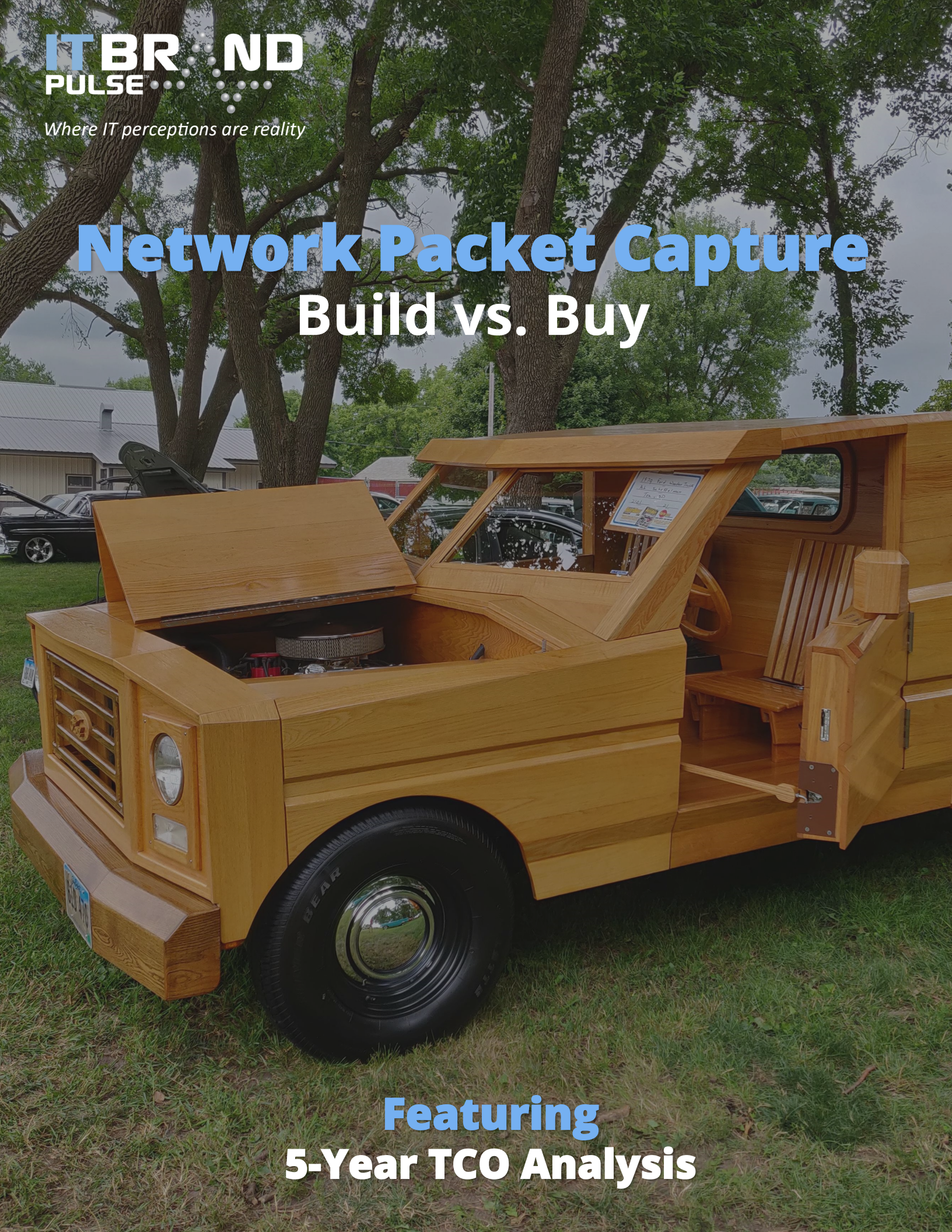
IT BRAND PULSE

Where IT perceptions are reality

Network Packet Capture
Build vs. Buy



Featuring
5-Year TCO Analysis

Total Cost of Ownership (TCO)

TCO Case Studies

IT professionals know the cost of owning servers, networking and storage equipment is more than the purchase price of the hardware. The total cost of IT equipment also includes installation, software licenses, service, support, training, upgrades, and other costs related to a specific product or project.

TCO case studies are designed to provide busy IT Pros with vendor-independent data about the total cost of specific products. This case study examines the build vs. buy decision that so many IT Pros encounter when trying to solve a problem. In this case we are analyzing the build vs. buy decision for a network packet capture system, and take into account the typical costs to develop, deploy and support such a system over a five-year timeframe. Read the report to find out how we came to our decision.

Cost Components

Below are the components used to calculate the total cost of owning the servers and storage to create a packet capture system, over a five-year period:

Hardware Product Cost - The purchase price for servers and HDDs to support the use case.

Software License Fees - Includes any initial costs and any recurring/annual license fees for software, if applicable.

Recurring Annual Service & Support Fees - The cost of a service agreement providing on-site service with next business day (NBD) response time.

Training - The cost of certifying one systems engineer for this class of product (not applicable in this report).

Development and Support Personnel Cost - Since this is a comparison of a "build" we have included personnel costs for System Engineers to design, develop and deploy the system, along with on-going support.

Getting the Cost Data

The product pricing (cost) data used in this case study comes from on-line resellers and solution providers who responded to a request for quote (RFQ) from IT Brand Pulse.

Apples-to-Apples Comparison

In this report we didn't include the networking infrastructure costs, since they can vary, and customers may already have available ports on switches, network packet broker/load balancer and cabling to support a build -out such as this. Additionally, no power and cooling costs were included, since we believe the costs of a rack, to support this configuration, in a data center is minor, and will vary per customer.

Full Packet Capture is Vital

Top 3 Reasons Why Network Full Packet Capture is Deployed

In today's environment more business is being conducted online, more "work from home" (WFH) personnel and students are driving the demand for network access and exposing more endpoints to an organization's IT security perimeter. Keeping those networks running and applications performing is a challenge for anyone in IT - SecOps, NetOps, and DevOps teams.

Full packet capture (FPC) appliances capture and continuously record all Ethernet/IP activity, whereas ad-hoc or triggered packet capture appliances capture only a subset of traffic, at a moment in time, based on a set of user-definable filters, such as IP address, MAC address, or protocol. It is best to use a FPC appliance or you will risk missing the vital data required for network forensics or cyber security purposes. By continuously recording every packet it enables you to see every threat or performance issue with clarity.

