

Cybersecurity:

Discover and stop threats faster to protect the confidentiality, integrity and availability of critical business data and systems



Cray for Cybersecurity

Security threats can originate both inside and outside an organization, so Cray offers solutions that help organizations detect internal and external threats faster. Our analytics platform gives security analysts a **secure, flexible and open solution** that's ready in days, for issues ranging from fraud detection and anti-money laundering in banking to precision medicine and disease prevention in healthcare and life sciences. And Deloitte Advisory's Advanced Cyber Reconnaissance services, powered by Cray, lets clients analyze their vulnerability footprint from an adversary's perspective, for proactive detection and efficient mitigation of cyberthreats.

TECHNICAL CHALLENGE:

THREAT SOPHISTICATION AND EVOLUTION

The proliferation of cyberthreat volume, tradecraft, talent and opportunity can be overwhelming for organizations trying to secure sensitive data and critical systems. By some estimates, nearly 400 new threats happen each minute, 70 percent of which go undetected¹. Additionally, an ever-increasing volume of data now comes in faster than it can be analyzed — so analysts are forced to pick a subset and apply only a limited range of analyses, hoping they don't miss the signs of a new attack.

Legacy security solutions are capable of identifying obvious threats, but attack methods are constantly morphing and evolving. Finding patterns that could indicate risk requires skill and perseverance, and analysts must run a variety of analytics against as many data sources as possible (e.g., NetFlow, DNS, IDS and firewall records) to filter normal traffic and identify the anomalies. In addition, attackers' methods and tradecraft are becoming more complex, and more attackers than ever are developing highly capable resources and capabilities.

Businesses cannot afford to ignore the probability they will be targeted for attack from inside or outside their organization. But while we can't impact adversaries' tradecraft, skills and intentions, we can minimize their opportunity for exploitation.

BUSINESS SOLUTION:

AGILE ANALYTICS DECREASES ATTACK OPPORTUNITIES

How can attackers' opportunities be limited? By equipping analysts with the ability to perform a more comprehensive range of analytics — including both ad-hoc searches for relationship patterns and real-time analytics on streaming network data to iteratively find and isolate suspicious activity as fast as possible.

Cray® Urika®-GX system benefits for cybersecurity:

- Decreased mean time to detection for cyberthreats
- Improved threat visibility responsiveness
- Reduced false positives for better analyst productivity
- Improved detection accuracy
- Increased analytical agility and adaptability to prepare for future demands

For details on Cray for cybersecurity, [click here.](#)

REQUIREMENTS TO SUPPORT A MORE EFFECTIVE CYBERANALYTICS APPROACH:

- **Hardware** that can accommodate massive amounts of data in memory
- **Software** that can flexibly link data from multiple sources, supporting data analysis including both Hadoop® and Spark™ workloads and ad-hoc queries on massive unstructured data for which graph databases are ideally suited
- **System speed** to return reliable results in minutes or seconds

Users should never compromise on speed – it provides a vital advantage. When results are delivered immediately, cybersecurity analysts can better understand what to do next, refine analytics more effectively and take action in time to prevent damage

CRAY CYBERSECURITY:

COMPREHENSIVE ANALYTICS FOR 360° DETECTION

Internal Threat Detection:

Cray cybersecurity solutions close the door on both internal and external security threats. The Urika®-GX solution provides an agile analytics platform with an unprecedented combination of versatility and speed. With Urika-GX, analysts can detect cyberattacks in real time and quickly remediate threats to the confidentiality, integrity and availability of critical business data and systems.

“Cray is closing the gap, bringing ‘supercomputing’ capabilities to big data and analytics in the enterprise.”

**Nik Rouda, Senior Analyst,
Enterprise Strategy Group**

The Urika-GX solution for cybersecurity combines the fast implementation and easy support of an appliance with the complete control and customization capabilities of an in-house solution. With the Urika-GX system, users can:

- Gain the deep, near-real-time insights needed to pinpoint external and internal threats and take action in the shortest possible timeframe
- Improve the performance of graph analytics problems by several orders of magnitude over commodity hardware
- Enable ad-hoc searches for relationship patterns (graph databases are ideally suited for this purpose)
- Enable continuous updates to the graph as new data streams in
- Leverage activities an adversary cannot prepare for – such as complex, empirical analysis on massive graphs (in other words, give network defense operators the advantage)
- Gain the skills of an experienced partner that knows how to improve your security posture

External Threat Detection:

Evaluating a business from the outside to pinpoint security vulnerabilities is a key element to any comprehensive security strategy. Cray provides the platform to speed and streamline the data analytics process for external threat detection.

