Reference Architecture

HPE Reference Configuration for Cybersecurity Graph Analytics for Financial Services on HPE Superdome Flex

Combining Graph Analytics with Memory-Driven Computing for detecting cyber threats and anomalies

Has this paper been approved for submission to Uno QA? This table will be removed by Uno QA before publishing.

|  |  |  |
| --- | --- | --- |
| Required Approver | Approver's Name | Date Approved |
| Engineering Mgr | Chengalath, Hemanand |  |
| Product Mgr | Brett Gibbs |  |
|  |  |  |

Contents

[Executive summary 3](#_Toc30069563)

[Introduction 3](#_Toc30069564)

[Data Exfiltration and Cyber Vulnerability Assessment 4](#_Toc30069565)

[Common Cyber Network Incidents 4](#_Toc30069566)

[Cybersecurity Analytics 5](#_Toc30069567)

[Graph Analytics 6](#_Toc30069568)

[Memory-Driven Computing 6](#_Toc30069569)

[Solution overview 7](#_Toc30069570)

[Scale-Up MDC Architecture 7](#_Toc30069571)

[Cybersecurity Graph Analytics Solution Blueprint 7](#_Toc30069572)

[Solution components 8](#_Toc30069573)

[Trovares xGT Cybersecurity Graph Analytics Toolkit 8](#_Toc30069574)

[HPE Superdome Flex Server 8](#_Toc30069575)

[HPE OneView 9](#_Toc30069576)

[Hardware 10](#_Toc30069577)

[Software 10](#_Toc30069578)

[Application software 10](#_Toc30069579)

[Proof-of-concept Solution Implementation 11](#_Toc30069580)

[Use Case: Detecting network anomalies by identifying zombie reboot and RDP hacking events 11](#_Toc30069581)

[Scaling Lateral Movement Cyber Threat Detection 12](#_Toc30069582)

[Summary 13](#_Toc30069583)

[Appendix A: Bill of materials 14](#_Toc30069584)

[Version History 17](#_Toc30069585)

[Resources and additional links 18](#_Toc30069586)

# Executive summary

IT Organizations must mitigate cybersecurity risk by understanding external access to the infrastructure and how a malware infection or attack in a particular network. Addressing these challenges are massively complex due to complexity of the data center. Between thousands of servers and a web of physical and virtual networks, IT professionals in the financial services sector need a technology that understands this data effortlessly in order to effectively mitigate cybersecurity attacks.

Key business drivers behind cybersecurity graph analytics in Financial Services Industries (FSI) are:

* Bring together isolated cyber network data and events to prioritize exposed vulnerabilities
* Derive known and unknown cyber threats in the context of mission critical infrastructure assets
* Correlate intrusion alerts to known vulnerability paths and suggest best course of action to respond to cyber attack
* Provide cyber threat detection scaling from millions to billions of network devices and associated connections
* Detect cyber threats in near real-time to reduce high risk of financial data and cost exposure

The HPE Cybersecurity Graph Analytics solution offering for FSI is designed for infinitely scalable cyber network to keep track of massive volume of endpoint vulnerabilities across deployed infrastructure. This solution can help detect largest and richest attack surfaces surfacing with frequency of cyber incidents up to 300 times more attacks in FSI than other industries. This solution takes advantage of HPE Superdome Flex Memory-Driven Computing architecture and achieves order of magnitude reduced time taken to detect known threats from hours to seconds.

Goal of this HPE Cybersecurity Graph Analytics Reference Configuration is to identify known cyber threats for defined set of Cyber Threat Patterns including (but not limited to) Lateral Movement Threat Pattern (e.g.: Zombie Reboot Hacking, RDP Hacking, Privilege Escalation Hacking) , Command-and-Control Threat Pattern (e.g.: Connection Proxies Hacking, Remote Service Hacking, Windows Remote Management Hacking) and Data Exfiltration.

Target audience: The intended audience of this document includes, but is not limited to CSO, CDO’s, LOB’s, Data Engineers, IT managers, pre-sales engineers, services consultants, partner engineers, and customers that are interested in implementation of Cybersecurity Graph Analytics in their existing or new deployments to include Cybersecurity Graph Analytics processing capabilities for their analytic workloads.

Document purpose: The purpose of this document is to describe a Reference Configuration, highlighting recognizable benefits to technical audiences. This reference configuration provides general guidelines for implementing Cybersecurity Graph Analytics workload with HPE Superdome Flex using the Trovares xGT Graph Analytics Toolkit. In addition to outlining the key solution components, this white paper also provides guidelines for configuring and deploying this combined solution.

This Reference Configuration describes solution testing performed in January 2020.

# Introduction

Cyber-attacks have brought a new recognition of the importance of cybersecurity efforts. Attacks have now become widespread, common, and expected in some firms. New attacks are emerging within weeks due to an underground economy that has seen specialists create built-to-sell malware to a waiting list of cyber criminals. The impacts of cyber-attacks have been felt and there are reports that these attacks are only going to get worse. Below are commonly operated crimes across infrastructure network elements.



Figure 1. Cyber-attacks and Cyber-crime Concerns

## Data Exfiltration and Cyber Vulnerability Assessment

Data exfiltration is the unauthorized copying, transfer or retrieval of data from a computer or server. Data exfiltration is a malicious activity performed through various different techniques, typically by cybercriminals over the Internet. Data exfiltration is also known as data extrusion, data exportation or data theft.

A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately.

## Common Cyber Network Incidents

A cybersecurity incident or information security incident is defined under ISO/IEC TR 18044:2004 as a "single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security”. When a cybersecurity incident occurs, it very often causes service disruption because one or more IT services might be affected. These IT services might have been destroyed beyond recovery or forced to shut down or the threat actor is monitoring the IT system, preventing employees from continuing their work. In most cases, the threat actors follow a cyberattack kill chain that includes the injection of malware in the network. A cybersecurity incident by definition is either in the past or ongoing.

We can use anomaly-based detection to mitigate DDoS attacks and zero-day outbreaks. DDoS attacks are often used maliciously to consume the resources of hosts and network that would otherwise be used to serve legitimate users. The goal with these types of attacks is to overwhelm the victim network resources, or a system’s resources such as CPU and memory. Below are some very popular cyber incidents that occur frequently.

