DNS Security

Disrupt attacks with predictive analytics

Name

Title

ATTACKS USING DNS FLY UNDER THE RADAR

DNS is required to run the business

Limited inspection of DNS traffic

DNS is abused for command-and-control and data theft

UNIT 42: ATTACKS USING DNS IN THE SPOTLIGHT

UNIT 42
RESEARCH

80% OF MALWARE

DNS is abused for command-and-control and data theft

RATE OF NEW DOMAINS

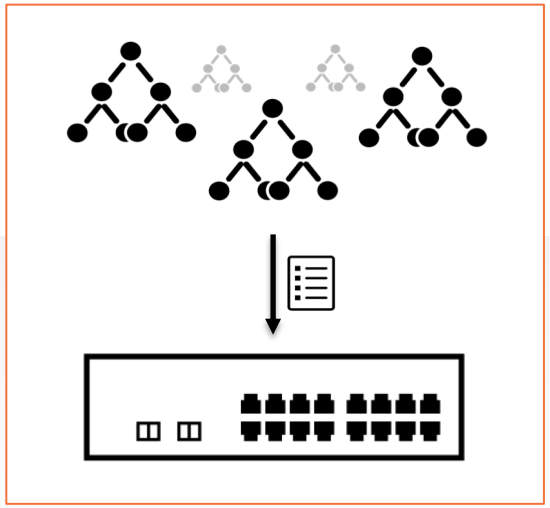
Malware using domain generation algorithms evade detection