The 3 top reasons for FPC are:

1. **Improved Security Incident Response and Reduced Risk** - a complete copy of your network traffic shows the full extent of any threat or breach. System logs and other evidence are often wiped by hackers, where as packet captures cannot be wiped. This is the clearest evidence of the extent and nature of any threat.
2. **IT Operations Troubleshooting** - resolving performance issues and pinpointing the cause of any outage is faster and more conclusive when you have a full record of how the applications transact over the network. 100% packet capture gives you the ability to detect a network performance issue in real time.
3. **Improved Resolution Time and Productivity** - security threats, network and application performance problems that don't get resolved for months are now resolved in minutes or hours when analysts have access to a full recording of network traffic. Threats can be characterized and re-mediated in hours boosting your analyst's productivity and your mean-time-to-resolution (MTTR). Without recorded network traffic threat resolutions can "stall" for months and may never be properly understood.

Full Packet Capture (FPC) data is the most extensive and represents all the network data that can be collected. Each one of your IT teams has a different need for FPC.

- Security Engineers can record and play back all the traffic on the network. This enables them to validate any IDS/IPS alerts and validate any items that NetFlow or log data is showing.
- Capturing all packets in real-time can assist your Network Performance team in visualizing, monitoring, optimizing, troubleshooting and reporting on the health and availability of your network. Troubleshooting packet loss and network high latency are just two issues that can be resolved with FPC.
- DevOps can integrate full network history into their application monitoring tools so they can quickly figure out which issues are negatively impacting an application's performance.

2 Types of Packet Capture Buyers

In today's environment the need for Full Packet Capture is quickly becoming a necessity for a number of IT organizations. Once the decision is made to acquire one, two types of buyers emerge.

1. **Business Critical** - This enterprise IT organization believes that FPC is business critical for not only the security team and network team, but for the DevOps team that are developing new applications to fulfill their digital transformation strategy. Access to packet data helps to quickly stop the finger pointing between the Apps and NetOps teams, when there's an issue. Security Engineers need FPC to quickly remediate threats before they become breaches. They all believe 100%, real-time packet capture is critical for their success and are willing to go to the experts to get the best-in-class products.
2. **Open-Source** - This enterprise IT organization believes that packet capture is necessary, but may or may not be business critical. They have a successful track record of "do it yourself" (DIY) and will approach Network Packet Capture the same way. There must be a good reason NOT to do it yourself.

This paper is written for the Open-Source shops that want to tackle the Network Package Capture build project. I will cover what is required, what I discovered, and the associated costs and risks involved. I will also compare this to a "buy" solution from a purpose-built appliance vendor. You can decide for yourself if, based on this information, it makes sense to do-it-yourself.

Let's start with a set of must-have features that you should look for in a Network Packet Capture system.

- 100% accurate, continuous, real-time packet capture
- No loss of packets during capture process
- Retention of packet-level network history for a period of time (let's say 2 weeks)
- Scalable to meet the speeds and growth of your network
- Packet Capture software system with indexing and search tools
- Easy to set-up, configure, re-configure when necessary, and operate
- Reliable maintenance and tech support/help for your system
- Software updates, bug fixes, and enhancements on a regular basis, including security patches for emerging CVEs (Common Vulnerabilities and Exposures)

And a couple of "nice to have" features include:

- Ability to host third-party analytics tools/applications on the capture servers (i.e., the ability to "push" analytics apps. to where the data resides)
- Ability to host open-source analytics tools/applications on the capture servers

I'm sure there might be a few more, but I think this list addresses the major items you would want to consider in any system.

The “Build” Option with Arkime

Open-Source Shop

In this scenario, I imagine you work in an IT Department of a medium-to-large-sized enterprise that has an open systems philosophy to IT. Your team supports that view, are willing to try new things, and have succeeded with this strategy in the past. So, you get them together and brainstorm some ideas on how to build this packet capture device. You come to a number of conclusions:

1. We can use one or two existing servers in the network with some hardware or software taps and copy packets to our SAN disk array. This will work, but we’ll need some way to index the packets so we can search quickly. Additionally, the SAN disk is expensive and dedicated to ERP, so maybe we should get some cheap drives or object storage from a SDS (software-defined storage) vendor. (Note: SAN disk arrays are 2-4x the price of SDS.) We also learned that continuous packet capture would put a heavy IOPS load on the SAN and probably negatively impact the performance of other applications.
2. How do we use our analytics tools to get access to this packet data without copying it to the analyzer?
3. Who will write the specification, develop, test, implement and support this new system?

Finds Arkime Packet Capture & Search Tool

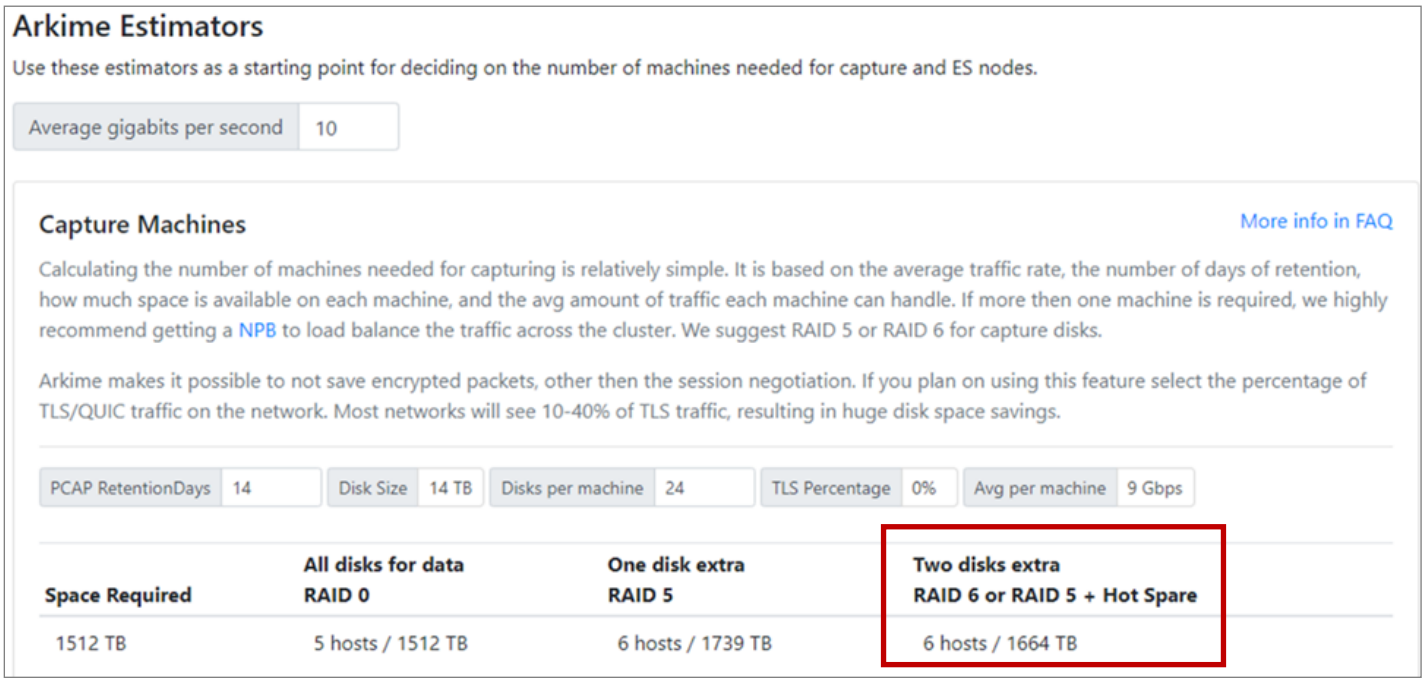
Fortunately, one of your Project Leads finds an open-source package called Arkime - a large scale, indexed packet capture and search tool. Great! And you start to get “smarter” on how this software package can get you to your goal.

