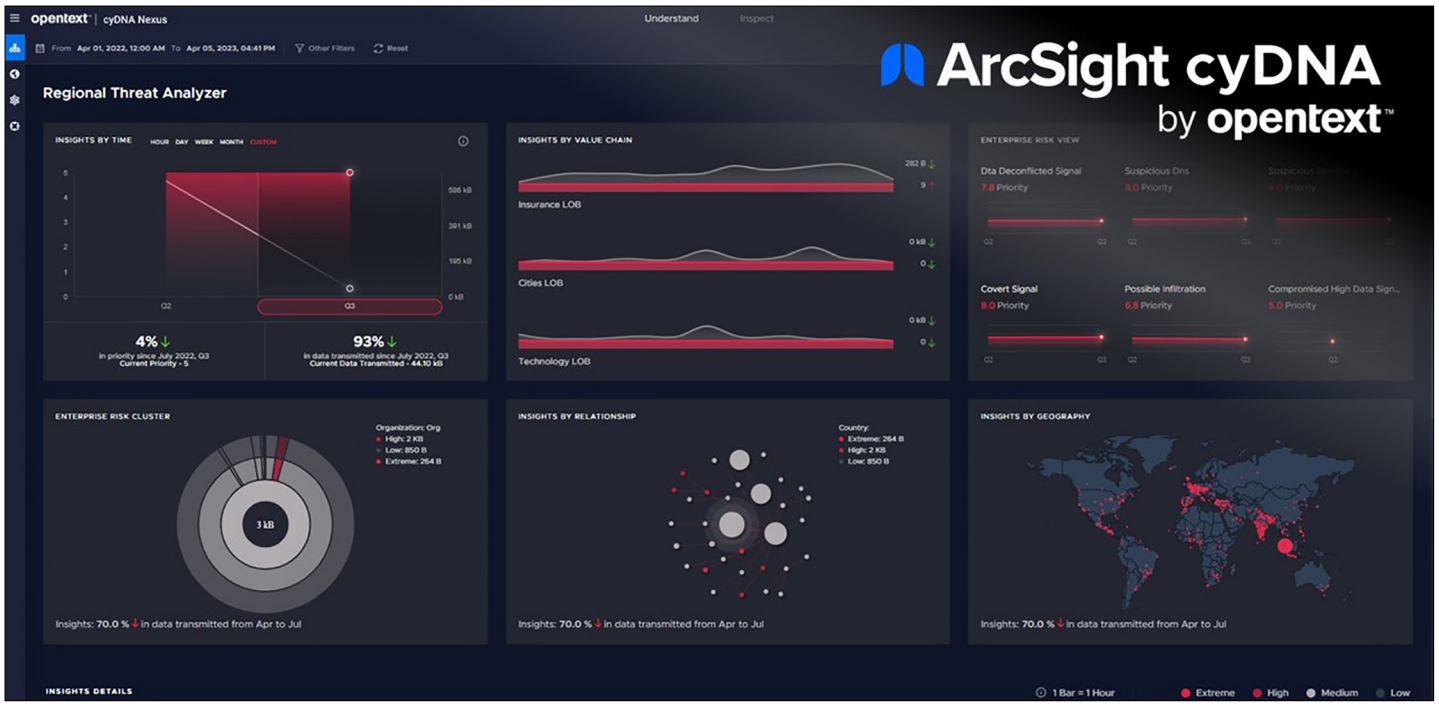
opentext™ | Cybersecurity

Data Sheet

ArcSight cyDNA

SaaS-based global signal analytics to discover, define, and contextualize threats.