OilRig

DNS tunneling

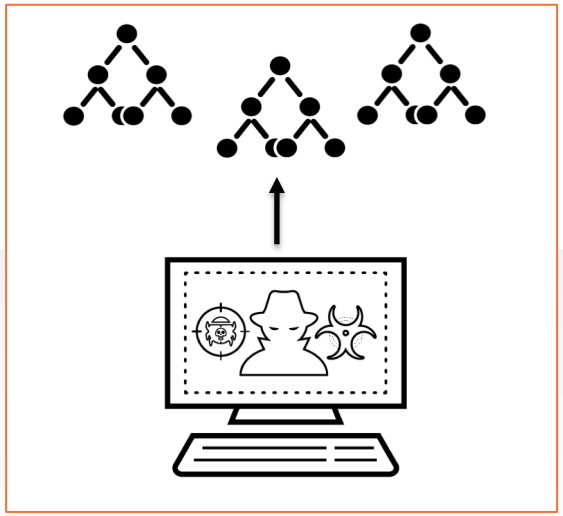
paloalto NETWORKS

CHALLENGES WITH CURRENT APPROACHES



Static lists are slow and do not scale

Analytics is required to predict malicious domains



Manual threat response doesn't scale

DNS SECURITY: DISRUPTING ATTACKS WITH MACHINE LEARNING