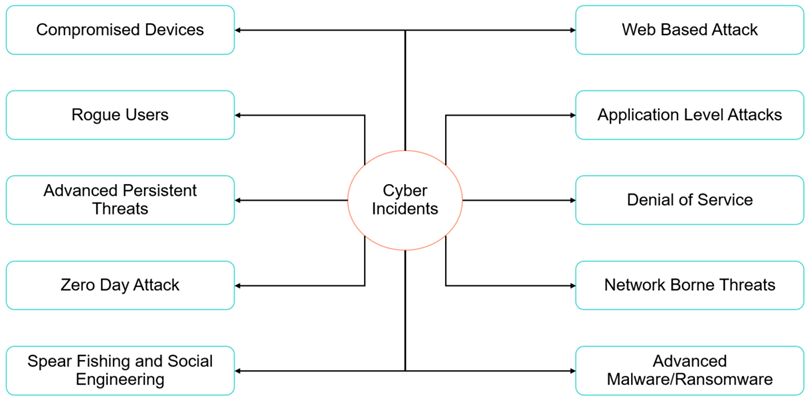
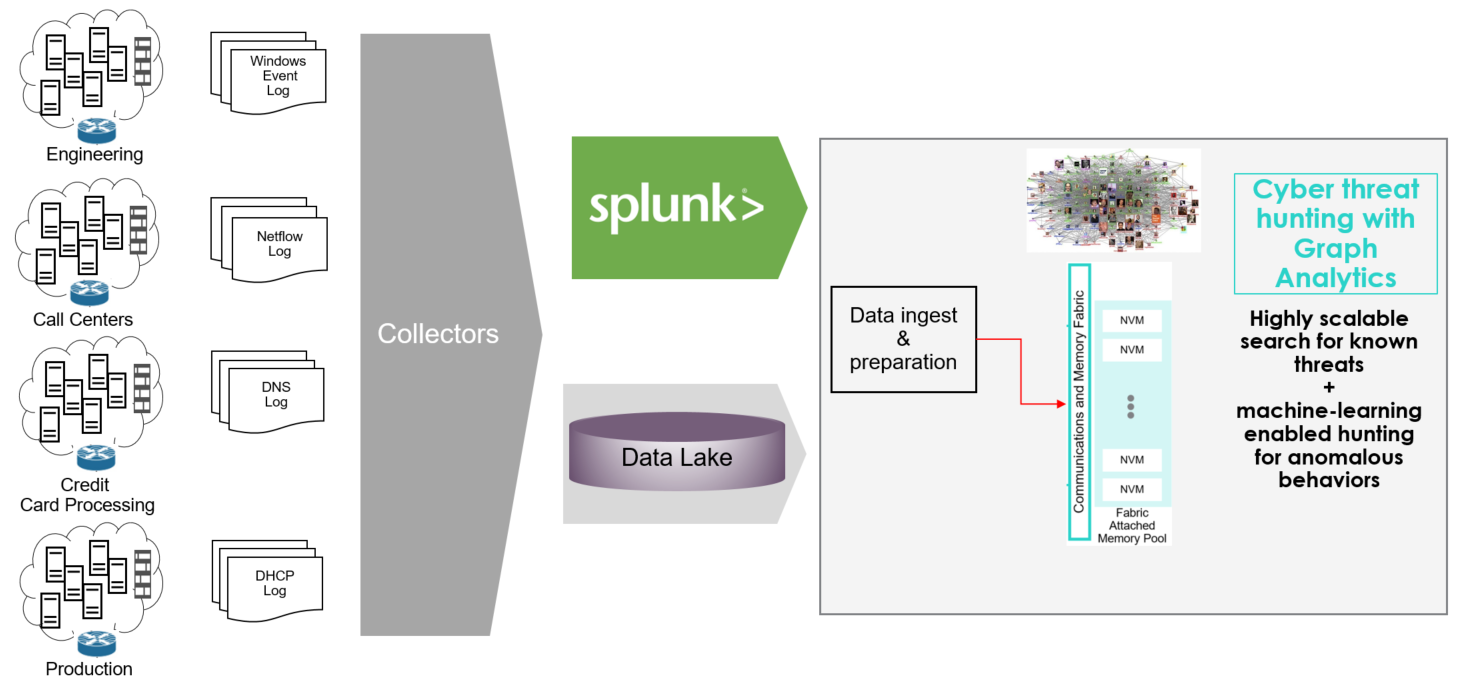


Figure 2. Common Cyber threats in IT Enterprise

* Cybercrime - Any crime that involves the use of a computer as the object of a crime or as an accessory used to commit a crime
* Ransomware - Malware built to extort money from victims by blocking access to their computers and files until they pay a ransom amount
* Malware – Malicious software. There are 3 categories of malwares – virus, worms and Trojanstrojans
* Social Engineering - An attack technique that is increasingly being used by cyber criminals to manipulate people into revealing some information or carrying out some actions
* Phishing - A common exploitation attack that involves sending fraudulent emails, that claim to be from reputable sources, to users
* Botnet - A network of zombie devices that have been infected with malware to make them perform certain tasks, such as denial of service attacks
* Data breach - A corporate network is attacked by cyber criminals and some valuable data is stolen.
* DDoS attack - Attackers target a machine with an overwhelming number of requests, thus clogging its bandwidth and ability to respond to legitimate requests
* Spyware - Malware used to spy on people for the purposes of obtaining their personal information, login credentials, or other sensitive information

## Cybersecurity Analytics

Cybersecurity Analytics involve analysis of server logs and network logs to find anomalies. The physical structure of the IT Network shows its topology and the interaction between the network hosts, routers and servers in the form of a graph. A large IP network consists of billions of nodes and numerous edges between these nodes, indicating the traffic between the nodes. This cyber traffic analysis forms the base for Cybersecurity Analytics of the IT network.



