ankura InterXeptor

DATA SHEET

Ankura InterXeptor™: Managed Detection and Response Solution

EXPERT LED. TECHNOLOGY AGNOSTIC.

We protect your business by detecting and responding to cyber threats every minute, every hour, every day. Ankura InterXeptor's combination of industry-best technology and human expertise will defend your infrastructure whether it's on-site, in the cloud, or in-between.

Ankura InterXeptor Provides the Best Defense Against:

- Ransomware attacks
- Compromised credentials incidents
- Advanced intrusions
- Business email compromise
- Data exfiltration
- Newly created spoofed domains
- Malware communicating within your infrastructure

Prevention is Ideal…But Detection is a Must

Ankura InterXeptor provides:

- Advanced network traffic analysis using advanced intrusion detection technology
- Live endpoint threat detection analysis and real-time response
- Fully managed XDR platform event correlation and behavioral analytics
- Cloud telemetry monitoring and anomalous activity detection
- Context and issue prioritization derived from proprietary threat intelligence

10+ Years of Experience:

24/7	Global Threat Detection Operations Team; Dedicated Detection Engineering Team
100+	Cyber and Data Privacy Specialists Globally
1 Million+	Endpoints Monitored
70,000+	Consecutive Hours of Threat Monitoring
Billions	of Security Events Analyzed Weekly
10,000+	Threats Identified and Neutralized
4,000+	Cyber Incident Response Engagements

OPTIMIZE → **FILL** → **MONITOR** → **DETECT** → **RESPOND**

YOUR EXISTING SECURITY INVESTMENTS AND CONTROLS

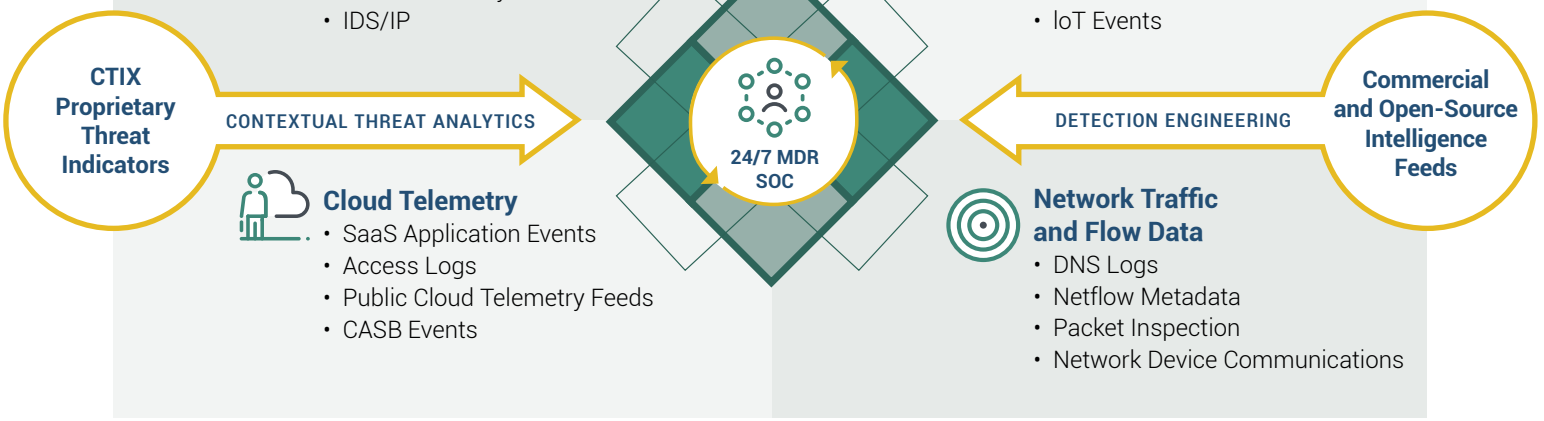
MONITORING COVERAGE GAPS with XDR tools and expertise to maximize visibility inside network perimeter and endpoints

CORRELATED SECURITY TELEMETRIES in your environment 24/7 to understand your normal state and detect any suspicious anomalies

THREATS EARLIER that evade perimeter security devices and controls

TO LIVE ATTACKS IN REAL-TIME with IR support from trained investigators and forensic pros

Detection Telemetry Diamond



Managed XDR

Ankura InterXeptor | Continuous threat detection. Real-time response.

Ankura InterXeptor Endpoint

- ✓ 24/7 Endpoint Detection and Response (EDR) Service
- ✓ Threat and compromise hunting using behavior-based methodology
- ✓ AI-driven, next generation antivirus (NGAV) protection
- ✓ Cyber attack visualization with easy-to-follow attack chain
- ✓ Cyber attack root cause analysis
- ✓ Real-time threat suppression and live response
- ✓ Continuous analysis of indicators:
  - File modifications
  - Cross-process events
  - File executions
  - Network connections
  - Registry modifications
- ✓ Threat intelligence feed reporting and alerting

Ankura InterXeptor Complete

Ankura InterXeptor Endpoint Service **PLUS:**

- ✓ 24/7 Extended Detection and Response (XDR) Service
- ✓ Comprehensive infrastructure threat detection to include monitoring of key telemetry sources
  - Firewalls
  - Authentication events
  - VPN and remote access logs
  - Proxy server logs
  - User behavior analytics and DLP logs
- ✓ Advanced Network Traffic Analysis
  - Packet inspection
  - Network intrusion detection
  - Netflow recording
  - Passive asset detection and logging
  - Passive DNS response logging
  - Log storage and file extraction
- ✓ Continuous monitoring of indicators of compromise associated with SaaS applications including:
  - Bypass of security measures (MFA, SSO)
  - Anomalous log-in activity
  - Session hijacking
  - Anomalous data/file access and transfer
  - Anomalous account creation/deletion

For more information, contact: Andy Mercer at Andy.Mercer@ankura.com