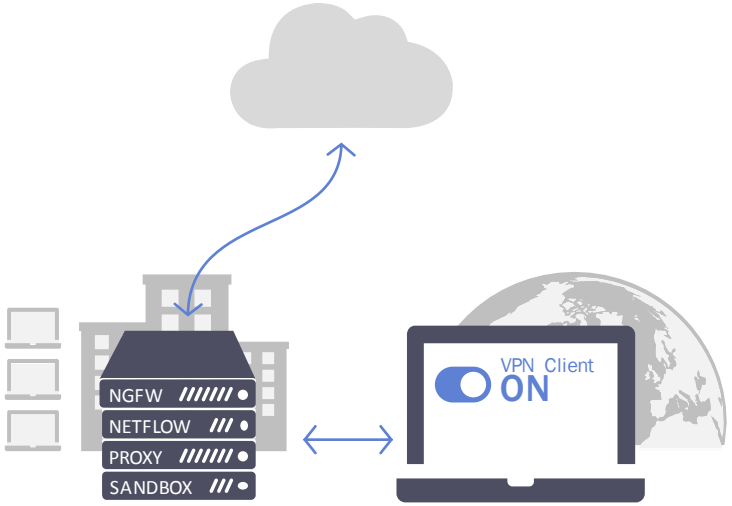


OpenDNS

ON-NET: How We Enforce by Public or Internal Networks

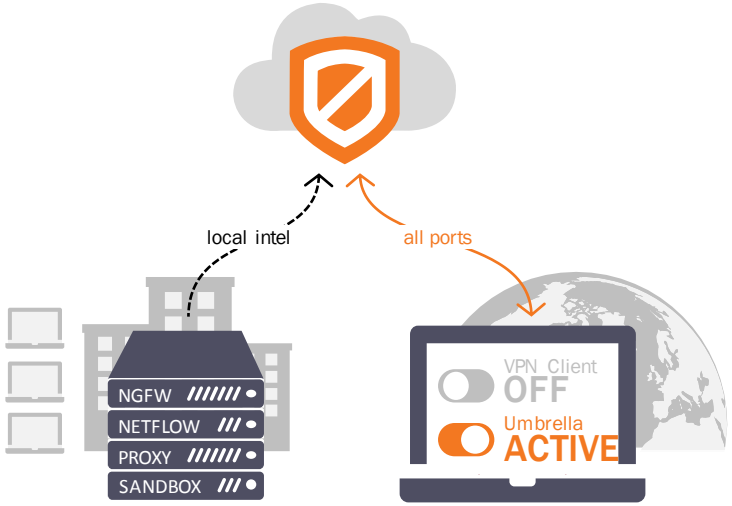


DNS-Layer Network Security Should Protect Any Location



YOU'VE RELIED ON

users requiring remote access into the corporate network to get work done



NEED OFF-NETWORK SECURITY

to protect mobile workers with always-on security and integration w/ your security stack to extend protection

OpenDNS

OpenDNS is
now part of Cisco.