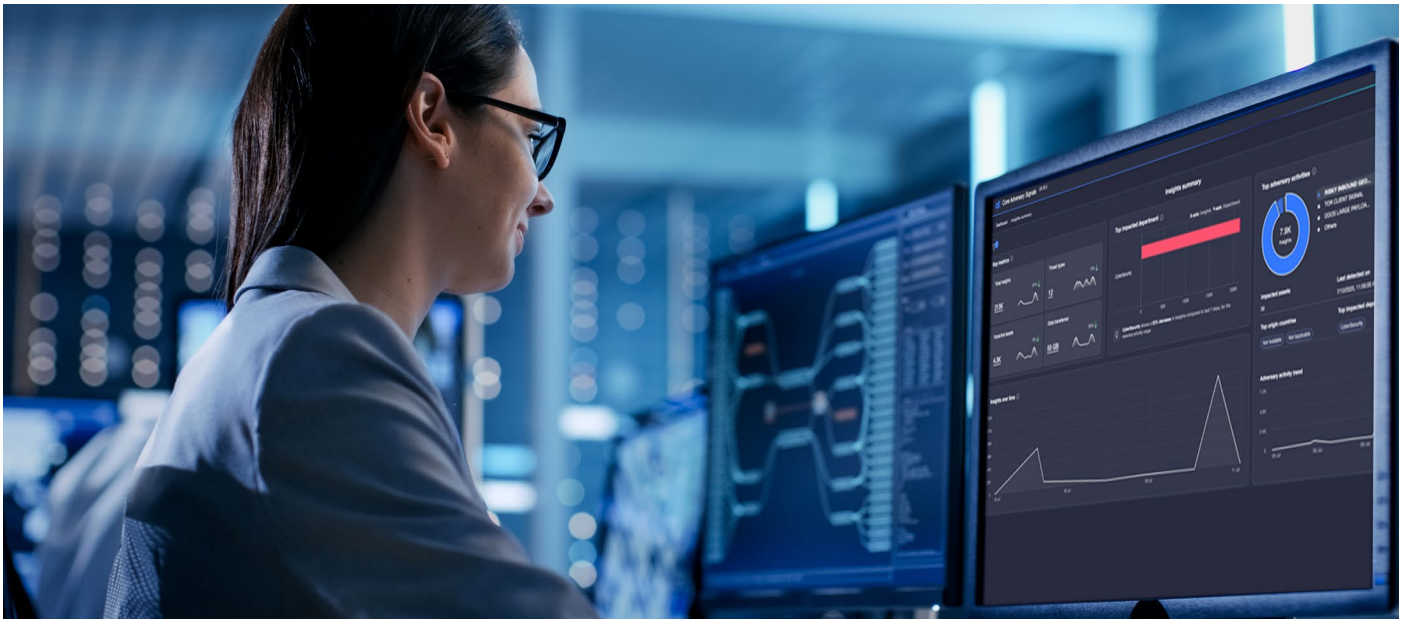
OpenText Core Adversary Signals

Discover, define, and contextualize cyberthreats with SaaS-based global signal analytics



Benefits

- Detect threats earlier with a precise view of global signals directed at your organization
- See beyond digital disguises to identify threat actors and monitor their activity
- Reduce costs through fast, zero-touch SaaS deployment
- Optimize response with tailored insights and automated countermeasures

Sophisticated threat actors attacking large organizations know how to disguise their identities and leverage complex networks to conceal their activity and intended targets. Traditional security measures often fall prey to these tactics by focusing on “NearSpace” monitoring, leaving a notable gap by overlooking the crucial “FarSpace.” Without relevant, actionable insight into threats and their signal activity, protecting critical assets becomes a guessing game.