Identify new malicious domains

Find DNS-based C2 and neutralize tunneling

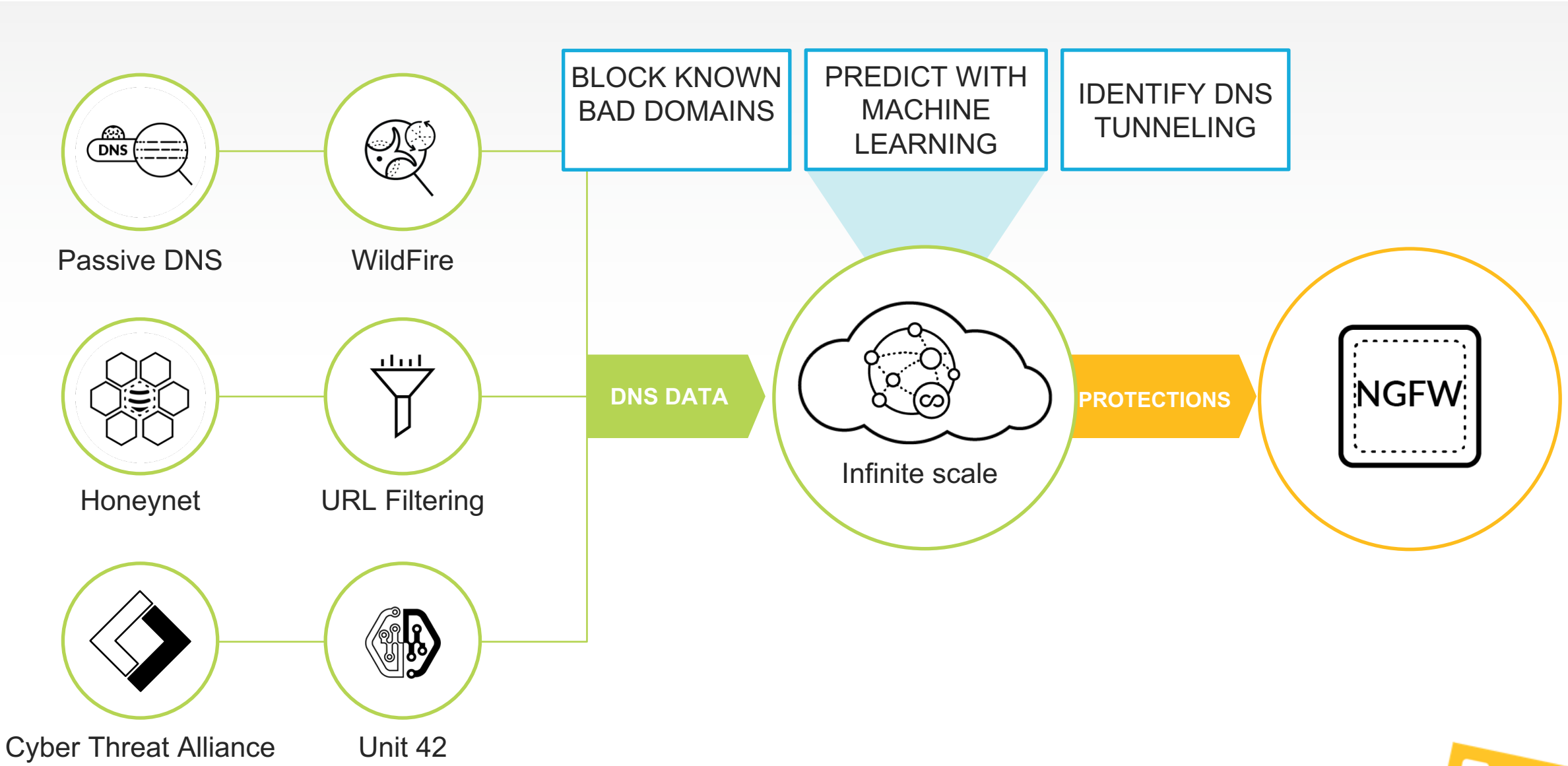
PREDICT WITH MACHINE LEARNING

Stop bad domains and C2

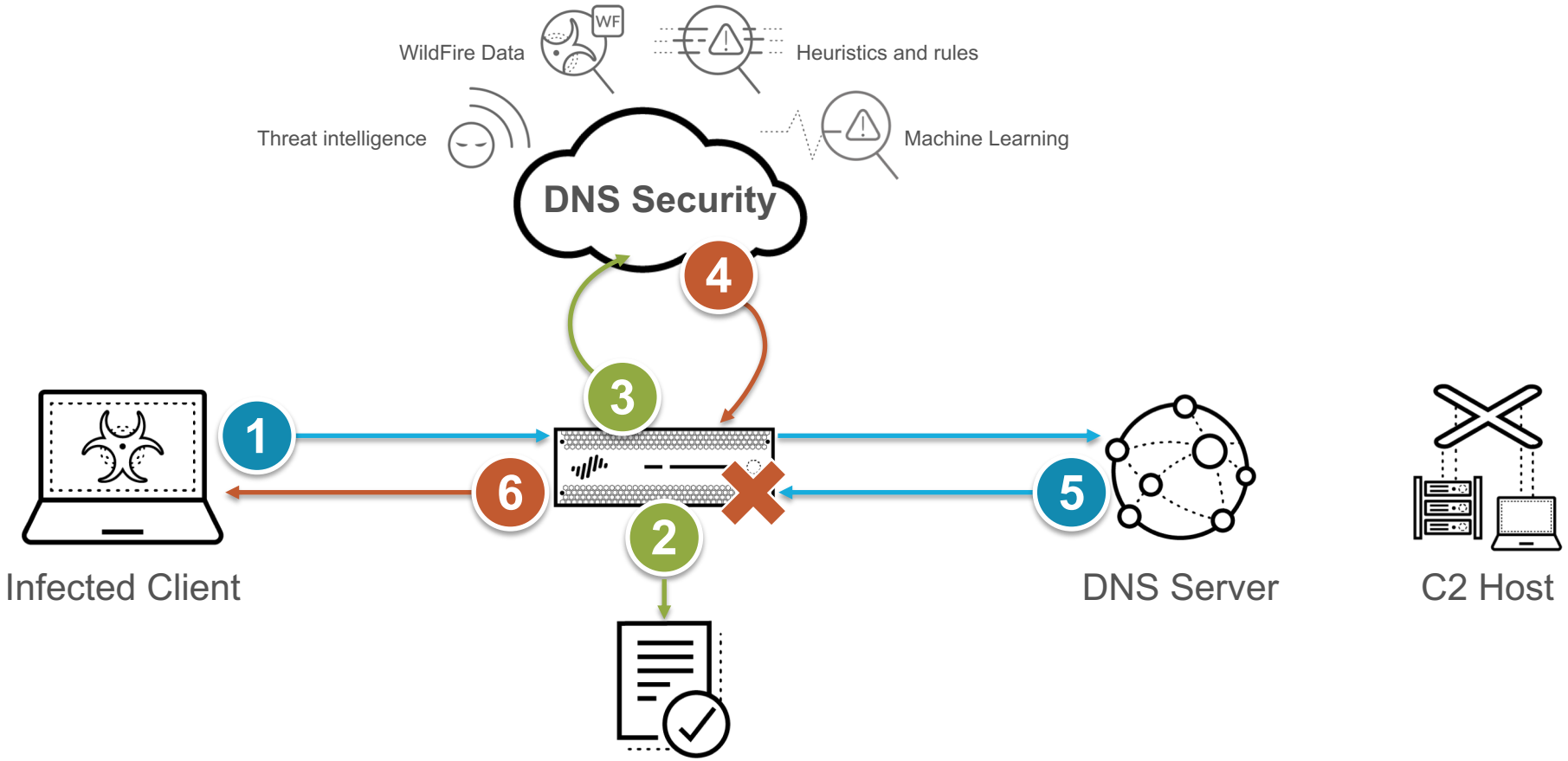
Reveal and contain infected hosts

PREVENT WITH AUTOMATION