At this point, I’m going to take you through the process I went through on the Arkime website to come up with a configuration and suggested vendors for servers to support the system. The Arkime site is really good and has a lot of helpful information and Estimators to help you decide on the number of machines needed for Capture and Elasticsearch (meta data) nodes, and storage. There is a YouTube video on the Official Elastic Community site by the authors, Andy Wick and Elyse Rinne.

Arkime Use Case

Our use case is to configure disks and servers required to build a Packet Capture System with 14 days retention, 10Gbit average sustained rate, and 40Gbit per second maximum capture rate.

Starting at the Estimators page I put in the following information and received a configuration for the Capture Machines and Elasticsearch machines, that I could then build.



Arkime Estimators

Use these estimators as a starting point for deciding on the number of machines needed for capture and ES nodes.

Average gigabits per second: 10

Capture Machines

More info in FAQ

Calculating the number of machines needed for capturing is relatively simple. It is based on the average traffic rate, the number of days of retention, how much space is available on each machine, and the avg amount of traffic each machine can handle. If more then one machine is required, we highly recommend getting a NPB to load balance the traffic across the cluster. We suggest RAID 5 or RAID 6 for capture disks.

Arkime makes it possible to not save encrypted packets, other then the session negotiation. If you plan on using this feature select the percentage of TLS/QUIC traffic on the network. Most networks will see 10-40% of TLS traffic, resulting in huge disk space savings.

PCAP RetentionDays: 14 | Disk Size: 14 TB | Disks per machine: 24 | TLS Percentage: 0% | Avg per machine: 9 Gbps

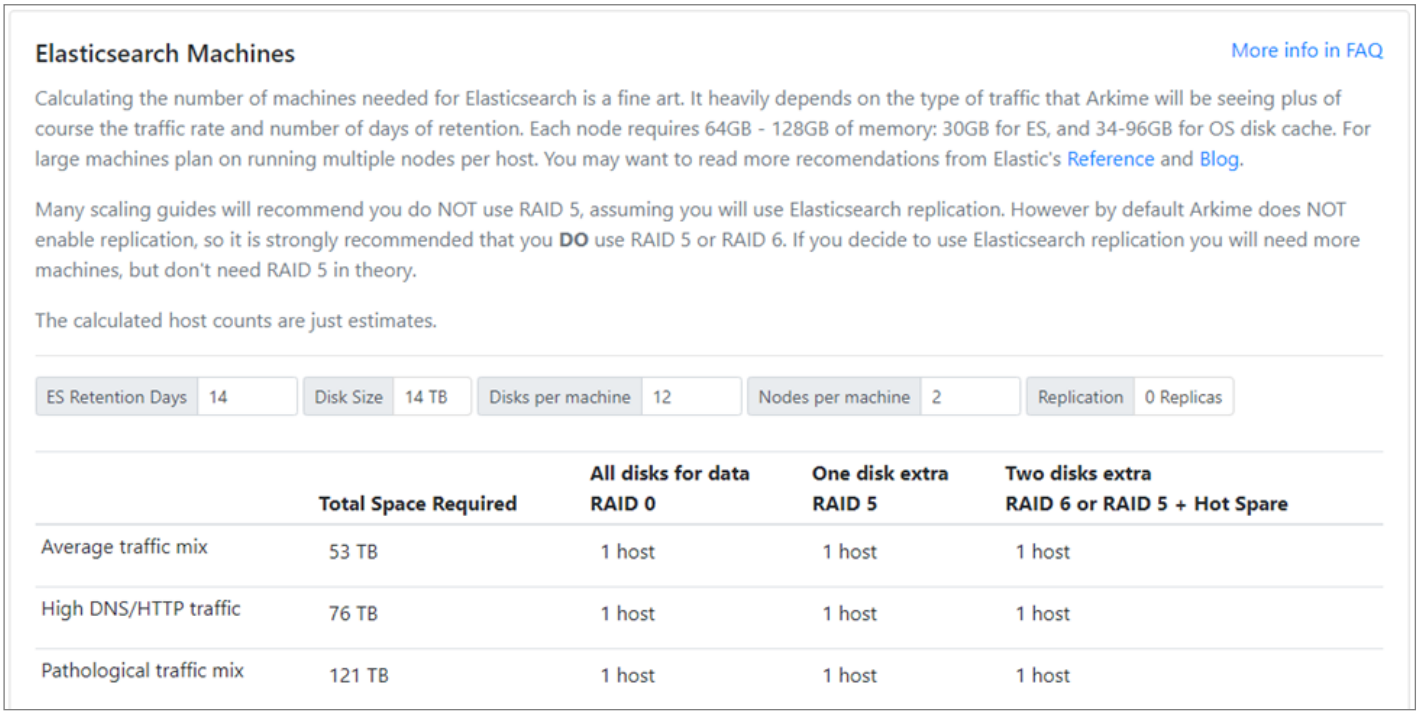
Space Required	All disks for data RAID 0	One disk extra RAID 5	Two disks extra RAID 6 or RAID 5 + Hot Spare
1512 TB	5 hosts / 1512 TB	6 hosts / 1739 TB	6 hosts / 1664 TB

Note: I want to capture all packets including encrypted so I set TLS to 0%, and I figured 10Gbits per server, but the pull-down didn't go any higher, so I put in 9Gbps.

I chose to use the RAID 6 solution so I will need 6 hosts/servers for Capture. Six servers with 24x14TB drives each = 336TB raw per server for a total of 2.016PB, approximately 1664TB useable, according to their calculations.

