# Network Analytics

## Case-study

## 1. Introduction

This document describes the project undertaken by PalC Networks for developing **Network Analytics** application and infrastructure for our client – Aeverie Inc.

## 1.1. Network Analytics Introduction

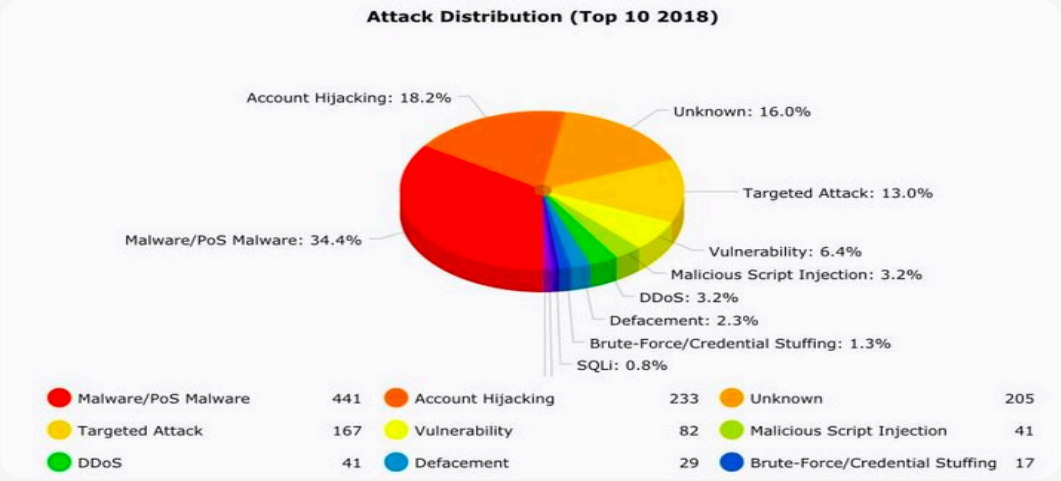
Network Analytics is a practice of the collecting and analyzing different types of network data like network events, state information, packets etc. to identify threats, trends, pattern of the network. This information will be later used to predict any real-time failures, better planning of the network for efficient usage of different components, securing the network and end points etc. Usage of Artificial Intelligence and Machine Language in network analysis helps the network be more adaptive with self-configuring, self- optimizing environment.

Growth in Data Centers:

- Multi Cloud / Hybrid clouds: In near future, there is going to massive growth in cloud data centers. The evolving Software Defined Data, telecom, IoT networks are becoming too complex to manually configure and maintain. Networks are evolving as they now support range of other functions than just packet transfer.
- Web/Hyper scale Data centers: There has been an explosion of wired and wireless data ranging from Social, Mobile, Video streaming, gaming and emerging heterogenous IoT sensors.
- Application and service visibility: Effective usage of Network analytics will not only give service providers and customers an understanding of network components but also help redefine service levels and contracts.
- Security risks, Identifying & troubleshooting issues: Numerous security threats (existing and new) introduced due to various solutions, protocols and applications. Network operational and maintenance challenges have been introduced due to the changing traffic patterns, rise of cloud services, rise of Big Data, consumerization of IT etc.

## 1.2. Current state of Network Attacks

Following is a sample of the top attacks seen in 2018:



## 1.3. 21st Century Crime Trending

While traditional homicide cases are generally trending downwards, other forms of technology-enabled crimes are skyrocketing, and surveys reflect the growing concerns of community members. Gallup has been surveying residents for nearly 20 years regarding their fears related to crime. The results of a poll published in November 2017, indicate that the public is most concerned about cybercrime, far more so than conventional criminal activity. Two-thirds of the respondents indicated that they are worried about having their identities stolen.

## 1.4. Emerging Infrastructure and Cybersecurity Threat Profiles

This section outlines some of the emerging data trends and the associated cyber security threats

### 1.4.1. Recent Threat Profiles and Analysis

Cyber security breaches have been in the center stage for several years and has not exactly been a ride in the park for cyber security professionals. Some of the highlight events so far last year have been the Shadow Brokers regularly dumping NSA hacking tools for public consumption, cybercriminals then using the seshiny new toys to run a mok producing WannaCry and Not Petya and most recently HBO being threatened with having its hottest show unveiled early unless a $6 million ransom is paid. So, will 2019 and beyond see a continued level of activity or will things calm down as the bad guys take a temporary hi at us? We see this as the biggest threats and problems that will be faced in the coming decades. This is a living list that we actively track with more threats being added as they appear.

**Malware with worm capabilities**: **Wannacry1** shocked the world by its rapid spread, and this wouldn't have been possible without its worm component. It reminded us of how quickly malware can propagate with devastating effects. Sadly, other malware authors have realized it also and are starting to add worm capabilities to their malware, such as recently with the Trick Bot banking trojan. Malware on cash registers at Arby's2fastfood restaurants in USA resulted in the breach of more than 355,000 credit and debit cards.

**Release of more Shadow Broker stools**: **EternalBlue and DoublePulsar,** the critical component of the WannaCry worm a repotentially just the tip of the iceberg of what may be coming from the Shadow Brokers. These sophisticated tools, in the hands of a less than a sophisticated adversary, had massive global impact. Expect more to come.

**Vulnerability of mobile carriers**: One of the more important security challenges facing most countries across the globe is the growing realization that the carrier networks that transport the world's voice and data communications are systemically vulnerable to interception and monitoring.

Hackers, terrorist organizations, foreign governments and others take advantage of these internetworking protocols and exploit them on a regular basis from anywhere around the world. In India, Reliance Jio3 has filed a police complaint against the recent cyber breach faced by the company. The registered complaint is in regard to the alleged "**unlawful access to Reliance Jio systems**."

**Growing Information Overload**: Security controls generate a lot of alerts that can easily. Overwhelm an organization. In large organizations such as banks, it is common to have over 100,000 security alerts per day. This requires a battalion of security engineers and analysts to sort through.

**Adapting the firewall to face new threats:** The evolution of the firewall is not complete. Networking technology is changing rapidly, and the firewall will have to adapt. Cloud, SDN and containers threaten the traditional role of the firewall. The traditional network segmentation is being replaced with very flat networks, which removes a lot of network complexity but introduces a significant challenge to the firewall. In India4 alone, in 2018 there were over 53,000 cyber security incidents like phishing, website intrusions and defacements, virus and ransomware attacks. In most cases firewalls and data protections were in place, but the security was circumvented due to advanced nature of the zero-day attacks.

**Monitoring Cloud Configuration and Security**: Organizations continue to adopt cloud technologies at a rapid rate, but information security isn't keeping up. There have been discovered misconfigurations leading to data leaks, but for every one of these found, there are likely many more that aren't published. With a rapid rate of technological change, huge variation of skills, and fast paced adoption, it's clear that monitoring cloud assets and infrastructure will continue to be a challenge. Cloud Storage Error exposed over Two Million Dow Jones 5 customer data records. InIndia6 a research report looked at four major government portals whose poor information security practices have exposed personal data including bank account details.