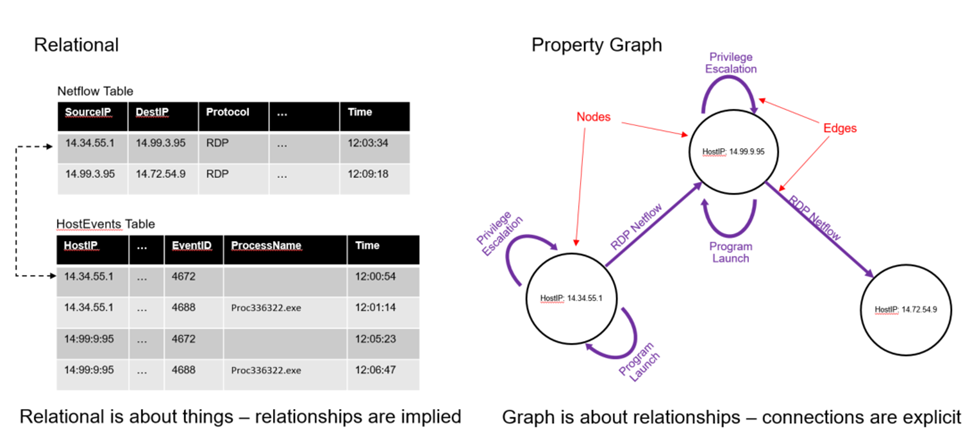
**Figure 3.** Cybersecurity Analytics deployment landscape

Typical landscape of Cybersecurity Analytics would include following key components:

1. Host and network data from deployed network elements are captured in various logs i.e. netflow log, conn log, dhcp log, http logs etc.
2. Critical data about deployed infrastructure and app would also be available in enterprise end-points like DIR Svcs, Usage Data, CMS etc
3. Data from these multiple sources would be collected for data aggregation and discovery as pre-processing for Cybersecurity Analytics
4. Log data is processed to identify Cyber Network elements and there-by build cyber network graph representing Network Elements
5. Data Scientists and Analytics would interact with In-Memory Cyber Graphs leveraging Interactive Data Science Notebooks
6. Cyber threat patterns would be identified and analyzed to detect cyber intrusion behavior
7. Develop pre-trained models in the form of Graph Queries to subsequently leverage for Day-Zero Threat Detection

## Graph Analytics

Graphs are mathematical structures used to model many types of entities and relationships in physical, biological, social and information systems. A graph consists of nodes or vertices (representing the entities in the system) which are connected by edges (representing relationships between those entities). Graphs, however, are more than just nodes and edges ‐ they are powerful data structures you can use to represent complex dependencies in your data. These Vertices and Edges carry properties describing characteristics of entities and relationships.

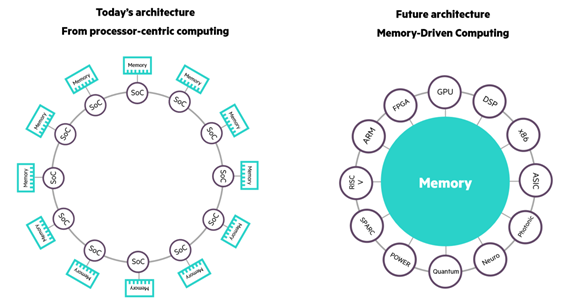


**Figure 4.** Graph Representation with entities and relationships

Graph Algorithms or Graph Analytics are analytic tools used to determine strength and direction of relationships between objects in a graph. The focus of graph analytics is on pairwise relationship between two objects at a time and structural characteristics of the graph as a whole.

## Memory-Driven Computing

Memory-Driven Computing offers every processor in a system access to giant shared pool of memory where as in traditional systems small amount of memory is tethered to each processor. Memory-Driven Computing is an almost infinitely flexible and scalable architecture that can complete any computing task much faster, using much less energy, than conventional systems. The performance of Memory-Driven Computing is possible because now any combination of computing elements can be composed and can communicate at the fastest possible speed.



**Figure 5.** Traditional Processor Driven Computing architecture vs Modern Memory-Driven Computing architecture

# Solution overview

Implementing a scalable Cybersecurity Graph Analytics solution requires understanding the scale of deployment to build cyber network of devices and connection between devices such that insights can be derived to uncover an attack pattern.

Below proposed deployment architecture enables bringing together of isolated data and associated events into an overall picture of decision support and situational awareness. This architecture scales infinitely to detect exposed vulnerabilities, mapped to potential threats in the context of mission critical threats.

## Scale-Up MDC Architecture

Cybersecurity Graph Analytics involves identifying cyber intrusion behaviours in a deployed infrastructure comprising of complex network of servers, routers, gateways, storage etc. Developing such Cybersecurity Graph Analytics involves analysing massive volume of Infrastructure network traffic information from network connection logs, http logs, dhcp logs, smtp logs, netflow information etc. and there by establishing a network of infrastructure entities and relationships. This is achieved by building a network graph, which enables detection of network anomaly patterns leading to identifying threats like Zombie reboot, RDP hacking etc.

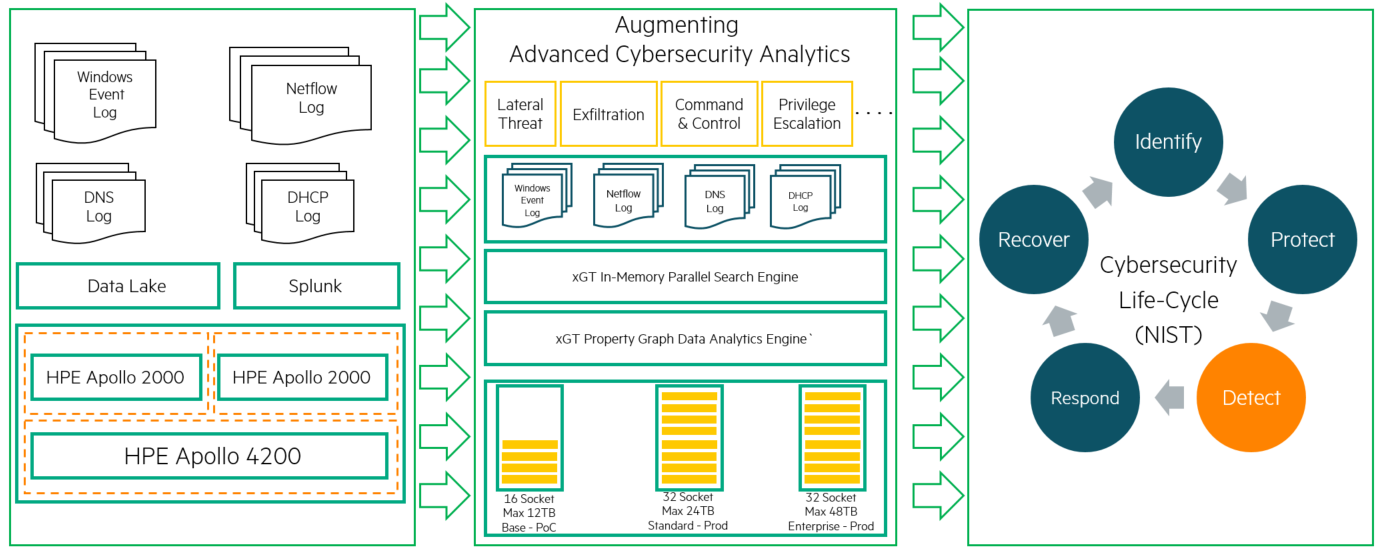
Typical size of these network graphs comprises of billions of graph nodes and properties and relationship between graph nodes. Deriving anomaly patterns across these billions of nodes in real-time requires existence of entire graph in-memory with TBs of large memory infrastructure.