“With Cray as part of our Cyber Reconnaissance solutions, we utilize graph analytics to identify relationships and look for behaviors versus querying for a known signature, allowing our clients richer insight into present or emerging threats.”

**Gordon Hannah, Principal
Deloitte & Touche LLP**

The Urika-GX platform provides the engine for threat detection systems to help organizations effectively identify, understand and take action against adversaries. With Urika-GX, analysts can increase the volume of analyzed data and applying advanced analytics, so clients gain a clearer view of true risk, exposure and malicious activity.

For example, Deloitte Advisory offers a cyber reconnaissance solution that evaluates an organization's security profile from the perspective of an attacker. Powered by the Urika-GX platform, this offering identifies likely weaknesses, vulnerabilities, openings, activity and nodes that contain risks and anomalous activity to the enterprise.

INDUSTRY SOLUTIONS

From science to banking, cybersecurity and threat remediation is a reality that Cray helps businesses face with success:

- In **healthcare**, hospitals, insurance companies and service providers can better protect confidential patient data and reduce the risk of a breach while ensuring regulatory compliance
- **Financial services** firms can improve accuracy and responsiveness to issues like anti-money laundering (AML), insider threat and fraud or trader surveillance
- Global **manufacturers** operating complex design and supply chain organizations can more quickly find anomalous activity and rule out false positives faster. Uncovering security breaches also prevents or minimizes the loss of intellectual property
- **Oil & gas** production companies and refineries can quickly detect threats to Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems

Why Urika-GX:

- Single, unified hardware-software solution that's ready in days
- Run Hadoop®, Spark™ and graph concurrently
- On-node memory to accelerate results
- Cray Aries™ interconnect for the fastest available in-memory analytics
- Cray Graph Engine integrated and tuned for complex pattern matching
- Open framework can integrate new technologies as they emerge



For more information on the Urika-GX platform, [click here.](#)



GETTING STARTED

- **Read more about Urika-GX for cybersecurity:** Find out why Cray's agile analytics solution is well suited to both internal and external threat detection
- **Request a private briefing:** Our cybersecurity experts can provide additional details on the capabilities of Cray's analytics systems and answer questions about how they can be deployed in your environment
- **Watch an informational webinar:** Learn about the need for agile analytics in this Cray webinar featuring Forrester Research
- **Request a quote:** Contact Cray for pricing information for an on-premise Urika-GX system



GLOBAL HEADQUARTERS

901 Fifth Avenue, Suite 1000
Seattle, WA 98164
Phone: 206-701-2000
Fax: 206-701-2500

Contact info:

EMEA HEADQUARTERS

Broad Quay House
Prince Street
Bristol BS1 4DJ
United Kingdom
Phone: +44 117 992 6790
Fax: +44 117 925 8617

APAC HEADQUARTERS

Suite 12, 24 Lakeside Drive
Burwood East, Victoria 3151
Australia
Phone: +61 3 9298 1800
Fax: +61 3 9886 4674

JAPAN HEADQUARTERS

15F Hibiya Daibiru
1-2-2, Uchisaiwai-Cho
Chiyoda-ku
Tokyo 100-0011, Japan
Phone: +81-3-3503-0901
Fax: +81-3-3503-0905

For more information about Deloitte Advisory's Cyber Reconnaissance service, please contact Gordon Hannah – ghannah@deloitte.com

References

¹ <http://blogs.barrons.com/focusonfunds/2015/09/08/americans-worry-about-falling-victim-to-cyberattacks-more-than-any-other-type-of-crime/>

² Gartner 2014; based on revenue

About Cray

Global supercomputing leader Cray Inc. (NASDAQ: CRAY) provides innovative systems and solutions enabling scientists and engineers in industry, academia and government to meet existing and future simulation and analytics challenges. More information is available at www.cray.com.