Arkime with Elasticsearch Machines

Next, I want to configure the Elasticsearch machines. Putting in this information, I noticed I could add less disks to this server and could go down to 8 disks before it increased the host requirement. I chose the full "pathological" traffic mix with one host and two nodes. As it says on the screen," Calculating the number of machines needed for Elasticsearch is a fine art." So, I may have to revisit this part.



Elasticsearch Machines

More info in FAQ

Calculating the number of machines needed for Elasticsearch is a fine art. It heavily depends on the type of traffic that Arkime will be seeing plus of course the traffic rate and number of days of retention. Each node requires 64GB - 128GB of memory: 30GB for ES, and 34-96GB for OS disk cache. For large machines plan on running multiple nodes per host. You may want to read more recomendations from Elastic's Reference and Blog.

Many scaling guides will recommend you do NOT use RAID 5, assuming you will use Elasticsearch replication. However by default Arkime does NOT enable replication, so it is strongly recommended that you **DO** use RAID 5 or RAID 6. If you decide to use Elasticsearch replication you will need more machines, but don't need RAID 5 in theory.

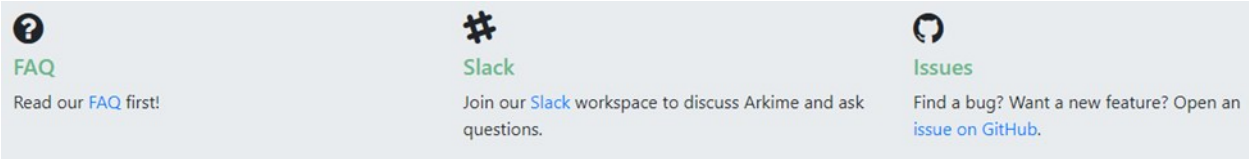
The calculated host counts are just estimates.

ES Retention Days 14 | Disk Size 14 TB | Disks per machine 12 | Nodes per machine 2 | Replication 0 Replicas

	Total Space Required	All disks for data RAID 0	One disk extra RAID 5	Two disks extra RAID 6 or RAID 5 + Hot Spare
Average traffic mix	53 TB	1 host	1 host	1 host
High DNS/HTTP traffic	76 TB	1 host	1 host	1 host
Pathological traffic mix	121 TB	1 host	1 host	1 host

Arkime Support

This topic is worth discussion since this is open-source software supported by a community of developers and engineers. In the financial model I assumed most IT teams would use GitHub or join the community to get support, and show that at no cost. On their website Arkime offers:



Elasticsearch Support

Additionally, there is support for Elasticsearch specifically, if that is needed. Elasticsearch is a distributed, free and open search and analytics engine for all types of data, including textual, numerical, geospatial, structured, and unstructured. Elasticsearch is built on Apache Lucene and was first released in 2010 by Elasticsearch N.V. (now known as Elastic). Known for its simple REST APIs, speed, and scalability, Elasticsearch is the central component of the Elastic Stack, a set of free and open tools for data ingestion, enrichment, storage, analysis, and visualization. Commonly referred to as the ELK Stack (after Elasticsearch, Logstash, and Kibana).

Like most open-source vendors their business model is to provide various levels of support of their Elastic Stack, and can be found here: https://www.elastic.co/pricing/

Things to Consider Before You Build

In this analysis I've assumed the "builder" has, or will provide skilled personnel to build, support and manage the packet capture systems. No external support is built into the pricing model.

Your support model becomes heavily dependent on a small group of people, within your organization, to keep the packet capture systems operational and secure. Here are a few things to consider:

- Ensure the hardware is compatible. The disk/RAID and NICs you choose will have a big influence on performance and reliability.
- Ensure that newly-published CVEs are acted on quickly to ensure the ongoing security of the platform.
- Enable proper integration with your enterprise services such as AAA, Logging, SNMP, etc.
- Integrate packet capture with all the other tools in your environment so you can streamline the workflow of Security Engineers and IT operations staff.
- Backup the development and support team members. If one of your main developers of the solution leaves or moves to another role you'll have a big hole in support. This can cause the project to stall or fail.

Server Selection

The FAQ section on Arkime has some good information on which hardware to consider: https://arkime.com/faq#what-kind-of-capture-machines-should-we-buy. For this report we chose to use two of their recommendations: Supermicro 6028R-E1CR24L and Dell EMC PowerEdge R740XD2.

Arkime Server Based on Dell EMC PowerEdge R740xd2

Let's start with a Dell EMC configuration since this is a popular server vendor and most businesses have a relationship with a partner to acquire their equipment.

Dell EMC PowerEdge R740xd2	Qty	Unit Cost	HDD (GB)	Total (GB)	Total Cost
Hardware					
Capture Servers (PowerEdge R740xd2 with 12 x 14TB drives)	6	$ 30,653	14,000	1,008,000	$ 183,918
Add-on Disk Drives (14TB)	72	$ 499	14,000	1,008,000	$ 35,928
Total Raw TB for Capture (1664TB after RAID6)				2,016,000	
Elastisearch Server (PowerEdge R740xd2 with 12 x 14TB drives)	1	$ 30,653	14,000	168,000	$ 30,653
Software					
Arkime Full Packet Capture	1	$ -	-	-	$ -
(Open source package capture application)					
Services					
Installation + Pro. Services (H/W included)	1	$ -	-	-	$ -
5-Year Maint. Per Server (included in server price)	7	$ -	-	-	$ -
Hardware/Software/Services TOTAL					**$ 250,499**

Notes on the configuration and pricing:

1. I put 12 x 14TB drives in each server instead of 24. I wanted to save some money on add-on disks and the Dell EMC price was almost 3x the "street" price for a Seagate 14TB drives.
2. The pricing from Dell EMC represents a 40% discount.
3. All ProDeploy and Warranty - Basic Next Business Day 60 Months, are included in the pricing.
4. No tax and shipping costs included

Arkime Server Based on Supermicro SuperStorage 6028R-E1CR24L

Next, let's see what a Supermicro configuration will cost.

Supermicro SuperStorage 6029P-E1CR24L	Qty	Unit Cost	HDD (GB)	Total (GB)	Total Cost
Hardware					
Capture Servers (Supermicro 6029P-E1CR24L with 24 x 14TB drives)	6	$ 20,775	14,000	2,016,000	$ 124,650
Total Raw TB for Capture (1664TB after RAID6)				2,016,000	
Elastisearch Server Supermicro 6029P-E1CR24L with 12 x 14TB drives)	1	$ 18,278	14,000	168,000	$ 18,278
Software					
Arkime Full Packet Capture	1	$ -	-	-	$ -
(Open source package capture application)					
Services					
Installation + Pro. Services (H/W included)	1	$ -	-	-	$ -
5-Year Maint. Per Server	7	$ 2,050	-	-	$ 14,350
Hardware/Software/Services TOTAL					**$ 157,278**

Notes on the configuration and pricing:

1. No tax and shipping costs included.
2. The pricing from Supermicro represents a 20% discount.
3. Installation costs are included in server.
4. 5-Year Next Business Day maintenance for each server is $2,050.