Cybersecurity Graph Analytics use-case with Graph Analytics is ideal for memory-driven analytics.

## Cybersecurity Graph Analytics Solution Blueprint

Conventional graph tools limit companies to sampling a slice of their log data rather than the whole thing, or querying the data over days, not hours. In both cases companies expose themselves to undue risk.

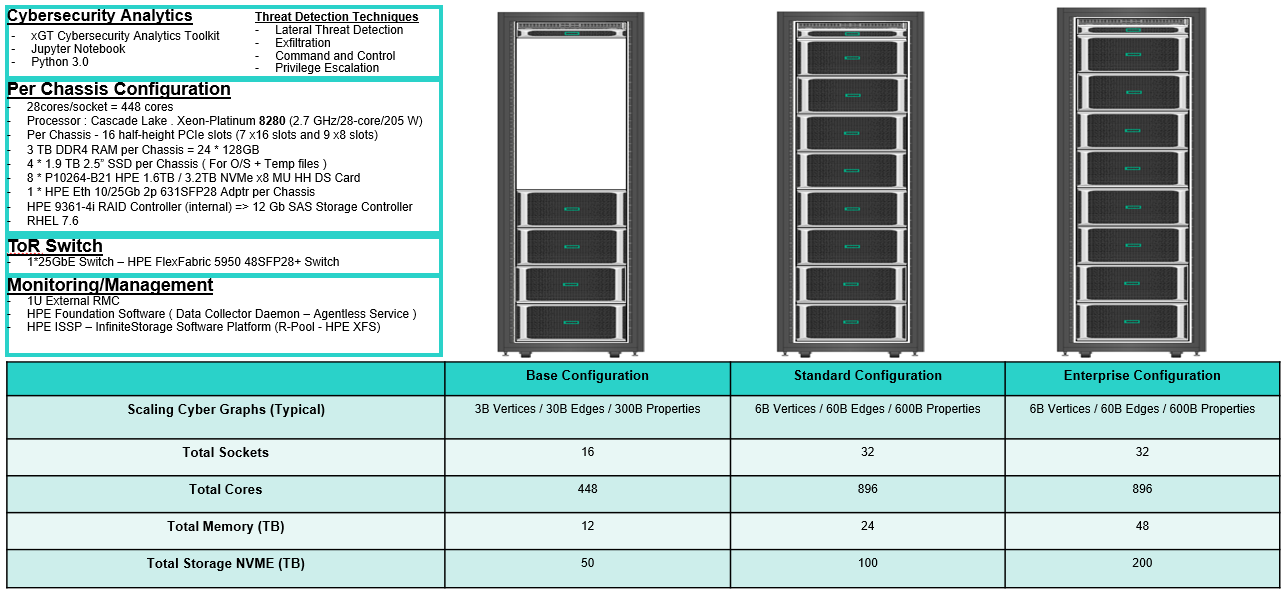
Trovares xGT is a property graph engine designed to support extremely large in-memory graphs. Trovares xGT analytics tool provides large graph search capabilities for data scientists and business analysts. With rapid ingest rates and the ability to execute complex queries driven by Python scripts, Trovares xGT provides unprecedented performance and scalability, especially when processing very large data.



**Figure 6.** Cybersecurity Graph Analytics with Trovares xGT on HPE Superdome Flex Solution Architecture

The configuration guide below provides the Graph Analytics S/W framework and infrastructure foundation needed for Cyber Threat anomaly detection to detect wide range of Cyber threat patterns. By leveraging these scalable configuration blueprints customer requirements can be designed for various threat pattern detection.

The sizing of the configurations outlined in this section is driven by Size of Cyber Network Graph and Threat Pattern Anomaly Detection requirements.



**Figure 7.** Reference Configuration – Cybersecurity Analytics with Trovares xGT Graph Analytics on Superdome Flex

# Solution components

## Trovares xGT Cybersecurity Graph Analytics Toolkit

Trovares offers a new type of graph analytics tool which returns search queries hundreds of times faster than conventional graph tools. It supports extremely large in-memory graphs for fast queries. Built on supercomputing technology, Trovares derives maximum performance for cyber, fraud detection, government, and other applications.

It enables the direct ingest of data into the system and avoids database performance issues. Trovares xGT adopts supercomputing techniques such as extreme multithreading and fine-grain locks to achieve orders of magnitude increase in speed and scale.

Trovares xGT offers following key differentiated features for Cybersecurity Graph Analytics

* Graph representation of Cyber Network Devices
* Massive parallel processing engine based on Symmetric Multiprocessor (SMP) architecture
* Optimized search engine for In-Memory processing with Cypher compatible Trovares Query Language (TQL)

## HPE Superdome Flex Server

The HPE Superdome Flex combines the best of Intel Xeon architecture and the new HPE Superdome Flex ASIC chipset to provide the most flexible x86-server solution available. The system is imbued with the necessary RAS features to operate in mission-critical environments where application availability is of paramount importance. With a modular chassis connected by cables, it is only necessary to buy the hardware, including power and cooling infrastructure, to fit the need, and not spend more securing expandability until that is needed, avoiding unnecessary and costly over-provisioning of infrastructure. Mission-critical resiliency is provided through end-to-end implementation of processor RAS features, redundancy of key system components, and advanced system software, to help ensure the server is up and running 24 x 7 . With the HPE Superdome Flex, your Cybersecurity Graph Analytics infrastructure can grow along with your data. HPE Superdome Flex Server features include:

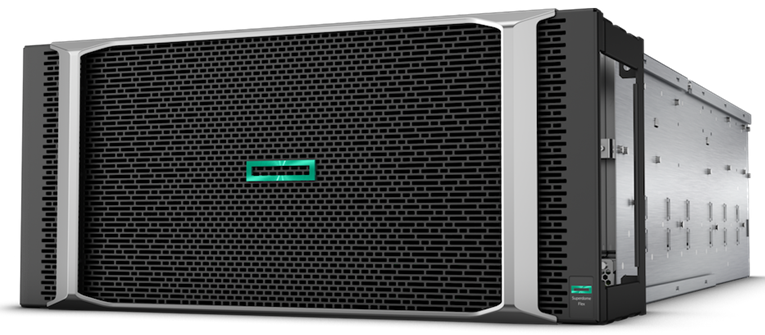
* Modular architecture that scales seamlessly from 4- to 32-sockets in 4-socket increments in a single system
* Shared memory capacity from 768 GB up to 48 TB
* Features Intel® Xeon® Scalable processors 1st or 2nd generation
* Proven RAS capabilities not available on other standard platforms
* Best-in-class predictive fault-handling Analysis Engine, predicts hardware faults and initiates self-repair without operator assistance
* Firmware First approach to log analysis ensures error containment at the firmware level, including memory errors, before any interruption can occur at the OS layer
* Mission-critical resiliency from end-to-end implementation of processor RAS features, to redundancy of key system components to advanced system software

The HPE Superdome Flex Server is managed via an external Rack Management Controller (RMC), although an embedded version of this (eRMC) is available for scalable 4 or 8 socket configurations.

The RMC is the administrative node for the HPE Superdome Flex and it includes one network port for administrative access to the system console. HPE Superdome Flex Server administrative functions are performed via the RMC or eRMC:

* Configuring system partition
* Network configuration
* Booting, rebooting, and shutting down the system
* Viewing hardware resources, etc.

Computing resources on the HPE Superdome Flex Server are assigned to a node partition (HPE nPar). HPE nPars are hard partition technology providing complete workload isolation, enabling you to configure a multichassis server complex as one large server or as multiple, smaller, independent servers. Each HPE nPar has its own independent processors, memory, and I/O resources of the chassis that make up the partition. This greatly enhances the ease in which CPUs can be added and memory can be expanded to the installed operating system partition.



**Figure 8**. HPE Superdome Flex chassis

## HPE OneView

HPE OneView is a converged infrastructure management platform that provides a unified interface for the administration of systems in a data center. Through a single GUI—sometimes referred to as a single pane of glass—administrators can automate management and maintenance tasks that have traditionally been performed manually and required several different tools. Within the data center, HPE OneView can manage physical systems, storage arrays, and network connectivity. HPE OneView is licensed to enable functionality in two modes, Monitor mode and Managed mode. HPE OneView will automatically enable the license for Managed mode if HPE OneView is version 5.0 or newer and HPE Superdome Flex firmware is version 3.0.x or newer. Please refer to [HPE SUPERDOME FLEX SERVER MANAGEABILITY](https://h20195.www2.hpe.com/v2/GetDocument.aspx?docname=a50000335enw) for more details.

NOTE:

HPE OneView Standard and Advanced licenses are included with the purchase of a HPE Superdome Flex Server.

## Hardware

The following hardware components were deployed for this solution.

Table 1. Solution hardware components

|  |  |
| --- | --- |
| Component | Description |
| 1U External RMC | A Superdome Flex Server complex contains one or more Superdome Flex Server chassis in a rack that each contain individual compute, memory, networking, and storage resources. An nPartition is created and managed using the Rack Management Controller (RMC) |
| HPE Superdome Flex 4-socket Base Chassis | A chassis that includes BaseIO in the hardware that provides drive bays, network ports, and USB ports |
| HPE Superdome Flex 4-socket Expansion Chassis | An add-on chassis to scale-up the capacity of a nonpartitionable system |
| HPE FlexFabric 5950 Switch | Top-of-the-rack Data Center Network Switch |
| HPE NVMe x8 Lanes Mixed Use | High performance NVMe drives for data storage for Cybersecurity Graph Analytics |

Table 2 Solution Server components – Base and Expansion Chassis

|  |  |
| --- | --- |
| Component | Description |
| Processor | Four 28-core Intel Xeon 8280 processors at 2.70GHz |
| Memory | 3TB memory (24 x 128GB HPE DDR4 SmartMemory LRDIMMs) |
| Built-in Network Adapters | 1 x 10 Gb dual port Ethernet adapter, 1 x 1GbE dual port Ethernet adapter |
| Additional Network Adapters | 1 x 10/25 Gb dual port 631SFP28 Ethernet adapter |
| OS disk | 4 x 1.9 TB SSD |
| Data disk | 8 x HPE 1.6 TB NVMe x8 MU HH DS Card |

## Software

The following softwares components were deployed for this solution.

Table 3. Solution software components

|  |  |
| --- | --- |
| Component | Description |
| Redhat 7.6 | Linux Distro |
| Open JDK 1.8 | Java Development Kit |
| Python 3.0 | Compatible Python Runtime for Interactive Notebook and Graph Analytics |
| HPE ISSP | Infinite Storage Software Platform |
| Jupyter iPython Notebook | Interactive Notebook for Cybersecurity Graph Analytics |
| SAR Analyzer | Performance Analyzer for CPU, Memory, Network, I/O Utilization |

## Application software

The following application softwares were deployed for this solution.

Table 4. Application components

|  |  |
| --- | --- |
| Quantity | Description |
| Trovares xGT 1.3 | Graph Analytics Toolkit |
|  |  |

# Proof-of-concept Solution Implementation

Following section describes Cybersecurity Graph Analytics Use-Case implemented with Trovares xGT deployment on HPE Superdome Flex.

## Use Case: Detecting network anomalies by identifying zombie reboot and RDP hacking events

Let us look at how the proposed In-Memory Cybersecurity Graph Analytics Solution can be deployed to identify cyber threats in an operational network of Financial Services Organization. Use case considered here is to detect network anomalies by identifying zombie reboot and RDP hacking events in a deployed enterprise network. The attack pattern for such network hack is called Lateral Movement attack.