**High Impact Attacks**: The biggest challenges for network administrators are the impact due to a network security breach. No one can deny the destructive effect of attacks we encountered in 2018, from Shamoon v2, toWannaCry, and NotPetya, the world witnessed the power of malicious code at its highest impact to date. Organizations cannot ignore the overall increasing risk of highly advanced leaked code which has been used widely against organizations of all types and sizes and spreads quickly without discrimination. These attacks have shown us that it's not just simply an organization's customer data, trade secrets, or finances that are at stake entire operations have been shut down with devastating effects on business, employees and end users. The first few months of 20187 have seen an inordinate number of cyber security meltdowns. And they weren't just your standard corporate breaches.

**Insider Threats**: Many of the breaches seen in the last year were not the result of hackers penetrating the organization and stealing data from it, but employees and third-parties that have access to sensitive data for the sake of their work, that in some cases steal the data, where in other cases leak it by sending it accidentally to unauthorized recipients. The challenge with data breaches involving insiders and third-parties is double. Not only do the attackers have much more inside info than an external attacker, but since no malware is involved and no penetration happens through the organization perimeter, many of the common security mechanisms, like firewalls and anti-viruses, become blind to these attacks happening. In India rogue employees of operators of Aadhaar fingerprinting locations sold information over WhatsApp8 a popular mobile file sharing application.

1. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
2. https://www.usatoday.com/story/tech/news/2017/02/09/arbys-breach-may-have-hit-355000-credit-cards/97702594/
3. https://inc42.com/buzz/reliance-jio-cyber-breach-subscribers/
4. https://timesofindia.indiatimes.com/business/india-business/over-53000-cyber-security-incidents-observed-in-2017/articleshow/62851834.cms
5. https://www.forbes.com/sites/lconstantin/2017/07/17/cloud-storage-error-exposes-over-two-million-dow-jones-customer-records/#25bbadc199f6
6. https://www.wired.com/story/2017-biggest-hacks-so-far/

## 1.5. Cyber Attacks in India

India has not been immune to Cyber-attacks on Defense, Government, Public and Private entities.

**Learning from Global initiatives on Cyber Security**

**Effective regulations**: Cyber security and privacy acts have been introduced to ensure security is given the foremost importance. Existing regulations have been updated at periodic intervals to incorporate the smart city security perspective.

**Framework and standards for ecosystem**: Several countries across the globe including India have established cyber security frameworks and defined security and privacy guidelines in the context of smart cities. Baseline security standards and guidelines have also been introduced for different stakeholders.

**Collaboration and capacity development**: Cyber security information sharing platforms have been created for collaboration across sectors, including smart cities, finance and energy. A number of programs have been launched globally for building skills and capabilities in cyber security. A conducive environment has also been set up to promote cyber start-up hubs.

## 1.6. Emerging Trends are Driving Cyber-security Change

The key computing trends driving the need for a new cybersecurity paradigm are as follows:

**Changing attack patterns**: Increase in cyber-crime, espionage and sabotage by rogue elements against weak, mis-configured cyber security protocols. The ongoing shift of attack vectors, from the network to the user, is causing a reappraisal of how to manage security.

**The "Cloud Insecurity"**: Increasing amounts of data are being deployed from disparate parts of organizations, with more and more of that data ending up unsecured and transmitted openly without encryption over the internet. Despite the continual publicity around repeated breaches, the majority of organizations do not have good housekeeping deployed and enforced across their whole data estate in the cloud.

**The rise of cloud services**: Users expect on-demand access to applications, infrastructure, and other IT resources.

**The influence of Big Data**: "Big data" means more bandwidth. Handling today's mega datasets requires massive parallel processing that is fueling a constant demand for additional capacity and any-to-any connectivity.

**Rapid proliferation of the Internet of Things (IoT)**: The convergence of information technology (IT) and operations technology (OT) with IP-based networks as the backbone is enabling a Connected Enterprise. IoT is increasing the connectedness of people and things on a scale that once was unimaginable. Connected devices outnumber the world's population by ratio of 1.5 to 1. The pace of IoT market adoption is accelerating because of:

- Growth in analytics and cloud computing
- Increasing interconnectivity of machines and personal smart devices
- Proliferation of applications connecting supply chains, partners, and customers

**Complexity that leads to stasis**: Adding or moving devices and implementing network-wide policies are complex, time-consuming, and primarily manual endeavors that risk service disruption, discouraging network changes. Moreover, the data content for visual analytics would increase dramatically if the data were not analyzed in near real-time.

**Inability to scale**: The time-honored approach of link oversubscription to provision scalability is not effective with the dynamic traffic patterns in virtualized networks—a problem that is even more pronounced in service provider networks with large-scale parallel processing algorithms and associated datasets across an entire computing pool.

**Vendor dependence**: Lengthy vendor equipment product cycles and a lack of standard, open interfaces limit the ability of operators to tailor the application to their individual environments.

## 1.7. Key Business Challenges for Cyber-security operators

The key business challenges facing cyber-security operators are as follows:

### 1.7.1. Ransomware Evolution

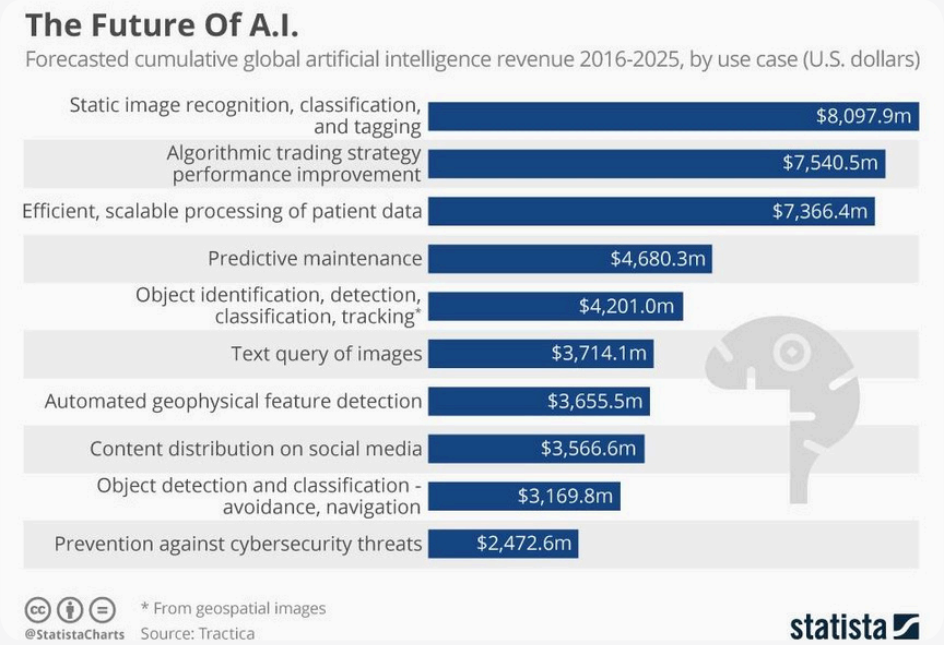
Ransomware is the bane of cybersecurity, IT, data professionals, and executives. Nothing is worse than a spreading virus that latches onto customer and business information that can only be removed if you meet the cyber criminals' egregious demands. And usually, those demands land in the hundreds of thousands (if not millions) of dollars.

