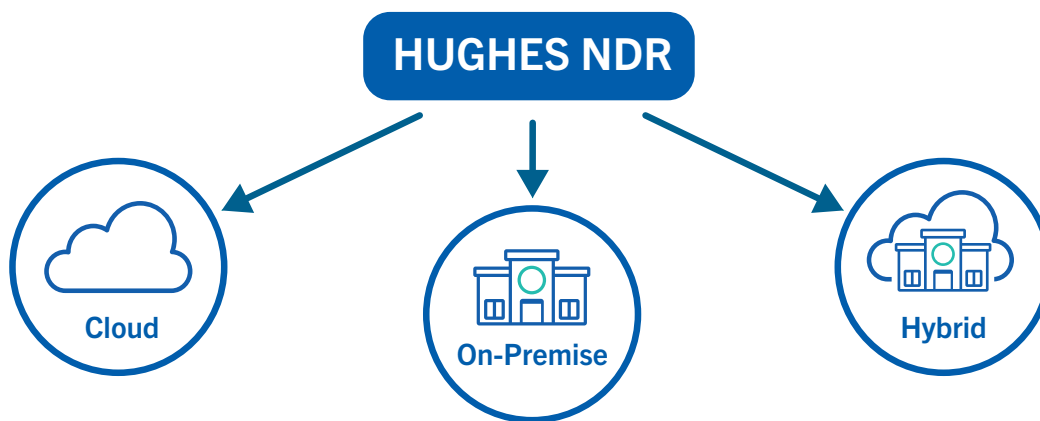


## Cloud Network Detection and Response

The future of NDR is total interoperability. Protection, detection, prediction—anywhere, anytime, with anything.

Hughes Network Detection and Response (NDR), powered by Cynamics, is the only next-generation cloud solution that uses standard sampling protocols and APIs which are built into every network gateway (physical or virtual, legacy or cloud), patented algorithms, AI and ML to provide threat prediction and visibility at speed and scale.

Cloud-Native NDR delivers interoperability with legacy environments for migration, hybrid or complete transition to the cloud. Hughes NDR removes visibility barriers by strengthening network monitoring, detection and prediction capabilities across all environments into a single pane view, accommodating shifting requirements for modern organizations.



### Granular Visibility

Covers complete network across on-premise, VPC and hybrid network environments



### Eliminate Blind Spots

Spotlight hidden threats and suspicious behavior, and mitigates ongoing attacks and activity



### Expose Backdoors

Identify vulnerabilities, intercept malicious activity and keep attackers out for good



### Advanced Detection

Compare historical traffic and trends that detects suspicious patterns and reduces investigation



### Threat Detection

AI technology autonomously learns and discovers hidden patterns preceding attacks

The Hughes NDR Network Blueprint technology collects small network traffic samples from every network gateway or VPC, that uses patented machine learning algorithms and innovative artificial intelligence technologies to provide complete network visibility and threat prediction for complicated networks.

By using small traffic samples, the Hughes NDR solution is fully agnostic to the customer’s network size, scale and architecture which can work for any mix of legacy networks, private clouds, public clouds and hybrid clouds environments.

The Hughes NDR Network Blueprint has the most effective visibility and completely networks a customer’s security posture and detects, predicts and prevents attacks.

By establishing granular unhindered network visibility, organizations can safeguard their environments despite network complexity.

### At a Glance



#### SaaS Based

Fast deployment, intuitive visibility of the network and high availability



#### Cost Efficient

No implementation overhead, no wear and tear and no maintenance overhead



#### Risk Free

No network configuration, appliance-free and agentless



#### Self Managed

Easy onboarding, do-it yourself approach with no training

### Monthly Customer Security Snapshot

#### Discoveries



**19**

major attacks detected



**83**

compromised end points/servers



**21**

data leakages and exfiltrations



**101**

critical vulnerabilities



**20%**

on average faster prediction time



**53**

important backdoors (e.g., ICMP)



**42**

vulnerable protocols in use (e.g., Telnet)



**105**

asset servers with significant attack-surface

For more information, visit [www.hughes.com/NDR](http://www.hughes.com/NDR).