OpenText™ Core Adversary Signals is a SaaS-based global signal analytics technology that discovers malicious internet traffic relevant to your organization, defines the digital genealogies of your attackers, and monitors against future attacks. It unmasks adversarial behavior, seeing past digital disguises and identifying early signs of attacks against your organization while outlining sophisticated attack paths. Using insights derived from internet traffic, it provides your organization with relevant and actionable intelligence about the activity affecting your network.

While similar to attack surface management, which provides a “what could happen” overview, the signals-based analytics of OpenText Core Adversary Signals instead provide a report of “what has happened” and “what is happening.” The solution looks beyond the borders of your organization, into global internet signals, known as the FarSpace, to provide a holistic view of divisions being targeted and how threat actors’ malicious attacks are being carried out across your attack surface.

Detect threats earlier with a precise view of global signals directed at your organization

OpenText Core Adversary Signals offers insights beyond traditional NearSpace models like SIEM, MDR, and XDR. It extends your reach beyond the borders of the organization to find key insights in global internet signals.

In its simplest deployment, OpenText Core Adversary Signals does not require additional infrastructure deployment or ingestion of log files to deliver targeted and accurate results. It runs machine-aided adversary analytics on global signals entering and exiting a user-defined “covered space” to help you determine the intent of scanning activities directed at your organization. It can then remove noise through “deconflicting entities,” filtering out broad threats observed elsewhere in the world to provide a more precise view of the attacks specific to your environment.

By integrating with your existing security infrastructure, OpenText Core Adversary Signals can then combine NearSpace and FarSpace data to provide “MultiSpace” analysis for enhanced insight into malicious signals and threats across multiple branches of your organization.

See beyond digital disguises to identify threat actors and monitor their activity

Uncover who is attacking you and get a bird’s eye view of malicious activity targeting your network with threat actor attribution and adversarial activity mapping. OpenText Core Adversary Signals lets you uncover the origin of malicious activity and provides enhanced details for context, attack techniques, and actor motivations to build accurate adversary profiles. A broad collection of global threat intelligence insights helps identify resources and techniques of known adversaries. Malicious actors are investigated and monitored, with their global activities cataloged, providing you with opportunities to block breaches before they occur.

Reduce costs through fast zero-touch SaaS deployment

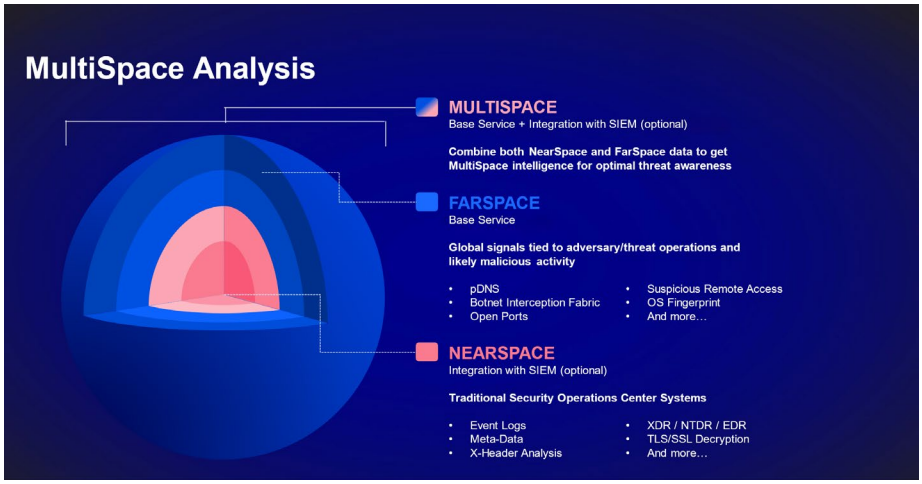
OpenText Core Adversary Signals can be deployed without additional hardware and requires only minimal effort for integration. It is delivered as a plug-and-play SaaS service, with tailored threat intelligence based on each environment’s unique set of incoming and outgoing internet signals. The solution easily co-exists with other security infrastructure and raises the ROI of SIEM, XDR, MDR, and more. It helps reduce the blind spots of traditional SOC tools and amplifies the effectiveness of security operations.