In 2015, the number was 2.5 million. In 2017, it was at 3.5 million. And 77 percent of those applications are malware. 20 percent of businesses still don't have a disaster recovery solution. Which means that when a malicious attack comes — and it will — one-fifth of businesses have no method or plan for recovering data, applications, customer information, servers, or systems. And 42 percent of the businesses that do have a disaster recovery strategy use a tape-based, outdated backup method. In today's world of evolving ransomware, yesterday's DR strategies no longer work.

### 1.7.2. AI Expansion

The breaches are getting reported as historical events, long after something could have been done about it. Artificial intelligence could be used detect intrusions, malware and other vicious data manipulations.

Refer to the graph (fig 2) which indicates an approximate amount of investment in AI in near future



### 1.7.3. IoT threats

The widespread adoption of smart sensor devices, mobile computing platforms and applications is leading to an unprecedented explosion of broadband data to wireless and wired networks alike. Applications are stressing the network in unpredictable, transient, and in some unexpected ways. Legacy monitoring and analytics tools are no longer adequate to understand these new issues.
Insecure web interfaces and data transfers, insufficient authentication methods, and a lack of consumer security knowledge leave users open to attacks. And that truth is compounded by the fact that so many consumer devices are now interconnected. In other words, if you access one device, you've accessed them all. Evidently, with more convenience comes more risk. That's a risk that security professionals need to be prepared to face by integrating password requirements, user verification, time-out sessions, two-factor authentication, and other sophisticated security protocols.

### 1.7.4. Big Data Store

With boom of IoT devices and influx of data from a variety of devices in different formats, handling all the structured, unstructured and semi-structured data in a centralized data-lake will have its own set of concerns. Organizations want to extract value from that data, but the centralized nature of big data stores creates new security challenges; the data that was previously siloed and not delivering intelligence becomes a data compliance challenge and elevated security risk when correlated with personally identifiable data. Traditional tools alone are not up to the task of processing the information the data contains, let alone ensuring it's secure in the process. While controls need to be placed around the data itself, controls should also be placed around the applications and systems that store data.

## 1.8. IOT, IIOT and Cybersecurity

IoT will certainly have a pro found impact on IT at large, with large scale changes to existing cybersecurity strategies and operations because:

IoT introduces an avalanche of new devices, network traffic, and protocols to the mix. Large organizations are still figuring out the cyber security implications of mobile devices, cloud applications, and BYOD policies. As IoT devices prolife rate, they will require secure access to data collection appliances and analytics applications from inside and outside the secure confines of the IT network. Furthermore, IoT is likely to be an extremely heterogeneous world featuring a multi tudeo fraw devices and communications protocols that security professionals have little or no experience with. The security team will need the right skills and tools to identify IoT devices, secure IoT data and traffic, and recognize the difference between legitimate and suspicious communications.

IoT applications demand data security improvements. According to the Privacy Rights Clearing house, there have been 215 publicly disclosed security breaches since 2014, exposing over 8.5million personal records.1 Data breaches continue to plague large organizations because they lack the right processes and oversight for data discovery, classification, and security controls. IoT could increase the number of data breaches for several reasons. First, IoT will increase the amount of operational data by a factor of ten, so data security controls and practices will need to scale accordingly. Second, IoT applications will consume assorted data from outside the network, there by opening new threat vectors. Finally, the variety of IoT device types, locations, and security profiles will demand dynamic policy enforcement based upon the trust worthiness of devices and the integrity of IoT data.

IoT introduces physical and physiological risks. At a base level, network administrators and CERT teams are responsible for the protection of IT assets and data today, but IoT introduces additional risks. As organizations monitor and take actions, IoT introduces both physical and physiological risks. For example, a cyber-adversary could use IoT to compromise automobiles, shut down transportation systems, destroy industrial components, or alter medical devices. An example of this new and emerging threat was validated by a series of incidents namely: Stux net virus which disrupted a to micre search in Iran; researchers demonstrated how to hack an Insulin pump at the 2013 Black Hat security conference; and hackers have proven ninCBS60 minutes news feature, that it is possible to take control of critical automobile mechanisms, including brakes and steering controls.

The most likely IoT attack types as they relate to the IoT are as follows:

- Wired and wireless scanning and mapping attacks.
- Protocol attacks.
- Eaves dropping attacks (loss of confidentiality).
- Crypto graphical go rithm and key management attacks
- Spoofing and masquerading (authentication attacks)
- Operating system and application integrity attacks.
- Denial of service and jamming.
- Physical security attacks (for example, tampering, interface exposures)
- Access control attacks (privilege escalation)

## 1.9. Requirement

The requirement is to bring the infrastructure support and the security application to GRACE Analytics solution.