Lateral movement is a cyberattack pattern that describes how an adversary leverages a single foothold to compromise other systems within a network. Identifying and stopping lateral movement is an important step in controlling the damage from a breach, and also plays a role in forensic analysis of a cyberattack, helping to identify its source and reconstruct what happened.

RDP hijacking is actually a family of attacks, each with different characteristics on how to attain the privileges required to perform the RDP hijacking. The attack broadly looks like this:

1. Lateral movement starts from a foothold where an adversary already has gained access. We'll call this host A.
2. The attacker uses some privilege escalation technique to attain SYSTEM privilege.
3. The attacker then leverages their SYSTEM privilege to hijack as RDP session to move through a network. The result is to become logged in to another system where the RDP session had been. We'll call this host B.
4. This hijacking action can be repeated to form longer chains of lateral movement; and these chains can be represented as graph patterns.

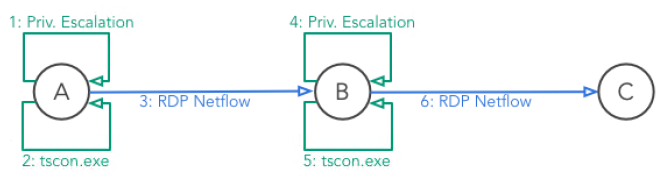


Figure 9. RDP hacking lateral movement attack pattern

Below are the steps involved:

1. Trovares xGT tool reads massive amount of data into RAM for performing fast pattern search operation. There are two ways to get the data into Trovares xGT i.e. across a network or from a filesystem. Fetch such data can be achieved leveraging load() function in Trovares xGT module.
2. Once the data is represented in the form of In-Memory Graph model (Local Structure), each vertex uniquely identifies Cyber Network elements and devices represented by vertex\_frames. The connection between these devices represent exchange of network traffic and these relationships represented as Edges also carry properties representing the nature of network traffic represented by edge\_frames.

MATCH <structure>

WHERE <optional constraints or properties>

SET <optional property modifications>

MERGE <optional addition of vertices>

CREATE <optional addition of vertices and edges>

DETACH DELETE <optional deletion of vertices>

DELETE <optional deletion of edges>

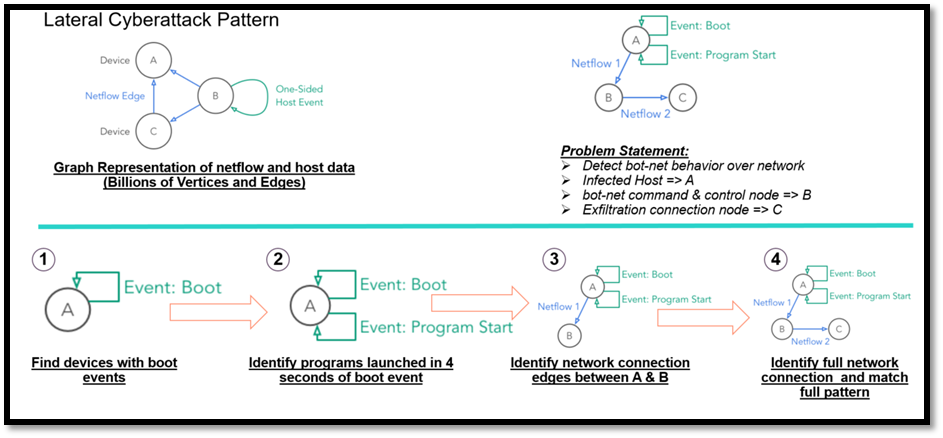
RETURN <description of answer set>

INTO <results table name>

1. Trovares Query Language (TQL) uses a subset of cypher language to express queries. Trovares xGT offers strongly typed graph elements (fixed schema) with cypher language based Trovares Query Language. Typical query subset is represented as above.

Steps involved in detection of zombie reboot and RDP hacking events for the identifying Cyber Network attack are as follows:

1. 2-Chassis Single Partition environment was created in HPE Superdome Flex system and RHEL 7.6 was installed and repositories were configured to implement Trovares xGT Graph Analytics Toolkit.
2. Ingest host and network log data and persist into fast storage media implemented with NVME drives in HPE Superdome Flex.
3. Data loading is performed using load function available in Trovares xGT. Aggregated data is transformed into a Graph Data Model and a network graph is built to represent these network entities with vertex\_frames and edge\_frames.
4. 90 Days of netflow event and host event data loaded and transformed in Graph Data Model in Trovares xGT creates a network graph of 20 Billion Graph Edges (17.9 Billion Netflow Edges and 1.5 Billion log edges) and 212 billion graph edge properties against 3TB of input data from network.



**Figure 10**. Detect RDP Cyber-attack pattern with Trovares xGT Graph Analytics Toolkit

1. Interactive Query operation is performed to detect bot-net behavior over network.
2. Extract the forward RDP Edges
3. Extract Reverse RDP Edges
4. Extract RDPFlow Edge Frames
5. Build Temporal Constraints in RDPFlow Edge Frames

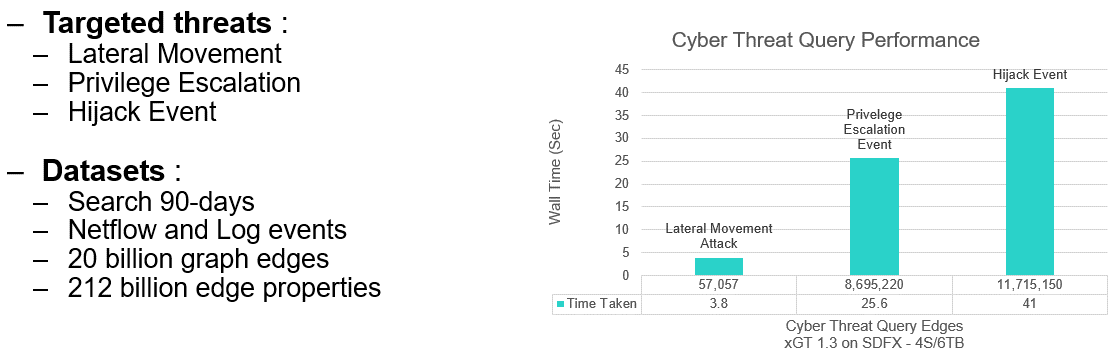
Cyber threat anomaly detection requires monitoring and management of cyber network devices across multiple departments. In order to achieve scalable deployment, preferred approach is to understand how Graph Search performance scales.

