Cybersecurity

Resources to develop and
deliver solutions

The Business Problem

Regardless of the size or technical maturity of your business, your organization is likely to fall victim to a cyber-attack.

A 2011 survey from Ponemon Institute found that 90 percent of organizations had been subject to one or more network breaches in the last 12 months. The fallout can be substantial: The survey found that it cost a minimum of $500,000 to mitigate the damage in terms of revenue losses, IT resources, business interruption, and other factors.

Beyond the financial cost, security breaches can cause untold damage to companies that are tasked with protecting confidential information for clients or customers, subjecting your organization to huge liability claims that may bankrupt your business. For organizations that are tasked with protecting classified data, such breaches could have a devastating impact on national security.

Firewalls and security software can identify known threats, but attack techniques are constantly evolving and mutating. Human analysts are required to discover and respond to these new threats before they succeed in compromising an organization under attack.

However, when analysts do not know what indicators to look for, they are not able to query their databases with the correct questions, and often do not recognize when their systems have been compromised. In order to identify and respond to cyber attacks in real-time, they need to integrate their existing security toolset with a more sophisticated data analysis solution that's custom-built for data discovery.

Partnering with YarcData offers many benefits:

- Expand your market reach with YarcData products and increase your revenue
- Access to exclusive material to help you grow your value proposition and improve sales effectiveness
- Improve and differentiate your product offering by building on top of the leading graph analytics appliance
- Benefit from our decades of experience in big data and relationship discovery with access to our solutions experts

The Technical Challenge

Discovering new threats requires the analyst to correlate and interpret information from a variety of network data sources, including NetFlow, DNS, IDS, and firewall records, among others. While network security tools are sufficient for identifying known threats, they cannot stop attacks that do not fit recognized data patterns. Human analysts themselves must be alert to such suspicious activities—however, they are often unsuccessful in identifying such issues for a number of reasons:

Analysts don't always know which queries will find the right answers

Information from an organization's disparate systems is stored in a variety of databases. The analyst must decide on a schema for the combined data, limiting the potential answers to those data sets that have been included. Adding a new source of data requires schema modification and extension—requiring a significant time commitment from the analyst. The slow time frame for integrating data from different sources leaves organizations vulnerable to new attacks; additionally, analysts may miss crucial information because they did not ask the correct questions.

The scale of data makes it difficult to identify malicious activity

For many large organizations, the enormous volume of web traffic creates false positives that make it difficult to recognize true malicious activity. Additionally, the perpetrators of cyber-attacks go to great lengths to remain anonymous and to develop complex new methods to infiltrate secure systems. Discovering new attack patterns requires skill and perseverance, running a variety of queries against as many sources of data as possible to filter normal traffic and identify anomalies.

Analysts cannot always identify attack patterns that don't fit their established rule sets

Network security analysts have an arsenal of tools that enable them to monitor for suspicious changes in network activity. As long as an attack fits one of their established rules, they are able to catch the attack—but if the breach does not fit a known pattern, they will only discover it by chance, if at all. They need access to a sophisticated system that will constantly analyze all incoming data to monitor for new patterns of attack.

Processing data in sub-groups can be time-consuming

Traditional analytics tools lack the processing power to analyze and interpret an organization's entire data library in real-time. Analysts cope by working with a subset of the available data—a few hundred million records, rather than the billions available. If the most critical information exists in the unanalyzed data and does not show up in queries (or shows up days or hours too late), the analysts may not become aware of a malicious attack immediately. When results are delivered rapidly, cyber-security analysts can refine searches more effectively, immediately plot next steps, and take action in time to prevent damage.

While traditional network security software and malware protection tools serve their purposes, network analysts need to integrate such solutions with an in-depth analytics platform that can help them discover the unknowns that could lead to data breaches. Cyber-security analysts need access to sophisticated analytics tools that can process massive amounts of data in a shared memory; support ad-hoc queries that are not based on existing schemas; and provide real-time response rates in order to search network data for unusual activity and immediately identify malicious attacks.

Becoming a YarcData partner admits you into our exclusive family of high performance graph analytics experts. To maintain our high standards, partners are required to show a commitment to learning about the unique products that YarcData offers and have a proven track record of success in the marketplace.

The Urika® Solution

A team of government security analysts facing such challenges turned to YarcData's Urika appliance to enable real-time discovery of suspicious network activity to prevent cyber-attacks. The Urika solution provided some significant benefits over their previous security toolset:

Schema-less data discovery

First, network data from multiple sources was loaded into a large graph, explicitly capturing all of the relationships contained within the data. The addition of new data, and new sources of data, into the graph is straightforward because schema extensions are not required; analysts do not need to define relationship fields between each data set.

Ad-hoc search capabilities

The search for new cyber-attacks requires the ability to perform ad-hoc searches for patterns of relationships, for which graph databases are ideally suited.

Real-time data analysis

Urika's performance makes it possible for the data analyst to iteratively find and isolate suspicious activity in real time, using all available network data. This helps analysts work more efficiently, and enables them to discover malicious activity in time to minimize the impact on the organization.

Urika owes its performance to its large shared memory, scalable I/O system and purpose-built Threadstorm™ graph processor.

Urika's huge, globally shared memory architecture of up to 512TB can hold the entire graph of relationships in memory. The scalable I/O subsystem, which can scale up to 350TB per hour, enables continuous updates to the graph as new data streams in.

The massively multi-threaded architecture of the Threadstorm™ processor (128 independent threads) is specially designed for analyzing graphs and allows threads to continue executing even if some are waiting for data to be returned from memory, preventing any downtime. This architecture delivers several orders of magnitude better performance on graph problems than commodity hardware.

YarcData
Getting to **Eureka!** faster™

About the Urika™ The YarcData Urika big data appliance for graph analytics helps enterprises gain business insight by discovering relationships in big data. Urika complements an existing data warehouse or Hadoop cluster by offloading graph workloads and interoperating within the existing analytics workflows. Subscription pricing or on-premise deployment of the appliance eases Urika adoption into existing IT environments.

About YarcData YarcData, a Cray company, delivers business-focused real-time graph analytics. Adopters include the Institute of Systems Biology, the Mayo Clinic, Noblis, Sandia National Labs, as well as multiple deployments in the US government. YarcData is based in the San Francisco bay area and more information is available at www.yarcdata.com.