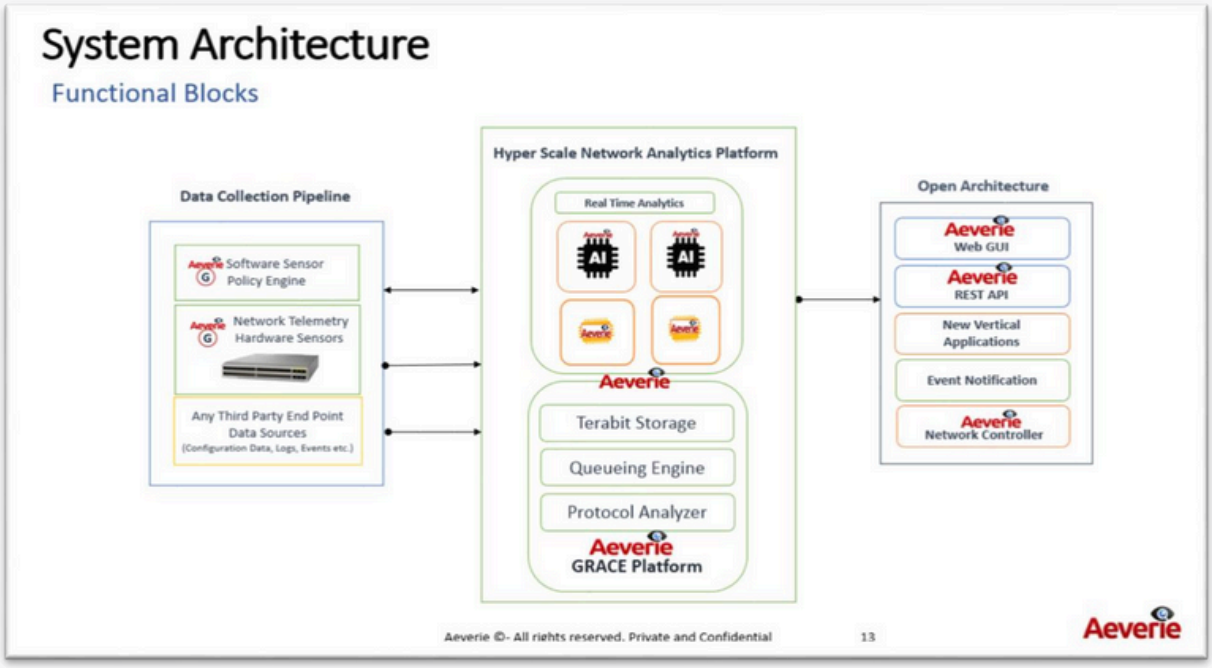
## 2.GRACE Analytics Solution

GRACE analytics solution will be a learning system capable of running in an adaptive mode by leveraging the advanced streaming analytics provided by a combination of Aeverie platform and suite of predictive analytics applications using machine learning and artificial intelligence.

This allows the operator to move from the current trial-and-error model of security to an automated proactive approach using unsupervised machine learning models in conjunction with advanced real time protocol analysis. Aeverie enabled software defined data, IIOT, IOT security platform can perform tasks for which, it has not been explicitly pre-provisioned or programmed, by dynamically adjusting the security behavior based on a series of real-time empirical observations and behavior analysis. GRACE analytics and security platform also allows the operators the ability to provide this capability in an “analytics as a service (AaaS)” to their internal and external customers.

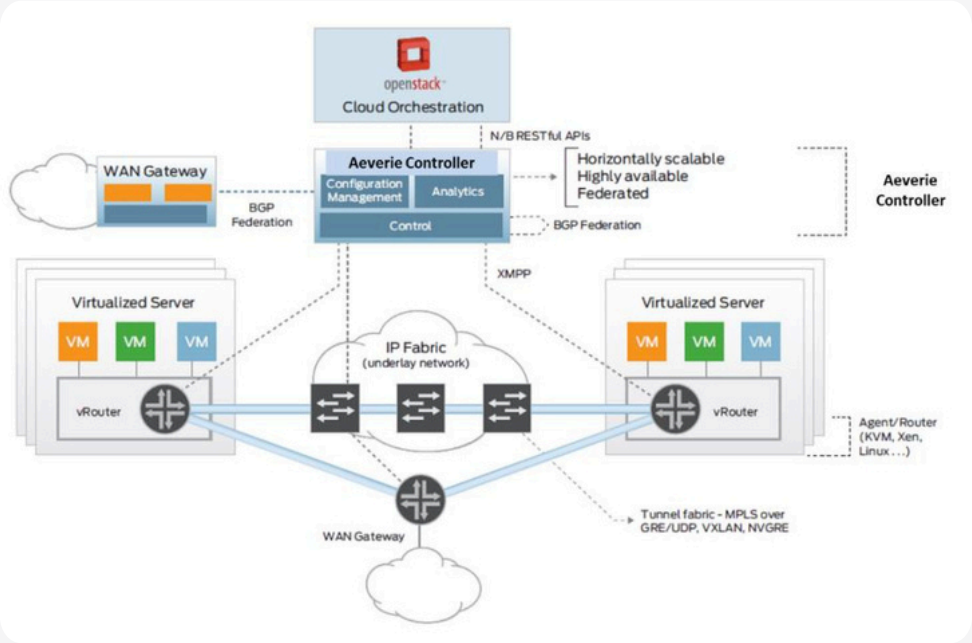
This case study will provide a comprehensive set of capabilities that includes data acquisition (streaming & batch), data cleansing and data loading on a massive data lake. Aeverie platform also provides a rich set of machine learning (ML/AI) libraries that will enable the Cyber Security department to build applications for security.

It provides real time visibility across all communication stack in your physical and virtual network. Aeverie Network Analytics platform provides behavior-based application insight using large scale unsupervised machine learning to build dynamic policy models which is used to automate real time policy enforcement.



## 2.1. Analytics Network Controller

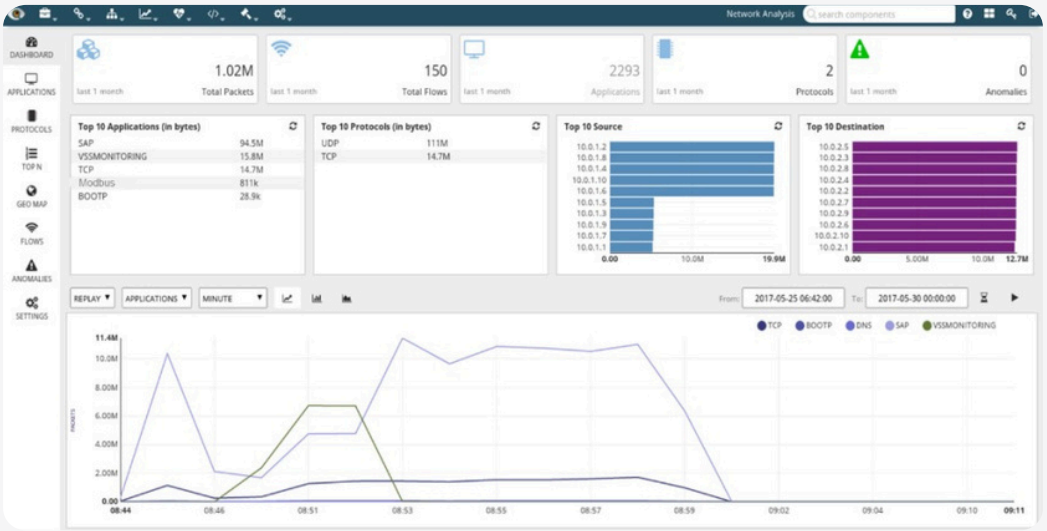
Network Controller automates network sensor resource provisioning and orchestration to dynamically create highly scalable virtual security analytics networks and to chain a rich set of Aeverie or third-party virtualized network functions (VNFs) and physical network functions (PNFs) to form differentiated analytic service chains on demand. Integrated with a cloud management platform such as OpenStack, the Network Controller enables the agile creation and dynamic scaling of service instances with high availability and reliability. The Controller also makes it really simple to onboard analytic network functions onto the platform without requiring any API integration or modifications to third-party service software. The Controller's advanced analytics capabilities provide deep insights into application and infrastructure performance for better visualization, easier diagnostics, rich reporting, custom application development and machine automation. The controller also interfaces with network policy engines and network elements and sensors to enforce network policy.