## Scaling Lateral Movement Cyber Threat Detection

We'll be using the LANL Unified Host and Network Dataset, a set of netflow and host event data collected on an internal Los Alamos National Lab network.

Our goal will be to turn about 3TB of CSV files into a single connected graph. Cybersecurity Analyst then provides the criteria for specific cyber threat patterns. Subgraph Isomorphism or pattern matching is performed on large memory graphs and sub-graphs are queried to detect attack infected hosts.

The Unified Host and Network Dataset is a subset of network and computer (host) events collected from the Los Alamos National Laboratory enterprise network over the course of approximately 90 days. The host event logs originated from most enterprise computers running the Microsoft Windows operating system on Los Alamos National Laboratory's (LANL) enterprise network. The network event data originated from many of the internal enterprise routers within the LANL enterprise network.



**Figure 11.** Cybersecurity Threat Detection with xGT on Superdome Flex

Graph above highlights performance scalability of Lateral Movement Cyber attack detection. Here is quick summary:

1. 90 Days of Host Event Logs and Network Logs were processed and transformed in Cyber Network Graph representing 933,714 devices, ~20 billion Graph Edges.
2. In-Memory Graph required 3TB of Memory to hold the entire Graph with >90% CPU Utilization
3. Lateral Movement attack query was executed to detect affected Network Edges. 57,057 network edges were detected from among ~20B Graph Edges.
4. Total Query execution time was 7 minutes and 17 seconds.

# Summary

Hewlett Packard Enterprise and Trovares xGT allow one to detect Known Cyber Threat Patterns with massive scale Cybersecurity Graph Analytics Toolkit of Trovares xGT implemented with Symmetric Multiprocessing Memory-Driven Computing architecture of Superdome Flex by building scalable cyber graphs in-memory and finding threat patterns. However, designing and building scalable Cyber Graph can be both complex and time consuming. This white paper provides a Reference Configuration for deploying Trovares xGT on HPE Superdome Flex infrastructure and management software. These configurations leverage HPE servers, storage and networking, along with integrated management software and bundled support. In addition, this white paper has been created to assist in the rapid design and deployment of Cyber Graphs on HPE Superdome Flex infrastructure for graphs of various sizes.

As a matter of best practice for all deployments, Hewlett Packard Enterprise recommends implementing a proof-of-concept using a test environment that matches as closely as possible the planned production environment. In this way, appropriate performance and scalability characterizations can be obtained. For help with a proof-of-concept, contact a Hewlett Packard Enterprise Services representative ([hpe.com/us/en/services/consulting.html](http://www.hpe.com/us/en/services/consulting.html)) or your Hewlett Packard Enterprise partner.

# Appendix A: Bill of materials

Note

Part numbers are at time of publication/testing and subject to change. The bill of materials does not include complete support options or other rack and power requirements. If you have questions regarding ordering, please consult with your Hewlett Packard Enterprise Reseller or Hewlett Packard Enterprise Sales Representative for more details. [hpe.com/us/en/services/consulting.html](http://www.hpe.com/us/en/services/consulting.html)

Table A1. Bill of materials – Base Configuration: Base Configuration is designed to kick-start development and PoC for Cybersecurity Graph Analytics

|  |  |  |
| --- | --- | --- |
| Quantity | Part number | Description |
| 1 | M0S66A | HPE Virtual Rack |
| 1 | Q2N05B | HPE Superdome Flex 4-socket Base Chassis |
| 4 | R0W99A | HPE Superdome Flex Intel Xeon-Platinum 8280 (2.7GHz/28-core/205W) Processor Kit |
| 24 | R0X07A | HPE Superdome Flex 128GB (1x128GB) Quad Rank x4 DDR4-2933 Load Reduced Memory Kit |
| 4 | R2A74A | HPE 1.92TB SATA 6G Mixed Use SFF (2.5in) RW 3yr Wty Digitally Signed Firmware SSD |
| 1 | Q2N09A | HPE Superdome Flex PCIe Low Profile 16-slot 4 Riser Configuration Kit |
| 1 | Q2N41A | HPE Superdome Flex DVD-RW Drive |
| 1 | 817718-B21 | HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter |
| 8 | P10264-H21 | HPE 1.6TB NVMe x8 Lanes Mixed Use HHHL 3yr Wty Digitally Signed Firmware Card |
| 3 | Q6L89B | HPE Superdome Flex 4-socket Partition Expansion Chassis |
| 12 | R0W99A | HPE Superdome Flex Intel Xeon-Platinum 8280 (2.7GHz/28-core/205W) Processor Kit |
| 72 | R0X07A | HPE Superdome Flex 128GB (1x128GB) Quad Rank x4 DDR4-2933 Load Reduced Memory Kit |
| 12 | R2A74A | HPE 1.92TB SATA 6G Mixed Use SFF (2.5in) RW 3yr Wty Digitally Signed Firmware SSD |
| 3 | Q2N09A | HPE Superdome Flex PCIe Low Profile 16-slot 4 Riser Configuration Kit |
| 3 | Q2N41A | HPE Superdome Flex DVD-RW Drive |
| 3 | 817718-B21 | HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter |
| 24 | P10264-H21 | HPE 1.6TB NVMe x8 Lanes Mixed Use HHHL 3yr Wty Digitally Signed Firmware Card |
| 1 | Q9Z05A | HPE Superdome Flex 16-socket Interconnect and Partition Activation Kit |
| 1 | Q2N07A | HPE Superdome Flex Rack Management Controller |
| 4 | Q7N11A | HPE Foundation Software 2 for Red Hat Enterprise Linux Media License RTU |