Comparing these two server vendors, you can see there is about $100K difference in the total hardware, installation and maintenance over 5 years.

Other Arkime Costs—Development and Support Personnel

Now that we've taken care of the hardware, software and maintenance required for our Packet Capture System, we now need to figure out the development and support costs over a 5-year period to complete our Total Cost of Ownership (TCO) analysis.

I came up with 2 scenarios for the Development and Support model using a Principal Systems Engineer, a Senior Systems Engineer, and a Junior Systems Engineer, and their respective average base salaries in $USD. You can choose one of these, a combination or change it according to your situation. I've included the numbers to guide you. (1). I chose these Engineers because you will need someone with development, integration and deployment skills/expertise. This person(s) will work with your other IT teams/departments, setup analysis tools to access the packet data and be the "go to" person(s) for all things packet related.

I used $131,000 average base salary for a Principal Systems Engineer (not including bonus, profit sharing, etc.) $108,000 average base salary for Senior Systems Engineer, and $60,000 average base salary for a Junior Systems Engineer. (Note: these are average salaries in Dallas, TX. Your location may be different.)

Here's the two scenarios I analyzed:

1. "GET IT DONE" put your Principal Systems Engineer on it for 6 months development, integration of tools, test and deploy. Bring on a Senior Systems Engineer 3 months into it (overlap) to bring it to completion and support it going forward. Sr. Systems Engineer will spend 1/2 time to support it after the 6 months.
2. "TEAM BUILDING" Put a Senior Systems Engineer and a Junior Systems Engineer on it together for 12 months development, integration of tools, test and deploy. Then the Junior Systems Engineer will spend 1/2 time to support.

On top of that I included 30% for each employee as the average overhead cost. (2)

During the first year we split up development and support costs according to each scenario. In years 2-5 we only included the on-going support costs. In Scenario #2 support costs don't kick in until year 2.

Other Costs - Development and Support Personnel	Mths.	Development	Total	Mths.	Support	Total
Scenario #1 - Principal SE for 6 months + Senior SE for 3 months, then Senior SE 1/2 time to support	6	$ 10,917	$ 65,500			
Senior Systems Engineer - Development & 1/2 time Support	3	$ 9,000	$ 27,000	6	$ 4,500	$ 27,000
Total Scenario #1 PLUS 1.3x for Overhead		**$ 155,350.0**				
Scenario #2 - Senior SE + Junior SE for 12 months then Junior SE 1/2 time to support	12	$ 9,000	$ 108,000	6	$ 2,375	$ 14,250
Junior Systems Engineer - Development & 1/2 time Support	12	$ 5,000	$ 60,000			
Total Scenario #2 PLUS 1.3x for Overhead		**$ 218,400.0**				

5-Year TCO for Complete Dell and Supermicro "Build" Scenarios

When we combine the hardware, software, maintenance, development and support costs for each scenario by each hardware vendor, we see very quickly that the bulk of the costs in this project are in the development and support over the years.

In our model we show at the end of the first year we have the equipment installed, configured and running, with all the associated costs. Years 2-5 we will be spending on personnel costs to support the system, keep it running, deploy it widely, work with network teams, etc. This cost can vary from $54,000 to $39,000 per year based on average annual salary for Senior and Jr. Systems Engineers in your location.

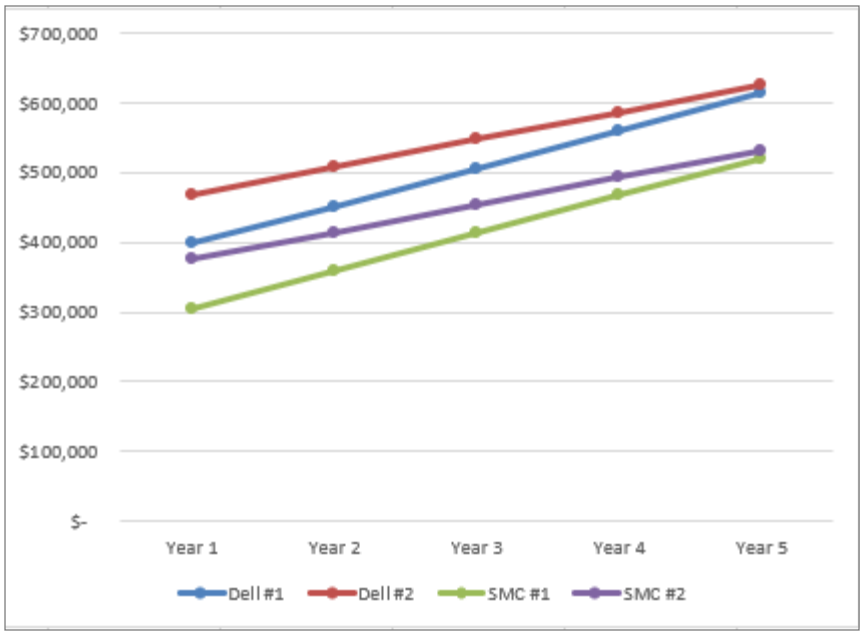
Dell EMC PowerEdge R740xd2		Year 1		Year 2		Year 3		Year 4		Year 5		Total	
Hardware/Software/Services TOTAL			**$ 250,499**		**$ -**		**$ -**		**$ -**		**$ -**		**$ 250,499**
Other Costs - Development and Support Personnel	Unit Cost	Qty	Cost	Qty	Cost	Qty	Cost	Qty	Cost	Qty	Cost	Qty	Cost
Scenario #1 - Principal SE for 6 months Development + Overhead	$ 14,192	6	$ 85,150	0	$ -	0	$ -	0	$ -	0	$ -	6	$ 85,150
Senior Systems Engineer - 3 months Development + Overhead	$ 11,700	3	$ 35,100										$ 35,100
Senior SE 1/2 time to Support + Overhead	$ 4,500	6	$ 27,000	12	$ 54,000	12	$ 54,000	12	$ 54,000	12	$ 54,000	54	$ 243,000
TOTAL Scenario #1			**$ 397,749**		**$ 54,000**		**$ 54,000**		**$ 54,000**		**$ 54,000**		**$ 613,749**
Scenario #2 - Senior SE for 12 months Development + Overhead	$ 11,700	12	$ 140,400	0	$ -	0	$ -	0	$ -	0	$ -	12	$ 140,400
Junior Systems Engineer - 12 months Development + Overhead	$ 6,500	12	$ 78,000										$ 78,000
Junior SE 1/2 time to Support + Overhead	$ 3,250		$ -	12	$ 39,000	12	$ 39,000	12	$ 39,000	12	$ 39,000	48	$ 156,000
TOTAL Scenario #2			**$ 468,899**		**$ 39,000**		**$ 39,000**		**$ 39,000**		**$ 39,000**		**$ 624,899**