Product Overview

ArcSight cyDNA by OpenText™ is a SaaS-based global signal analytics technology that discovers malicious traffic, defines digital genealogies, and monitors against future attacks. It unmasks adversarial behavior, discovers early signs of attacks and outlines sophisticated attack paths. It bolsters resilient defenses with insights derived from internet traffic, indicating the *intent* of activity in your network. It looks beyond the borders of your organization to provide a holistic view of threat actors attempting (sometimes successfully) to infiltrate your defenses.

cyDNA provides your organization with a bird's eye view of the divisions being targeted and how malicious attacks are being carried out. While similar to attack surface management, which provides a "what could happen" overview, the signals-based analytics of cyDNA provide a "what *is* happening" report that includes how the organization is being targeted, and how your attack surface is being used in attacks.

Threat intelligence is an essential part of any adaptive security program, and cyDNA was built to consume, cross-verify, and

Key Benefits

- Multi-Space Analysis
- Threat Actor Attribution
- Adversarial Activity Mapping

Key Features

- SaaS-Based Deployment
- Adversary Signals Analytics
- Optimized Incident Response
- Cross-Agency Models

interoperate with existing standards-based solutions. cyDNA's added value is that it provides visibility with signals intelligence and provides near-time threat analysis of those signals.

Key Benefits

Multi-Space Analysis
cyDNA offers insights beyond traditional "near space" models like SIEM, MDR and XDR. It extends your reach beyond the borders of the organization to find key insights with multi-space analysis. Machine learning and advanced analysis techniques help determine the intent of scanning activities directed at your organization.

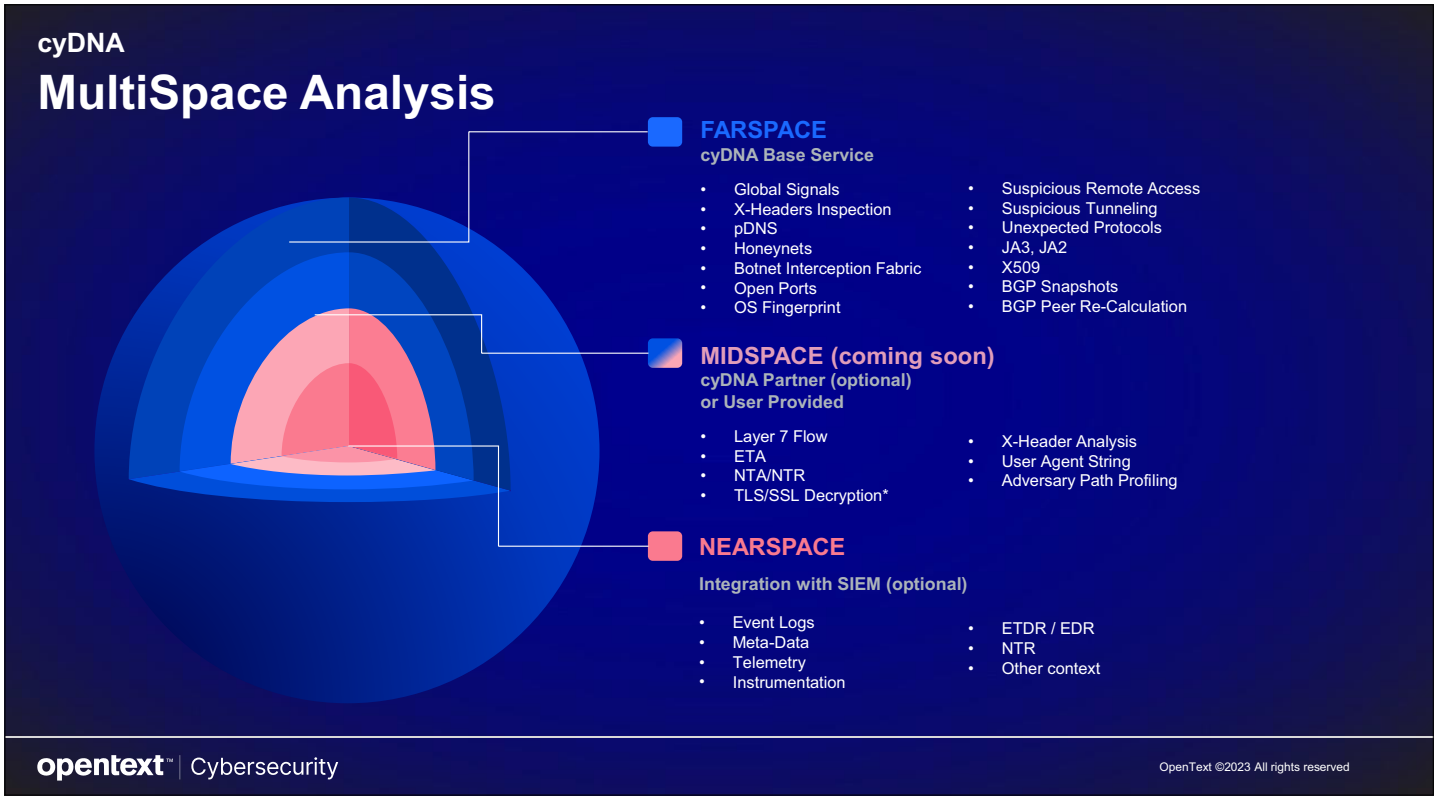
Multi-space analysis utilizes existing security infrastructure to identify common threats across multiple branches of the organization, and de-conflicts threats across non-targeted baselines.

