ExtraHop

ACHIEVING CYBER HYGIENE
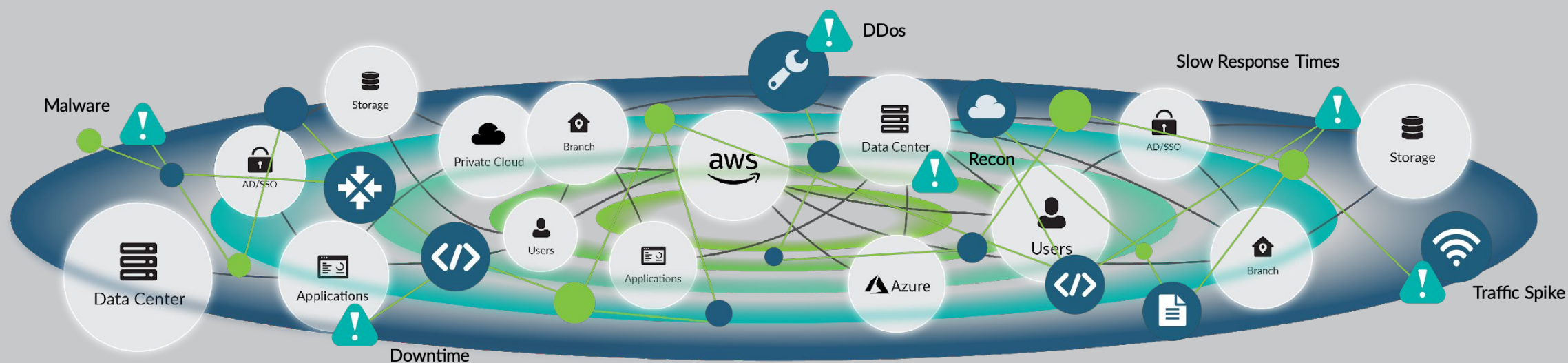
WITH

CLOUD-NATIVE
NETWORK DETECTION & RESPONSE
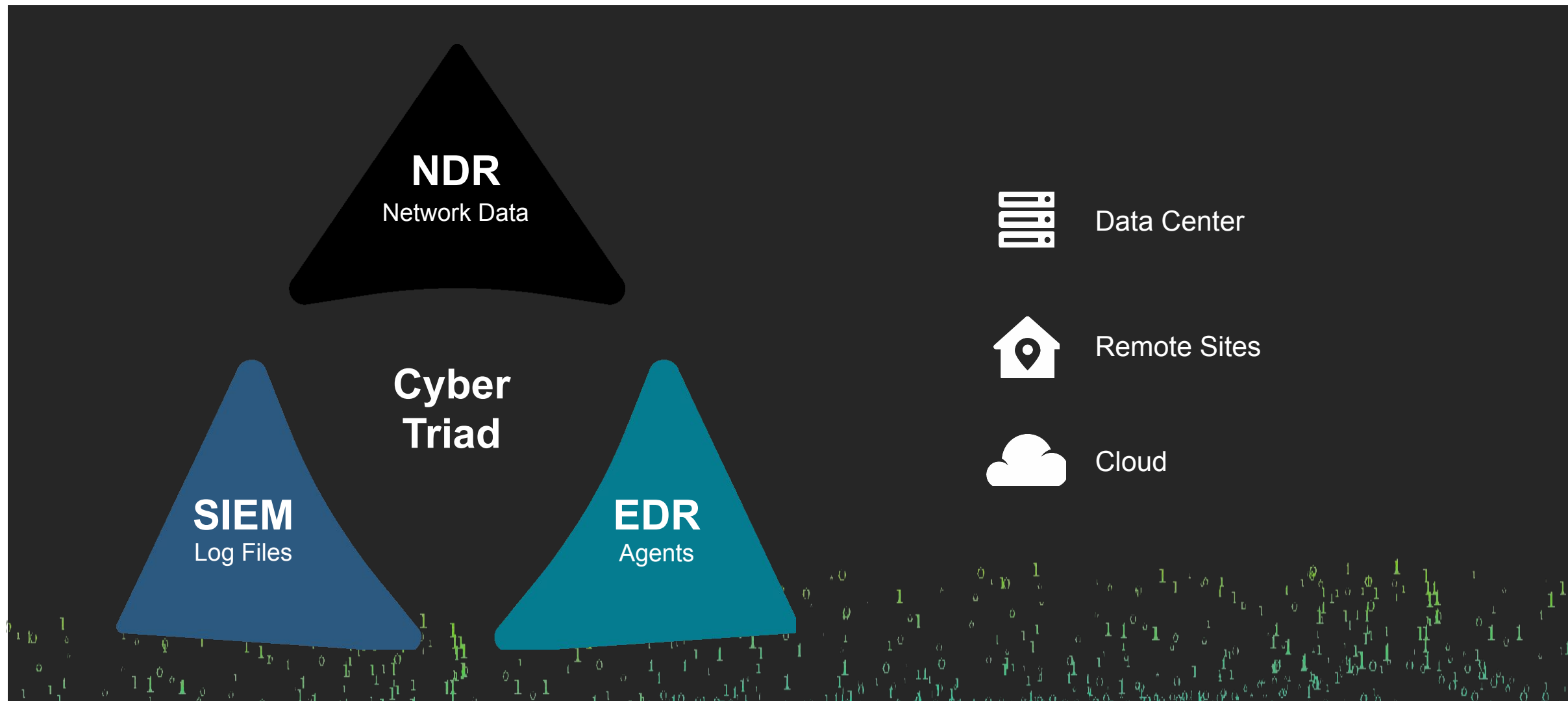
RISE ABOVE THE NOISE TO
SECURE THE HYBRID ENTERPRISE