Supermicro SuperStorage 6029P-E1CR24L		Year 1		Year 2		Year 3		Year 4		Year 5		Total	
Hardware/Software/Services TOTAL			**$ 157,278**		**$ -**		**$ -**		**$ -**		**$ -**		**$ 157,278**
Other Costs - Development and Support Personnel	Unit Cost	Qty	Cost	Qty	Cost	Qty	Cost	Qty	Cost	Qty	Cost	Qty	Cost
Scenario #1 - Principal SE for 6 months Development + Overhead	$ 14,192	6	$ 85,150	0	$ -	0	$ -	0	$ -	0	$ -	6	$ 85,150
Senior Systems Engineer - 3 months Development + Overhead	$ 11,700	3	$ 35,100		**$ -**		**$ -**		**$ -**		**$ -**		$ 35,100
Senior SE 1/2 time to Support + Overhead	$ 4,500	6	$ 27,000	12	$ 54,000	12	$ 54,000	12	$ 54,000	12	$ 54,000	54	$ 243,000
TOTAL Scenario #1			**$ 304,528**		**$ 54,000**		**$ 54,000**		**$ 54,000**		**$ 54,000**		**$ 520,528**
Scenario #2 - Senior SE for 12 months Development + Overhead	$ 11,700	12	$ 140,400	0	$ -	0	$ -	0	$ -	0	$ -	12	$ 140,400
Junior Systems Engineer - 12 months Development + Overhead	$ 6,500	12	$ 78,000	0	$ -	0	$ -	0	$ -	0	$ -	0	$ 78,000
Junior SE 1/2 time to Support + Overhead	$ 3,250		$ -	12	$ 39,000	12	$ 39,000	12	$ 39,000	12	$ 39,000	48	$ 156,000
TOTAL Scenario #2			**$ 375,678**		**$ 39,000**		**$ 39,000**		**$ 39,000**		**$ 39,000**		**$ 531,678**

5-Year Cumulative TCO for Dell and Supermicro “Build” Scenarios

Taking both the Dell EMC config. and the Supermicro config. and showing the 2 Development and Support scenarios (#1, #2), on a graph, we can readily see the difference in hardware, installation and maintenance costs between the two systems. And the difference between the Scenarios #1, and #2 in both configs. Fundamentally the cost between a Principal, Senior and Jr. Systems Engineer for the development phase. Either way you look at it, this is an expensive project.

5-Year Cumulative TCO for “Build” Scenarios



The “Buy” Option with Endace

Enterprise-Class Network Infrastructure

In this scenario, I can imagine that you work in an IT Department of a medium- to large-sized enterprise that realizes that effective, successful packet capture is best handled by a vendor who has a dedicated team of developers, tech support and maintenance personnel. An organization with people that wake up every morning thinking about packet capture and how to make it easier, more reliable, and have invested in the success of their customers.

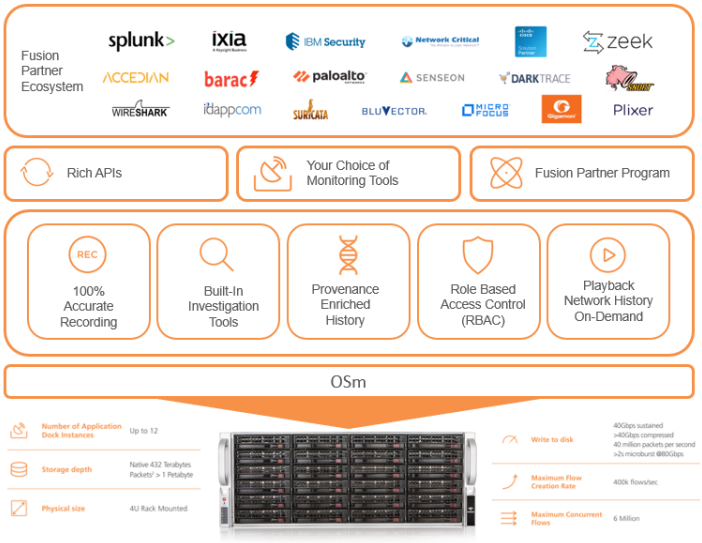
Instead of taking a general-purpose compute approach, they’ve created a purpose-built appliance that has unique and patented technology and expertise that you can leverage for your success. One such vendor is Endace. We’ve chosen their equipment to represent the buy-side of our financial model.

Using the same use case: configure disks and servers required to build a Packet Capture System with 14 days retention, 10Gbit average sustained rate, and 40Gbit per second maximum capture rate, we asked them for a configuration and pricing.