Threat Actor Attribution
Track threats beyond the borders of your security environment to uncover who is attacking and begin understanding *why*. cyDNA's enhanced threat actor attribution lets you see beyond digital disguises and uncover the origin of malicious activity. A signals-based analysis provides enhanced details for context, attack techniques, and actor motivations to build accurate adversary profiles.

Adversarial Activity Mapping
Get a bird's eye view of malicious activity targeting your network with adversarial activity mapping. cyDNA identifies the resources and techniques of known adversaries by employing a broad collection of global threat intelligence insights. Malicious actors are investigated and monitored, their global activities catalogued, which consequently provides opportunities to block breaches before they occur.

Key Features

SaaS-Based Deployment
cyDNA can be deployed without the need for additional hardware and requires minimal effort for integration. It is delivered as a plug-and-play SaaS service, with tailored threat intelligence based on each environment's unique set of incoming and outgoing internet signals. cyDNA easily co-exists with existing security investments, and raises the ROI of SIEM, XDR, MDR, and more. It helps reduce blind spots of traditional SOC tools and amplifies the effectiveness of security operations as a whole.



Connect with Us
www.CyberRes.com

Adversary Signal Analytics
cyDNA provides advanced analytics of malicious internet signals. In its simplest deployment, signals-based analytics do not require additional infrastructure deployment, or ingestion of log files to deliver targeted and accurate results. The capability to remove noise by "deconflicting entities" filters out broad threats observed elsewhere in the world and provides a more precise view of the attacks specific to your environment. cyDNA can distinguish between attacks targeted at your organization versus broad-level campaigns by deconflicting baseline attacks on relevant industries and regions. This approach minimizes false positives that waste time and resources, which helps prioritize threats specifically targeting your network.

- Near-time detection
- Internet signals rather than log files
- Minimize false-positives

Optimized Incident Response
cyDNA provides automated countermeasures and defensive capabilities based on the characteristics of identified threats. This can be mapped to the Galaxy Online platform for additional integrated guidance. The cyDNA solution includes the capability to prioritize and implement countermeasures based on early-warning risk and threat signals. This accelerates the development of overall threat readiness and response.

Cross-Agency Models
Security analytics across multiple agencies can play a crucial role in validating findings and enhancing the accuracy of threat assessments. ArcSight cyDNA combines and cross-references internet signals, patterns, and indicators of compromise, allowing agencies to identify commonalities and corroborate findings, strengthening the validity of their assessments. This multidimensional approach helps identify blind spots, uncover hidden connections, and reduce false positives for the organization overall.

Learn More

Learn more about cyDNA and request a demo at: **www.arcsight.com**

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.