Optimize response with tailored insights and automated countermeasures

OpenText Core Adversary Signals provides automated countermeasures and defensive capabilities based on the characteristics of identified threats. This can also be mapped to the ThreatHub Research platform for additional integrated guidance. The solution can prioritize and implement countermeasures based on early-warning risk and threat signals. This accelerates the development of overall threat readiness and response.

By providing insights into malicious internet signals, OpenText Core Adversary Signals offers a unique perspective into ongoing attacks, enabling organizations to understand precisely what is happening and how theyare being targeted. Through advanced FarSpace analytics, backed by deconfliction filters, OpenText Core Adversary Signals equips you with relevant and actionable insights customized to your organization’s unique network so you can detect threats earlier and mitigate risks effectively.

With OpenText Core Adversary Signals, organizations can evolve beyond reactive NearSpace security operations to proactively discover, define, and contextualize cyberthreats in the FarSpace with global signal analytics.



Understanding MultiSpace Analysis with OpenText Core Adversary Signals

OpenText Core Adversary Signals features	
FarSpace Analysis	Look beyond your digital borders with global signal analytics that leverage machine models to analyze malicious internet signals directed at your organization to determine how and where you're being targeted.
MultiSpace Analysis	Integrate OpenText Core Adversary Signals with your existing security infrastructure to combine your NearSpace and FarSpace data for analysis that identifies common threats across multiple branches.
Deconfliction Threat Analysis	Filter out noise and provide precise views of attacks specific to your environment, distinguishing between targeted attacks and broad-level campaigns.
Threat Actor Attribution	Gain insights into the origins of malicious activity with enhanced threat actor attribution that sees past digital disguises to provide valuable context for building accurate adversary profiles.
Adversarial Activity Mapping	Identify known adversaries' resources and techniques while cataloging their global activities to help block breaches before they occur.
Optimized Incident Response	Prioritize and implement response with automated countermeasures based on identified threats for enhanced readiness.
Cross-Agency Models	Combine and cross-reference signals, patterns, and indicators of compromise across multiple agencies to corroborate findings and uncover blind spots, commonalities, and hidden connections.
SaaS-based Deployment	Deploy OpenText Core Adversary Signals effortlessly as a plug-and-play SaaS service.

Resources

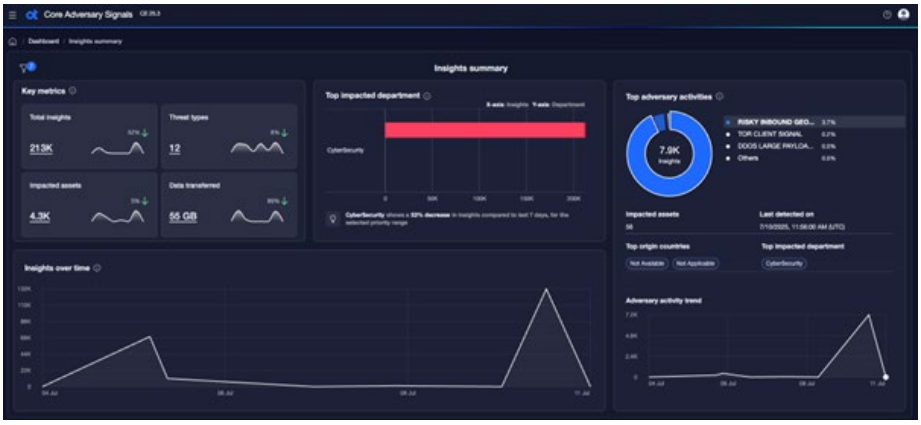
Learn more ›

Watch the intro video ›

OpenText Core Adversary Signals for government ›

OpenText Core Adversary Signals for energy and utilities ›

Keep up to date ›



Executive dashboard highlights key threat insights with easy drill-downs for details.