## 2.2. Presentation layer

The Portal enables consumption of this data through an easy-to-navigate and scalable web GUI and through representational state transfer (REST) APIs. GRACE platform also provides Apache Kafka based push notification to which northbound systems can subscribe to receive notifications about policy compliance deviations, flow anomalies, etc. Advanced users have access to the built in data lake and can write custom applications using programming languages such as Python and Scala that are run on the platform using the powerful computing resources available.


GRACE provides a state-of-the art, customizable, visual dashboard that presents information and insights in a clear and understandable format, providing high-level summaries while still allowing a user to go as deep into the data as required.




- Top 10 Protocols - Displays top 10 protocols determined by their packet size from last one month`s data present in the network flow table.
- Top 10 Source - Displays top 10 Source IP address determined by their packet size in last one month`s data present in the network flow table.
- Top 10 Destination - Displays top 10 Destination IP address determined by their packet size in last one month`s data present in the network flow table.
- Live Streaming - Displays Live packet data. Every 5 seconds interval, data is fetched from the database for duration of last 1 minute and displayed in line/bar/area chart. This helps user to analyze the total packets per second in the network and detect any unusual activity like packet size has spiked more than normal. By default, packets are grouped by applications. Grouping can be changed to None, Applications and Protocols.

- Replay Streaming - Re-plays packet data flow in the network between selected time intervals. Start time and end time can we selected for replay. Grouping of packets is similar to live streaming.
- Total Packets Count - Displays record count for last one month`s data present in the network flow table. Since each record is a packet data, it is displayed as total packet count. Time range can be changed in Settings.
- Total Flows - Displays flow count for last one month`s data present in the network flow summary table. Time range can be changed in Settings.
- Applications - Displays total number of applications available in network flow summary table for last one month`s data. Time range can be changed in Settings.
- Protocols - Displays total number of protocols in last one month`s data present in the network flow summary table. Time range can be changed in Settings.
- Anomalies - Displays number of anomalies occurred in network flow for last one month`s data present in the network flow summary table. Time interval can be changed in Settings.
- Top 10 Applications - Displays top 10 applications determined by their packet size from one month`s data present in the network flow table.

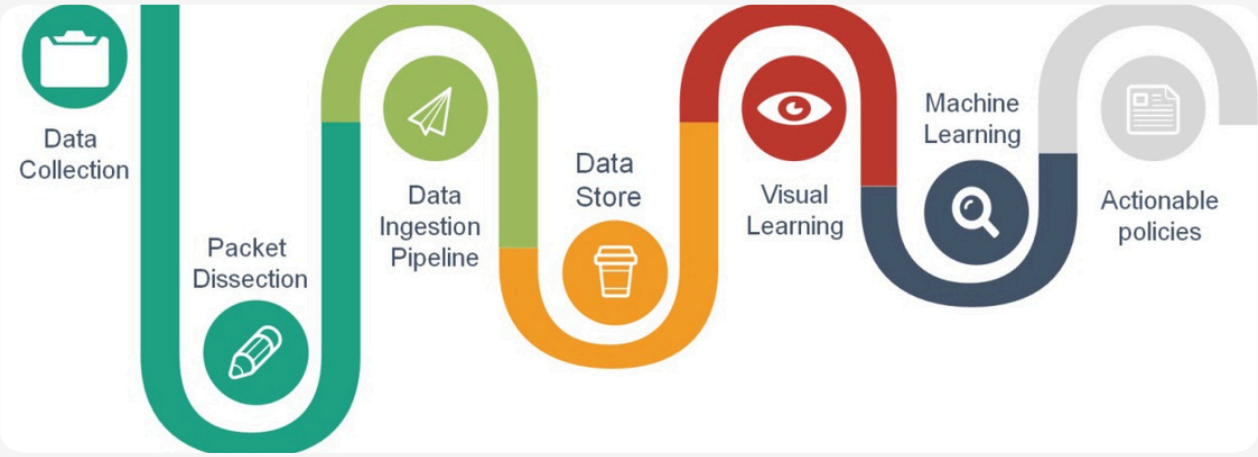
Geo Map: Tell where the traffic comes from, and where it goes, in geographical term; Get information of packets based on geo location; can view the transfer rate of packets using geographical map.

## 3. Features to be supported

- High-performance, real-time analytics with high scalability and low latency for various sources of data. Collect real-time data from application components and apply behavior-analysis algorithms to identify application groups and their communication patterns and service dependencies.
- This is in turn used to automate whitelist policy recommendations for zero-trust security. The telemetry data from every packet in the data center is collected and analysis is performed on millions of events to provide comprehensive actionable insight from billions of records within seconds.
- Long term data retention and playback without loss of detail is also available to simulate and analyze problems after the fact for future use case scenarios.
- Run analytics on the big data to acquire real-time actionable insights of what is happening in the datacenter and display it on the GUI as shown above.