EndaceProbe 9200 G4 Series

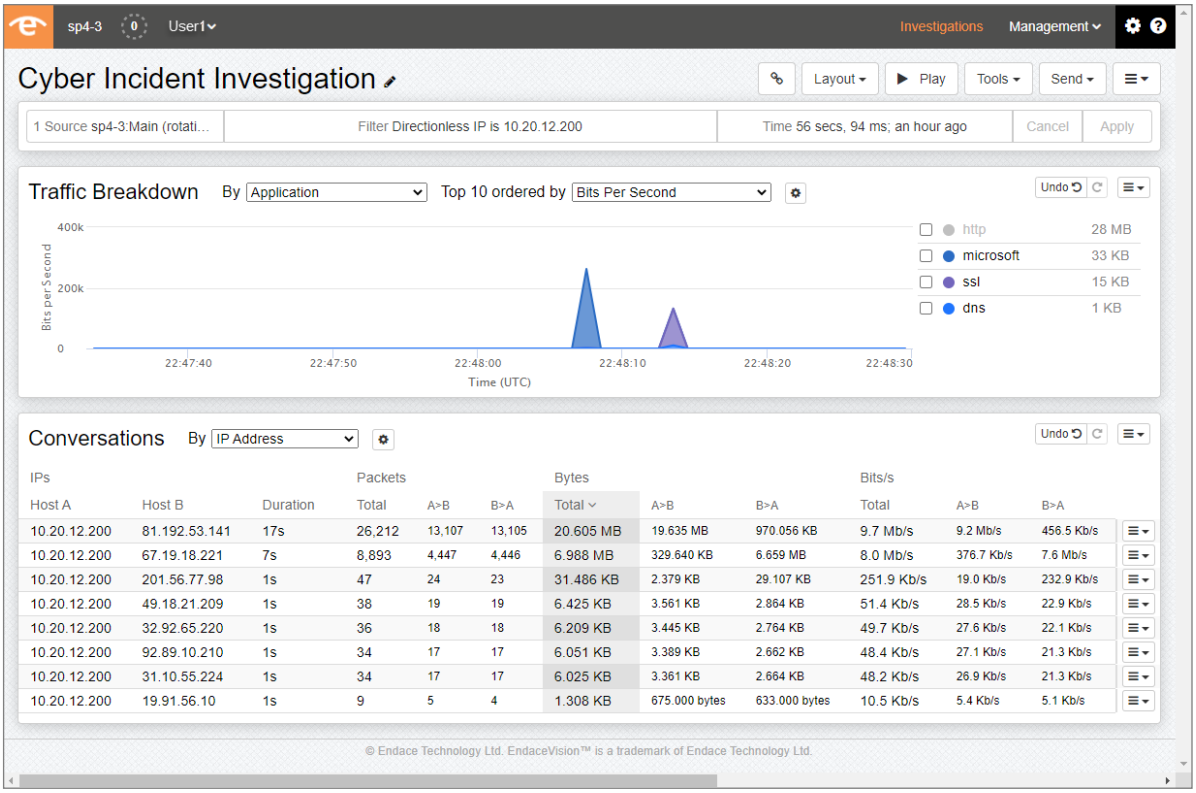
Endace provided an EndaceProbe 9200 G4 Series, a comprehensive platform for packet capture and analytics. The platform can be deployed in hours to days by an Endace engineer, includes a rich suite of software tools for investigation, security and playback, APIs, and can be enhanced with software upgrades from Endace.

And, by the way, the ultra-high capacity, high-performance appliance is capable of providing 100% accurate network history recording and Playback on up to eight 1/10GbE or two 40GbE links with dedicated hardware timing port (PTP/PPS/GPS) and 2 x 1/10G management ports, IPMI port. The 9200 provides sustained write speeds up to 40Gbps and 432TB of deep storage, in a 4U rack mount.



Browser-based Investigation Tools

Out-of-the-box, the 9200 G4 Series comes with EndaceVision™ and Wireshark hosted which enables powerful, browser-based investigation tools. EndaceVision enables network operations, security, or your incident response teams to quickly navigate through network data history, identify the cause of network performance or security issues, lowering your mean-time-to-resolution (MTTR). Wireshark provides on-probe decoding of packet history, removing the need for analysts to download large packet trace files for analysis.



I'm told that the 9200 G4 Series has enough CPU power to host up to 12 VMs. These VMs typically run network security sensors or network monitoring sensors supplied by 3rd parties or open source, which include: Palo Alto VM Series firewalls and Cisco Stealthwatch sensor. They've provisioned 24 cores (48 vCPUs), 144GB RAM and 600GB SSD for these applications in addition to the resources required to support capture.

EndaceProbe Analytics Platform for Ecosystem Partners

To support commercial and open-source applications and their need to access packet-level Network History, they've created Application Dock™. Endace has worked closely with technology partners to provide integrated workflows that reduce the time to resolve critical incidents. Out-of-the-box integrations provide one-click "pivots" from an event in a tool such as SIEM or Firewall, to the related packets captured by the EndaceProbe. These integrations are quick and easy to install, with no development required and they utilize the open Endace RestAPI to provide fast and accurate access to relevant network traffic.

Application Dock makes it easy to deploy open-source tools or custom applications with commercial solutions from their Fusion Partners. To me, this shows a strong commitment by leading vendors to support this product.

Patented Technology

Another measure of the maturity and sophistication of a product is patents. For customers that want to discard encrypted packets during the capture process, they can employ SmartTruncation that detects highly encrypted payloads and truncates them before hitting storage. A big storage space saver!

EndaceProbe Analytics Platform Cost

EndaceProbe 9200 G4 Series	Qty	Unit Cost	Total Cost
432TB up to 1PB (RAID and metadata overheads and assuming a 4.5:1 ratio for compression and Smart Truncation of packet data)	2	$ 132,000	$ 264,000
Accessories: Optics - SFP	4	$ 2,000	$ 8,000
Software			
EndaceVision (browser-based investigation tool - included)	2	$ -	$ -
Services			
Installation + Pro. Services - Customer Installable	0	$ -	$ -
First Year Maint. per EndaceProbe	2	$ 15,333	$ 30,666
Hardware/Software/Services TOTAL			**$ 302,666**
ADD $30,666 per year for Maintenance on 2 EndaceProbes			

Notes on the config and pricing:

1. No tax and shipping costs included.
2. The pricing from Endace represents a 22% discount.
3. Installation is done by the customer.
4. Maintenance is Advanced Replacement shipment within 1 business day.
5. Includes 1 day of setup assistance and ½ day of user training. Additionally training can be purchased as required.

Build vs. Buy Comparison

Costs Comparison

On a purely hardware, software, installation and maintenance basis Endace is more expensive than the Supermicro and Dell EMC configurations. But, with the "buy" decision you get a "ready to go" packet capture system, and a number of direct, significant benefits:

- No front-end development and system integration costs
- No on-going personnel costs (Systems Engineer) to maintain the system
- Faster time to market – put capture to use immediately
- Access to knowledge, training and support
- Ability to scale out the system quickly and easily as your needs grow
- Quick response to support issues. Imagine a complete company with support personnel to support you rather than a single person
- Ecosystem partners that have integration with your other tools such as SIEM, Security, SOAR, AAA, Logging, etc.

Additionally, when you buy a purpose-built system, it usually includes access to experts who can assist with the implementation and maintenance of their product. That's really important because in a "build" scenario, you run the risk of losing the required expertise when developers leave the organization.