Table A2. Bill of materials – Standard Configuration: Standard Configuration is designed for scaling from Deveployment to Prod deployment of Cybersecurity Graph Analytics

| Quantity | Part number | Description |
| --- | --- | --- |
| 1 | M0S66A | HPE Virtual Rack |
| 1 | Q2N05B | HPE Superdome Flex 4-socket Base Chassis |
| 4 | R0W99A | HPE Superdome Flex Intel Xeon-Platinum 8280 (2.7GHz/28-core/205W) Processor Kit |
| 24 | R0X07A | HPE Superdome Flex 128GB (1x128GB) Quad Rank x4 DDR4-2933 Load Reduced Memory Kit |
| 4 | R2A74A | HPE 1.92TB SATA 6G Mixed Use SFF (2.5in) RW 3yr Wty Digitally Signed Firmware SSD |
| 1 | Q2N09A | HPE Superdome Flex PCIe Low Profile 16-slot 4 Riser Configuration Kit |
| 1 | Q2N41A | HPE Superdome Flex DVD-RW Drive |
| 1 | 817718-B21 | HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter |
| 8 | P10264-H21 | HPE 1.6TB NVMe x8 Lanes Mixed Use HHHL 3yr Wty Digitally Signed Firmware Card |
| 7 | Q2N06B | HPE Superdome Flex 4-socket Expansion Chassis |
| 28 | R0W99A | HPE Superdome Flex Intel Xeon-Platinum 8280 (2.7GHz/28-core/205W) Processor Kit |
| 168 | R0X07A | HPE Superdome Flex 128GB (1x128GB) Quad Rank x4 DDR4-2933 Load Reduced Memory Kit |
| 7 | Q2N09A | HPE Superdome Flex Rack Management Controller |
| 7 | 817718-B21 | HPE Superdome Flex PCIe Low Profile 16-slot 4 Riser Configuration Kit |
| 56 | P10264-H21 | HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter |
| 1 | Q2N20A | HPE 1.6TB NVMe x8 Lanes Mixed Use HHHL 3yr Wty Digitally Signed Firmware Card |
| 1 | Q2N07A | HPE Superdome Flex 32-socket Interconnect and Scale Activation Kit |

Table A3. Bill of materials – Enterprise Configuration: Enterprise Configuration is designed for large scale Production deployment of Cybersecurity Graph Analytics

| Quantity | Part number | Description |
| --- | --- | --- |
| 1 | M0S66A | HPE Virtual Rack |
| 1 | Q2N05B | HPE Superdome Flex 4-socket Base Chassis |
| 4 | R0X00A | HPE Superdome Flex Intel Xeon-Platinum 8280M (2.7GHz/28-core/205W) Processor Kit |
| 48 | R0X07A | HPE Superdome Flex 128GB (1x128GB) Quad Rank x4 DDR4-2933 Load Reduced Memory Kit |
| 4 | R2A74A | HPE 1.92TB SATA 6G Mixed Use SFF (2.5in) RW 3yr Wty Digitally Signed Firmware SSD |
| 1 | Q2N09A | HPE Superdome Flex PCIe Low Profile 16-slot 4 Riser Configuration Kit |
| 1 | Q2N41A | HPE Superdome Flex DVD-RW Drive |
| 1 | 817718-B21 | HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter |
| 8 | P10266-H21 | HPE 3.2TB NVMe x8 Lanes Mixed Use HHHL 3yr Wty Digitally Signed Firmware Card |
| 7 | Q2N06B | HPE Superdome Flex 4-socket Expansion Chassis |
| 28 | R0X00A | HPE Superdome Flex Intel Xeon-Platinum 8280M (2.7GHz/28-core/205W) Processor Kit |
| 336 | R0X07A | HPE Superdome Flex 128GB (1x128GB) Quad Rank x4 DDR4-2933 Load Reduced Memory Kit |
| 7 | Q2N09A | HPE Superdome Flex PCIe Low Profile 16-slot 4 Riser Configuration Kit |
| 7 | 817718-B21 | HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter |
| 56 | P10266-H21 | HPE 3.2TB NVMe x8 Lanes Mixed Use HHHL 3yr Wty Digitally Signed Firmware Card |
| 1 | Q2N20A | HPE Superdome Flex 32-socket Interconnect and Scale Activation Kit |
| 1 | Q2N07A | HPE Superdome Flex Rack Management Controller |

# Version History

Project: HPE Reference <Architecture or Configuration> for <Software Company name/product> on HPE <product name>

Status: Draft, Published

|  |  |  |
| --- | --- | --- |
| Document version | Date | Description of change |
| 1.0 | 01/13/2020 | Initial publication |
|  |  |  |
|  |  |  |
|  |  |  |

# Resources and additional links

HPE Reference Architectures, [hpe.com/info/ra](http://www.hpe.com/info/ra)

HPE Servers, [hpe.com/servers](http://www.hpe.com/servers)

HPE Storage, [hpe.com/storage](http://www.hpe.com/storage)

HPE Networking, [hpe.com/networking](http://www.hpe.com/networking)

HPE Technology Consulting Services, [hpe.com/us/en/services/consulting.html](http://www.hpe.com/us/en/services/consulting.html)

6-cybersecurity Mega Trends, [hpe.com/us/en/insights/articles/6-security-megatrends-1905.html](file:///C:\aWorkatHPE\RA_RC_Projects\MDC\hpe.com\us\en\insights\articles\6-security-megatrends-1905.html)

Memory Drive Computing in Superdome Flex, [hpe.com/us/en/newsroom/blog-post/2017/05/memory-driven-computing-explained.html](file:///C:\aWorkatHPE\RA_RC_Projects\MDC\hpe.com\us\en\newsroom\blog-post\2017\05\memory-driven-computing-explained.html)

Mission critical Infrastructure for Data Driven Enterprise, [hpe.com/hpe-external-resources/a00037000-7999/enw/a00037029?resourceTitle=Mission-critical+infrastructure+for+the+data-driven+enterprise](file:///C:\aWorkatHPE\RA_RC_Projects\MDC\hpe.com\hpe-external-resources\a00037000-7999\enw\a00037029%3fresourceTitle=Mission-critical+infrastructure+for+the+data-driven+enterprise)

HPE Performance Cluster Manager <http://www.hpe.com/software/hpcm>

Trovares, [trovares.com](file:///C:\aWorkatHPE\RA_RC_Projects\MDC\trovares.com)

Trovares, <http://docs.trovares.com/1.2.0/>

HPE Superdome Flex servers, <https://www.hpe.com/us/en/servers/superdome.html>

HPE Education Services, <http://h10076.www1.hpe.com/ww/en/training/portfolio/bigdata.html>

To help us improve our documents, please provide feedback at [hpe.com/contact/feedback](http://www.hpe.com/contact/feedback).

Learn more at

hpe.com/xxxxxx