MEASURING CYBER HYGIENE REQUIRES COMPLETE VISIBILITY
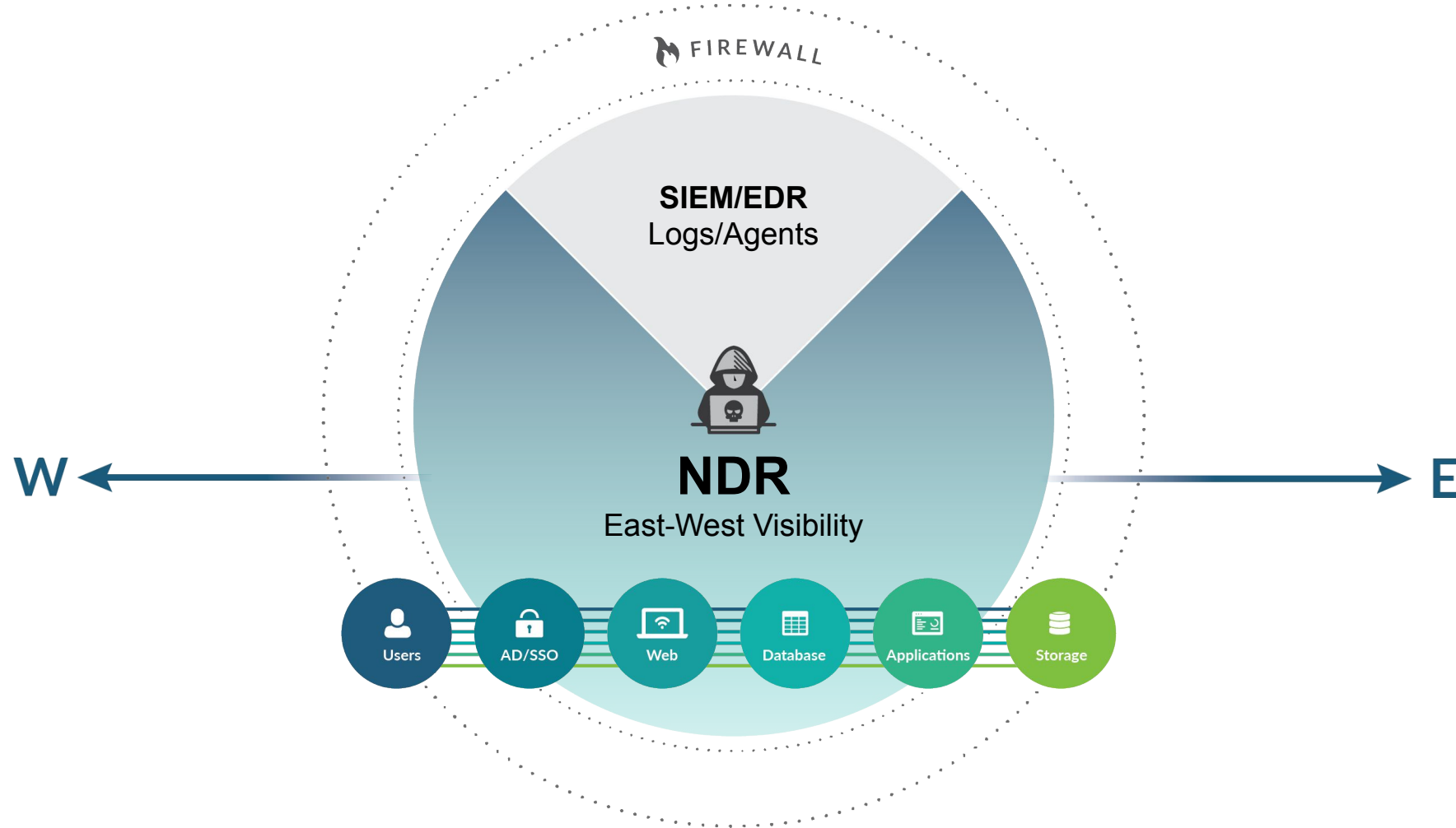## USERS, DEVICES, TRANSACTIONS