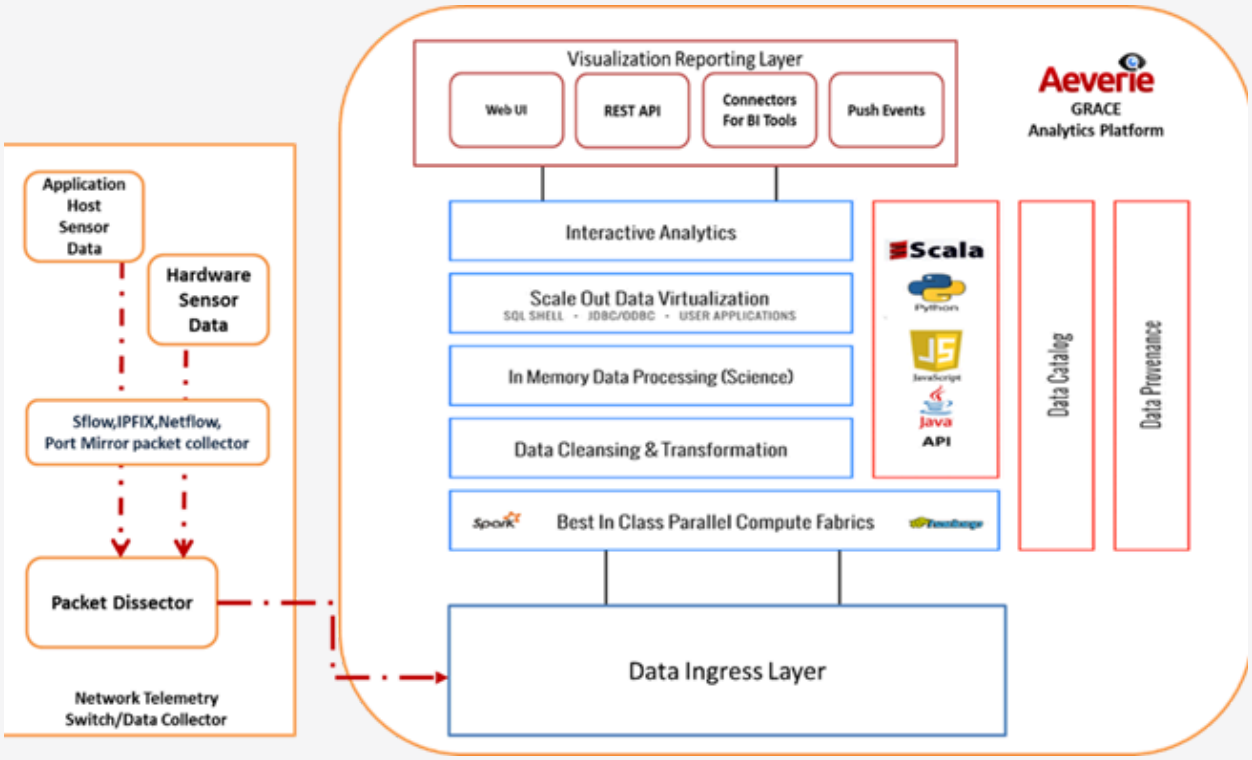
## 4. Approach

The workflow for GRACE Analytics platform is shown below:




Network Telemetry data is collected using Aeverie's purpose-built sensors and enforcement points. Two types of sensors are used: hardware sensors and software (endpoint) sensors. These sensors allow the network analytics and enforcement solution to support both existing (brownfield) and new (greenfield) network infrastructure.

The overall infrastructure of GRACE Platform is shown below:



## 4.1. Software and Hardware Sensors

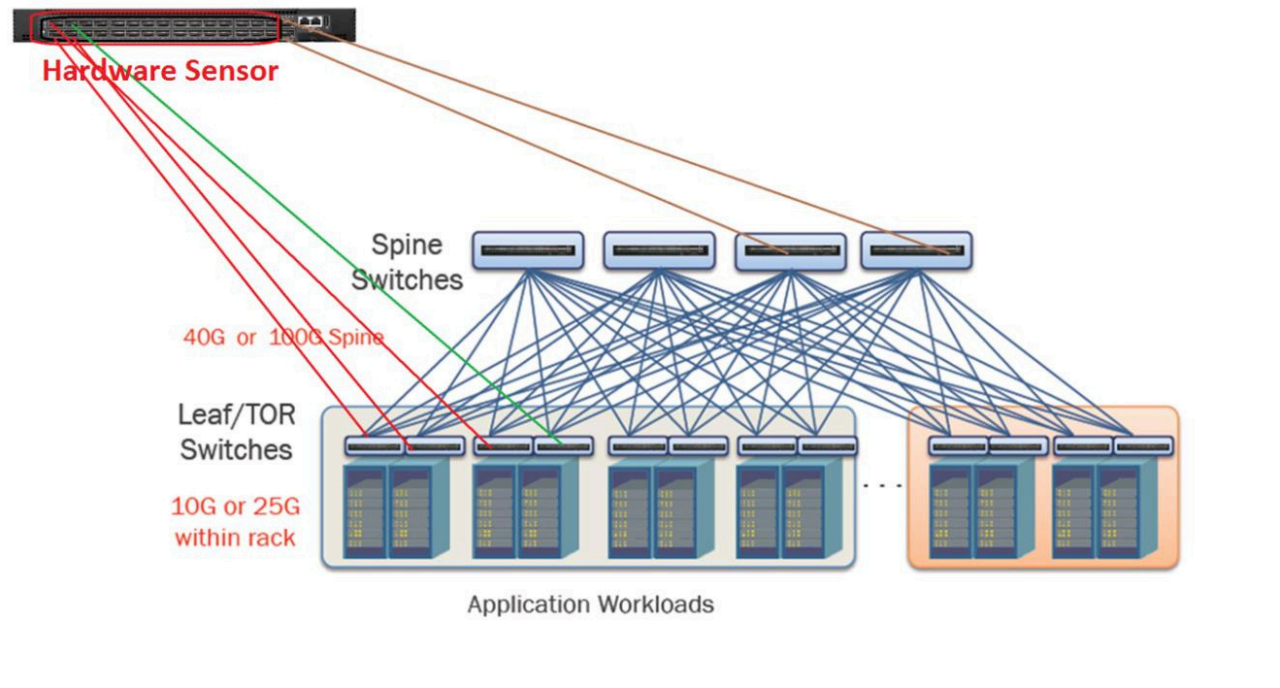
The GRACE Network Analytics platform has the following main functional layers:
Telemetry DATA Ingestion Layer: This layer consists primarily of sensor functions. Sensors are the eyes and ears of the analytics platform. Two types of sensors are used:

**Software sensors**: These lightweight sensors run as user processes and can be installed on any server (virtualized or bare metal). Two types of software sensors are used: full-visibility sensors and limited-visibility sensors. Limited-visibility software sensors are designed to collect connection information to support specific IoT Security Analytics use cases. These sensors are not designed to provide comprehensive telemetry data. The sensors also enforce network security on the network, IoT and IIOT edge gateways in real time working with network firewalls and security applications. It requires 1.5kB DRAM and about 5-6 kB for storage, so it is very resource friendly.


The software sensor provides actionable insight as follows.

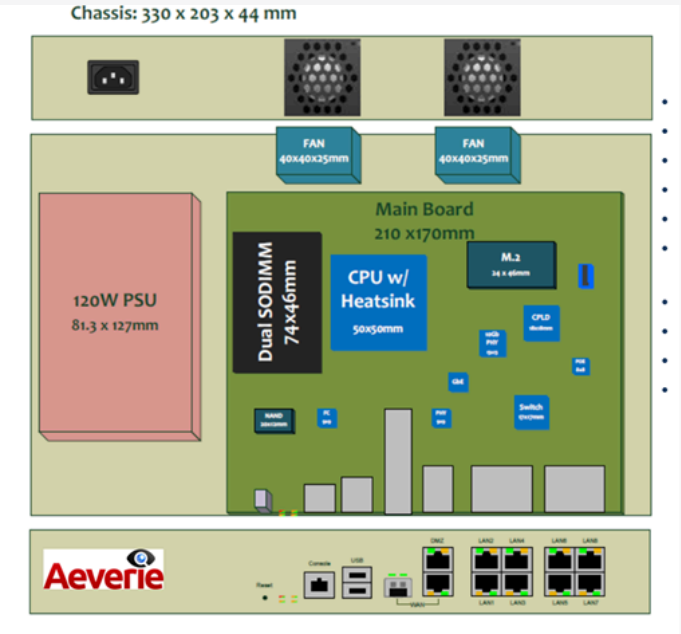
- What is happening inside the server?
- Why my server is very slow?
- Which application is taking more CPU resources?
- Is there any application which has any memory leaks?
- Is there any application running inside the server is compromised and can cause potential harm to the network
- Can I provision more VMs / application containers inside a server?
- Whether the mission critical application has availability of right set of resources?
- How the OS treats this application in terms of scheduling and allocating the memories?
- How well the application program is written?
- Whether it has too many I/O operations which causes poor performance of application?
- What is the relation between this application and other applications running in the network?