RICH DNS DATA POWERS MACHINE LEARNING FOR PROTECTION

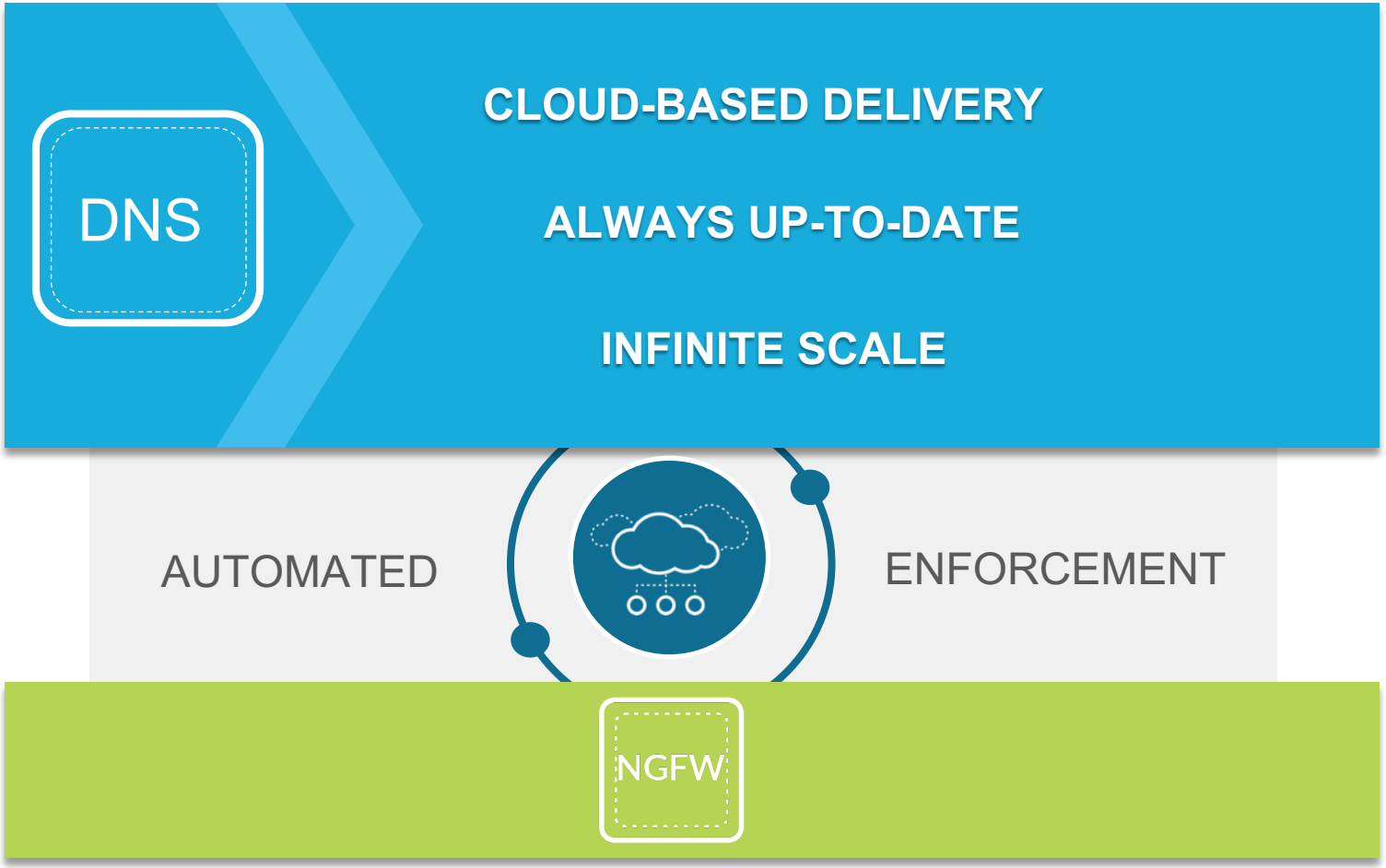


DNS Security service – How it works

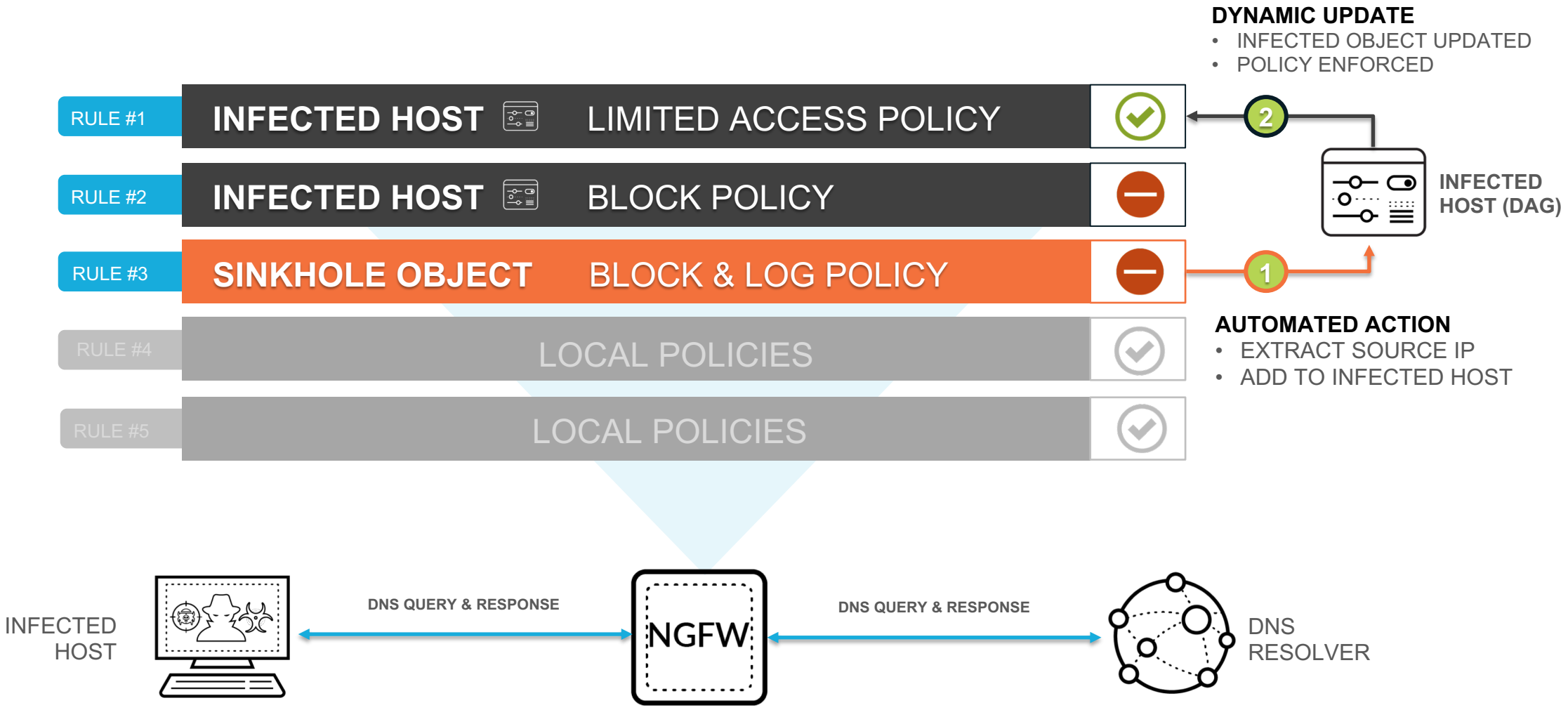


1 *DNS Request* 2 *Local Lookup* 3 *Cloud Lookup* 4 *Cloud Response* 5 *DNS Response* 6 *Enforcement*