, CONVERSATIONS, ENCRYPTION, CERTIFICATES, & MORE
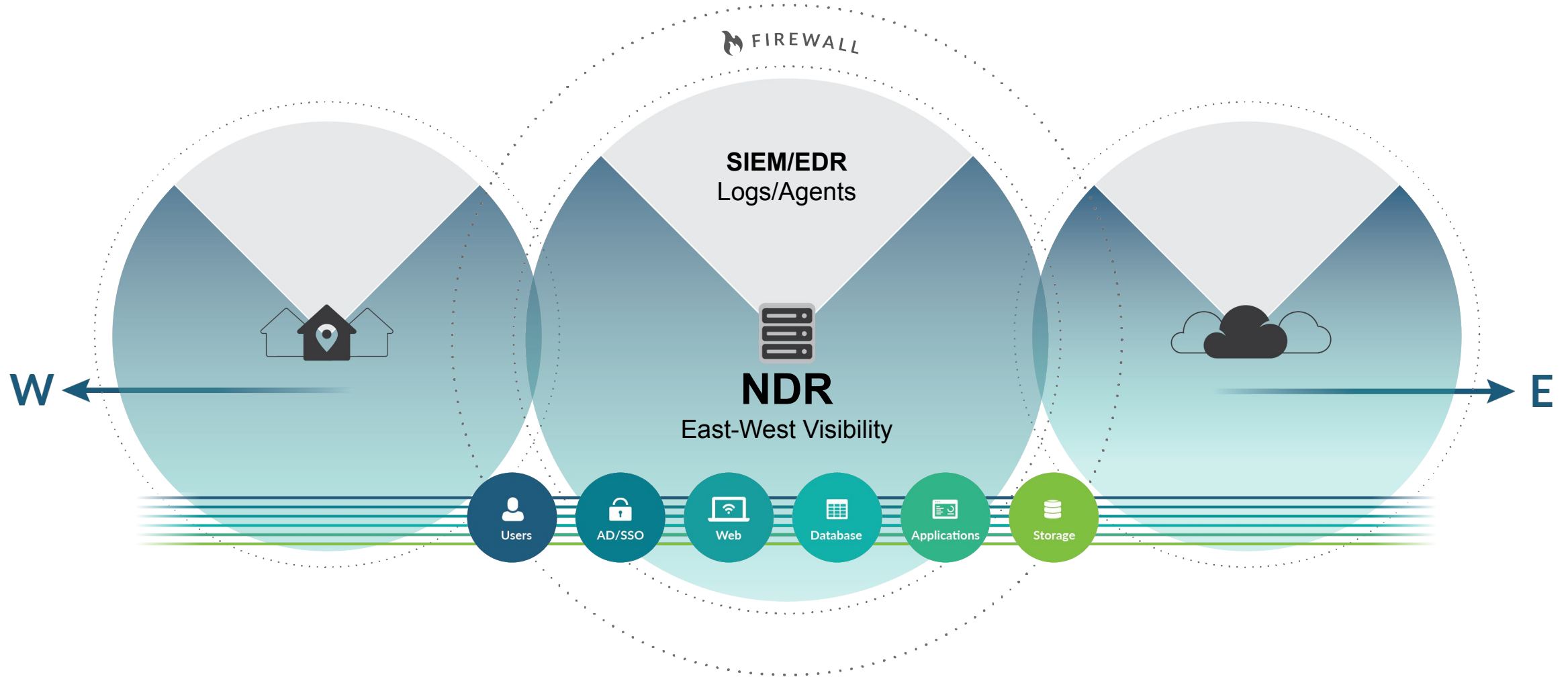
NDR IS THE SIGNAL IN THE NOISE