Hardware sensors: These sensors are embedded in 10/40/100 Gbps open compute switches from DELL, ACCTON, HPE, DELTA for large scale industrial settings or on an Appliance form factor in remote settings for IoT field deployments. It is usually placed adjacent to ToRs and Leaf node in the Data Center.



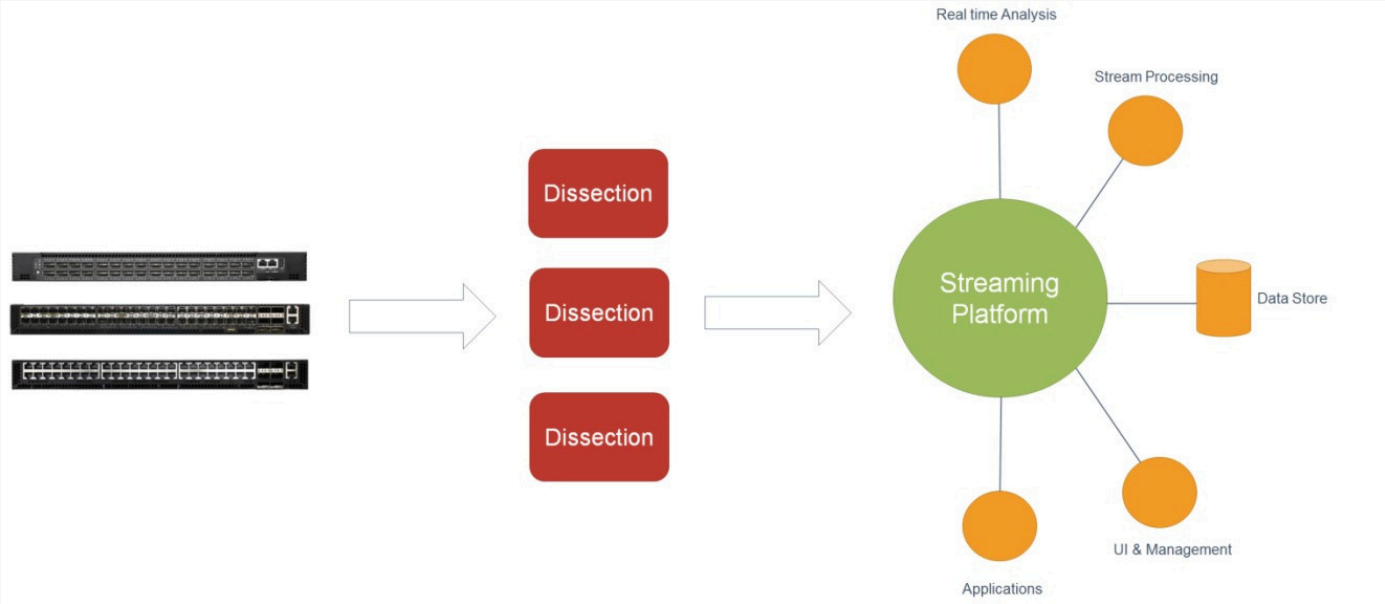

The Aeverie Network Analytics platform can work with only software or only hardware sensors. Standard deployment consists of hardware and software sensors, and they provide the following functions:

- Hardware sensors provide full visibility into application process-related context details.
- Hardware sensors act as enforcement points to enable application segmentation.




- Intel Denverton-NS SoC (14nm, BGA)
- DDR4 2133MHz SODIMM support
- 2x GbE RF45/SFP Combo ports for WAN, DMZ
- 8 x GbE LAN, support 4x POE PSE (2x 802.3at or 4x af)
- Built-in Intel QuickAssist Technology
- Symmetric Cryptographic Engine, Public Key Engine, Compression/Decompression Engine
- 2x mini PCI Express Expansion Slot (Zigbee/Any future)
- WiFi 2.4/5G dual band, 2x2 MIMO, with total 2 antennas
- Multi level storage support by eMMC, M.2 SSD/ 2.5" Disk
- Two form factors

Hardware sensors provide packet level details, buffer details, tunnel endpoint mappings, detect traffic bursts. Hardware and Software sensors provide measurement of network latency and application latency. Software sensors and the hardware sensors collect three types of telemetry information:




**Flow information**: This information contains details about flow endpoints, protocols, and ports; when the flow started; how long the flow was active; etc.

**Inter-packet variation**: This information captures any inter-packet variations seen within the flow. Examples include variations in the packet's time to live (TTL), IP/TCP flags, and payload length.

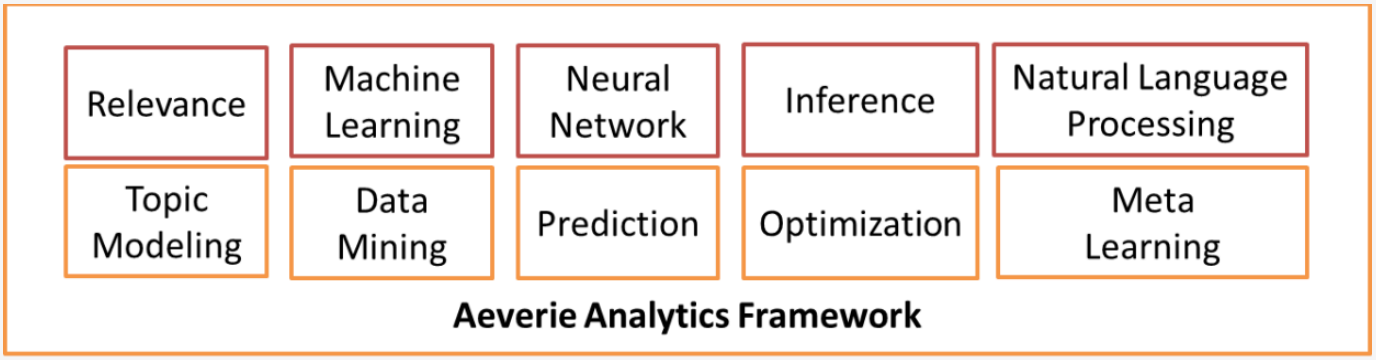
**Context details**: Context information is derived outside the packet header. In the case of a software sensor, this information includes details about the process, including which process generated the flow, the process ID, and the user associated with the process.