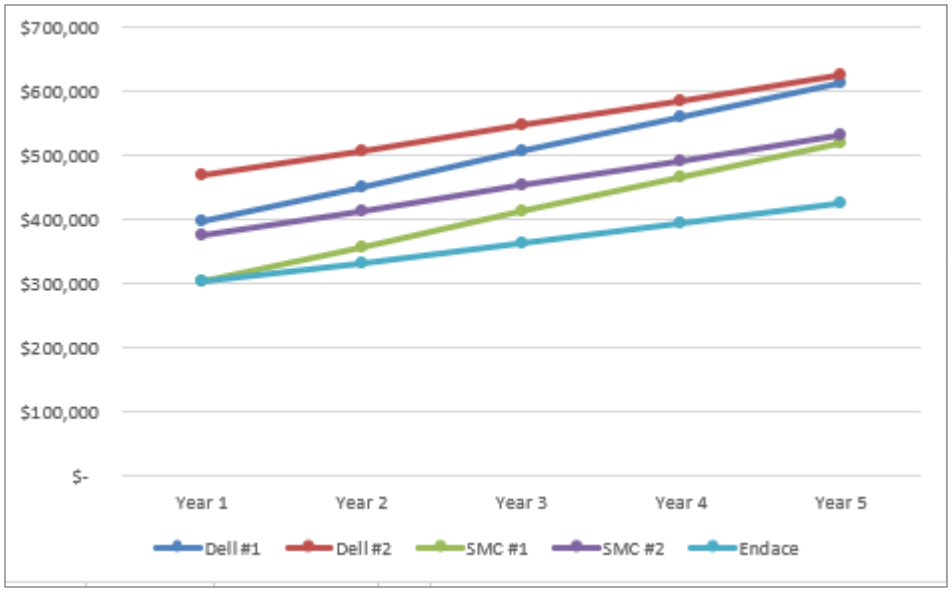
The cost of downtime is another factor to consider, when the "build" solution is "down" due to faulty hardware or software issues, one Engineer becomes the bottleneck for getting your security or IT operations team back online. Difficult server or software issues could result in days or weeks of downtime, or unreliable operation of the system that results in gaps in your data. The cost of data loss could be extremely high if it results in your inability to support the business with security incident response or IT operations troubleshooting of customer-facing services. How do we factor in that cost?

Build vs. Buy 5-Year TCO Comparison

TCO Comparison

Now taking into account all the costs including hardware, software, installation, maintenance, development personnel and on-going support personnel we get a complete picture.

5-Year Cumulative TCO Build vs. Buy Comparison



Putting the Endace costs up against the ongoing, yearly costs of Dell EMC or Supermicro with Arkime open-source packet capture software you can quickly see Endace and SuperMicro Scenario #1 are very close in the first year and then the personnel costs push SuperMicro and Dell EMC costs higher, in subsequent years. For Endace, the costs remain relatively flat over 2-5 years, and represent just the maintenance costs. Since you don't have development and support personnel costs you have a full packet capture system running from day -one, from a trusted source.

Risk Assessment

Build vs. Buy Risk

We would be remiss in our analysis if we didn't address risk. In any financial decision there is always an element of risk involved and it's our ability to mitigate any risks that arise, that will ensure our success.

In a "buy" decision, this is fairly straightforward. You can contact users, talk to other IT managers, check out blogs, user's groups, etc. to get a good feeling for what is involved in acquiring a purpose-built packet capture system, like EndaceProbe.

In a "build" decision there are a number of risks in the development phase, project timeline, expertise of personnel, on-going support, technical assistance when things go wrong – "who do you call?", and software updates and bug fixes from an open-source community, to name a few. Even if you are able to mitigate all these issues and complete the project, I think the nagging issues I would have are:

- Is the packet capture system we built good enough for our needs?
- Can it scale?
- Is it as good as other solutions in the market?
- Do we have a world-class system?
- What happens if my lead developer or support Engineer leave the company?
- How do you know if the system is capturing accurately and not dropping packets.

My home-grown system may not be as good, have quality issues, network issues, dropping packets, etc. The fear of not getting as good a system as you could get from a vendor who has experience, expertise and 1000s of successful installations in the field, is a risk I don't think I could mitigate.

The Bottom Line

Purpose-built Packet Capture Platform

Full Packet Capture (FPC) is a critical component of medium-large enterprise IT, network and security stacks. Streamlining incident response is a top priority along with access to full packet capture which enables your team to accurately and rapidly remediate any issue.

With today's increase in security threats and security alerts there is tremendous value in having a reliable, supported and well integrated solution. Our conclusion is that a "build" approach creates significant risk and in practical terms will likely cost your organization significantly more in the long term. These risks would be difficult to mitigate. Hence, we strongly recommend a "Buy" decision.

When it comes to lossless, real-time, time-stamped packet capture systems, the best acquisition route is from a trusted vendor, like Endace, that has years of experience and successful installations. Bottom line: the benefit of a purpose-built appliance is the same benefit specialization offers in other fields, such as medicine - when you focus on doing one thing, you tend to do it very well.

Build vs. Buy Comparison Chart

Capability	Build	Buy
100% accurate, continuous, real-time packet capture	Yes	Yes
No loss of packets during capture process	Yes	Yes
Scalable to meet your needs	??	Yes
Packet Capture software system with indexing and search tools	Yes	Yes
Easy to set-up, configure, re-configure, and operate	??	Yes
Quick response to support issues	N/A	Yes
Software updates, bug fixes, and enhancements on a regular basis	N/A	Yes
Security patches for emerging CVEs	N/A	Yes
Turnkey plug-n-play integration with an ecosystem of tools	N/A	Yes
No front-end development and system integration costs	No	Yes
Use Packet Capture system immediately	No	Yes
Cost of downtime	High	Low

Appendix

References and Links:

(1) Jr. Systems Engineering average annual salary, based in Dallas, TX.

Source: https://www.payscale.com/research/US/Job=Junior_System_Engineer/Salary

Senior Systems Engineer average annual salary, based in Dallas, TX

Source: https://www.payscale.com/research/US/Job=Senior_Systems_Engineer/Salary

Principal Systems Engineer average annual salary, based in Dallas, TX

Source : https://www.payscale.com/research/US/Job=Principal_Systems_Engineer/Salary

(2) Overhead Cost for Employees

Source: https://www.sba.gov/blog/how-much-does-employee-cost-you
Rule of thumb: 1.25 to 1.4 x their salary. (average 1.3x)

https://towardsdatascience.com/an-overview-on-elasticsearch-and-its-usage-e26df1d1d24a
https://www.trustradius.com/products/elasticsearch/reviews?qs=pros-and-cons
https://www.quora.com/When-should-we-not-use-Elasticsearch
https://www.endace.com/endacevision-overview.pdf

The Author

Tim Dales, VP of Labs and an analyst for IT Brand Pulse, a trusted source of data and analysis about IT infrastructure, including servers, storage and networking. A former executive for networking vendor Solarflare, product marketing and sales for a CDP startup, MTI, Emulex and the largest EMC VAR in South California. Mr. Dales has over 30 years experience in the development, marketing and sales of IT infrastructures. If you have any questions or comments about this report, contact tim.dales@itbrandpulse.com.