COMPLETE VISIBILITY ACROSS EAST-WEST

NDR
Network Data

Cyber Triad

SIEM
Log Files

EDR
Agents

Data Center

Remote Sites

Cloud

ExtraHop

THE GAP: EAST-WEST ATTACK SURFACE

FIREWALL

SIEM/EDR
Logs/Agents

NDR
East-West Visibility

W ← → E

Users | AD/SSO | Web | Database | Applications | Storage

ExtraHop

THE EXPANDING EAST-WEST ATTACK SURFACE

FIREWALL

SIEM/EDR
Logs/Agents

NDR
East-West Visibility

W ← → E

Users AD/SSO Web Database Applications Storage

ExtraHop

FRAMEWORKS FOR IDENTIFYING GAPS IN CYBER HYGIENE

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

SECURITY OPERATIONS
HYGIENE AND COMPLIANCE

Analytics and Automation for a Healthier SOC

Automated
Audits, Faster
Investigations,
Easier
Reporting

Saddled with increasingly complicated environments as well as stricter compliance and encryption regulations, SecOps will find it harder and harder to answer questions like, "Which hardware and software assets are using weak ciphersuites?" or "Is that new device on our network doing something malicious and if so, what?" Perimeter and endpoint monitoring can only answer so much, and neither will help you proactively maintain hygiene and compliance at massive scale.

ExtraHop Reveal(x) provides the complete visibility, automated auditing, and guided investigation capabilities that help SecOps teams keep an eye on all the tools and systems at work in their hybrid infrastructures at scale. The industry leader in Network Detection and Response (NDR), Reveal(x) gives you immediate answers to complex questions with zero negative impacts to performance and with far higher fidelity than logs or humans combined.

Improve CIS Top 20
Coverage with
Reveal(x) ⊙

MEET THE FEARLESS

▲ Accolade   WOOD COUNTY HOSPITAL

THE 2019 GARTNER MARKET GUIDE
FOR NETWORK TRAFFIC ANALYSIS

ExtraHop is a Representative Vendor - See Why!

READ IT NOW

ExtraHop

ExtraHop

Rise Above the Noise.