ACHIEVING CYBER HYGIENE
WITH
CLOUD-NATIVE
NETWORK DETECTION & RESPONSE
RISE ABOVE THE NOISE TO SECURE THE HYBRID ENTERPRISE
MEASURING CYBER HYGIENE REQUIRES COMPLETE VISIBILITY
USERS, DEVICES, TRANSACTIONS, CONVERSATIONS, ENCRYPTION, CERTIFICATES, & MORE
NDR IS THE SIGNAL IN THE NOISE
COMPLETE VISIBILITY ACROSS EAST-WEST

- NDR: Network Data
- Cyber Triad: SIEM (Log Files), EDR (Agents)
  - SIEM
  - EDR
- Data Center
- Remote Sites
- Cloud
THE GAP: EAST-WEST ATTACK SURFACE
THE EXPANDING EAST-WEST ATTACK SURFACE

SIEM/EDR
Logs/Agents

NDR
East-West Visibility

W
Users
AD/SSO
Web
Database
Applications
Storage
E
The NIST Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber attacks.

MITRE's ATT&CK, a globally accessible knowledge base of cyber adversary tactics and techniques, is useful for understanding security risk against known adversary behavior, planning security improvements, and verifying that defenses work as expected.

The CIS Critical Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks.
VISIT
WWW.EXTRAHOP.COM/CYBER-HYGIENE
TO LEARN MORE