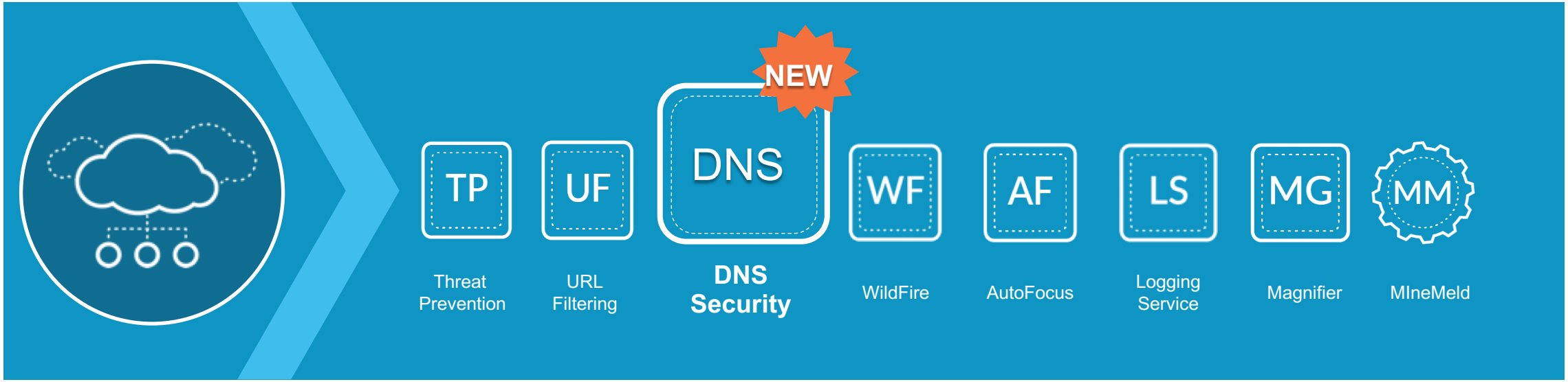
INTEGRATED WITH THE NEXT-GENERATION FIREWALL



DNS SECURITY DRIVES AUTOMATED ACTION



EXTENDING THE NEXT-GENERATION FIREWALL PLATFORM



IPS C2 SIGNATURES	C2 URL FILTERING	AV PROTECTIONS	DOMAIN FILTERING DNS TUNNELING DETECTION DGA PREVENTION

NETWORK SECURITY

THANK YOU