## 4.2. Analytics Layer

Proprietary machine learning based algorithms enable signature-less flagging of anomalous traffic patterns, only using Network Flow data. Get an alarm when the network is under attack.

Aeverie Grace machine learning based algorithms perform behavioral analysis on the incoming Network Flow data, and highlight traffic patterns that are unusual, extreme, or threatening.

Our analysis learns what services exist in your network, and avoids raising false alarms for their usual activities. Since we do not rely on pre-programmed traffic signatures, you don't need to fine-tune them endlessly.




The Grace Network Analytics ML (Machine Learning) layer brings in the following functionalities to the user

- Model Generation
- White-list and Black-list policy generation
- Zero-trust model
- Application dependency matrix
- Network and application performance insights
- Traffic Anomaly Detection
- Insider Threat
- Cyber Network Attacks

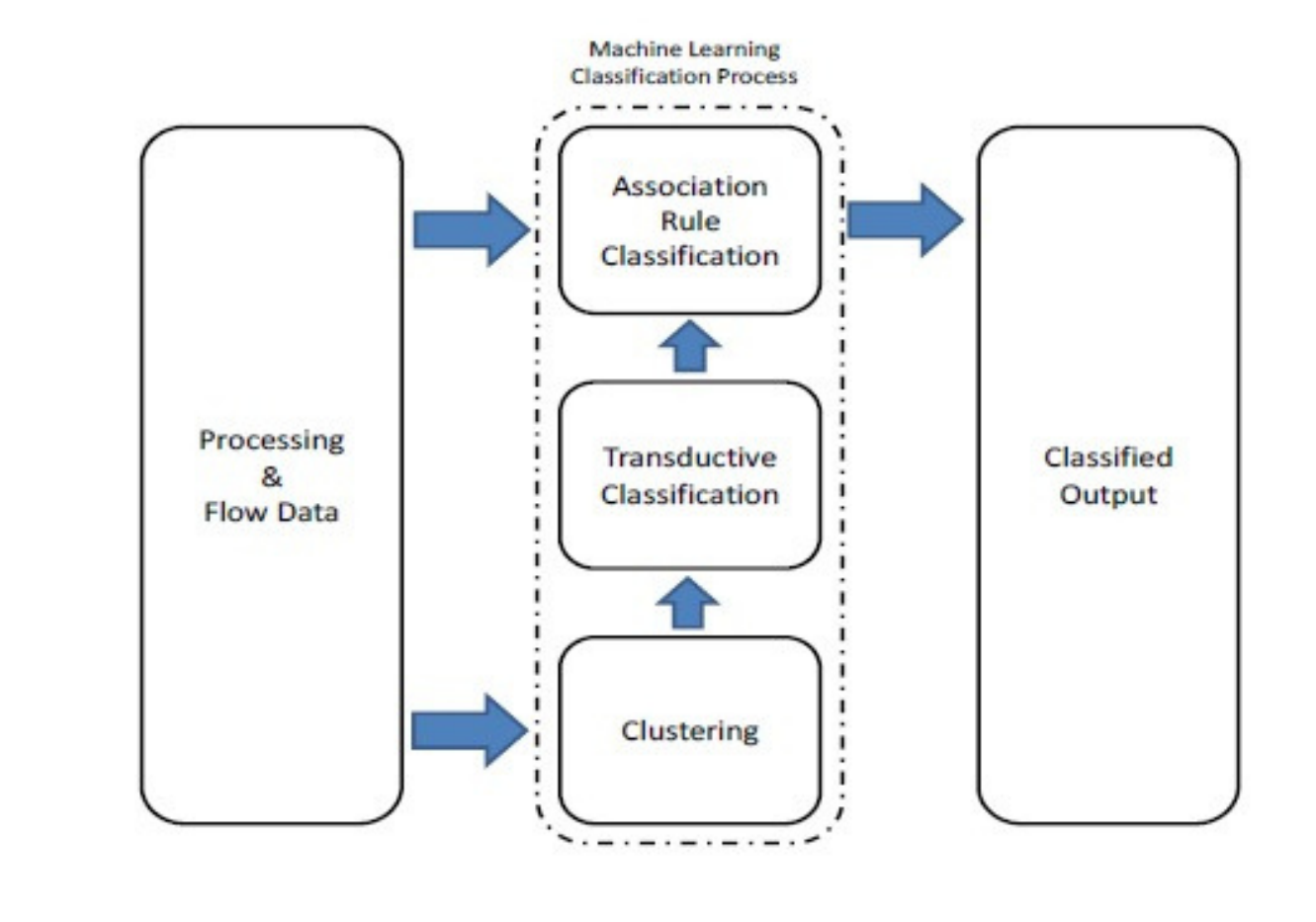
1. DOS & DDOS
2. Man in the middle attack
3. Database Ingestion Attack
4. Malware

- Protocol Based Attacks

5. DNS
6. Fork Bomb
7. HTTP Flood
8. IP Fragmentation Attacks
9. NTP Amplification
10. Flood Ping / Death Ping
11. TCP SYN Flood
12. UDP Flood
13. Etc.

There are five stages in the analysis of network packet data. The first two stages are taken care by Aeverie's network analytics ingestion pipeline. The last three stages will be done on SAP HANA.

- Baselining
- Transductive Classification
- Clustering
- Association Rule Mining
- Anomaly Detection




Baselining the data involves converting all the collected data from different sensors and store it in a database. The Grace platform has three different types of databases as

**Baselining**: The ingestion pipeline takes all the packets which are flowing in the network using Aeverie's Analytical switch and dissects the packet headers information. The dissected packet header information is then stored in the appropriate tables in Aeverie database after performing pre-processing of packet, based on the type of packets.

- Hot Storage
- Warm Storage
- Cold Storage

**Classification**: Along with saving the packet header information, the ingestion pipeline also does the transductive flow classification by identifying the application and application group using Deep Packet Inspection methodologies. The traffic classification can be broadly divided into

- Port and packet payload-based classification
- Statistical measurement-based approaches
- Unsupervised ML
- Supervised ML
- Behavioral identification techniques

This pre-processed classified data is used for next step which is clustering

**Clustering**: One of the prominent unsupervised clustering techniques is the K-means clustering algorithm preferred over other methods such as hierarchical clustering, due to its enhanced computational efficiency. Using unsupervised K-means, flows belonging to individual applications are separately cluster analyzed to extract unique subclasses per application, offering a finer granularity of the classification

## 4.3. Enforcement Layer

Software sensors act as the enforcement point for the detailed application policy generated by the platform, helping enable application segmentation. Using the data from the sensors, the GRACE Network Analytics platform provides consistent enforcement across public, private, and on-premises deployments. This layer also helps ensure that policy moves along with the workload, even when an application component is migrated from a bare-metal server to a virtualized environment. In addition, the enforcement layer helps ensure scalability, with consistent policy implemented for thousands of applications spanning tens of thousands of workloads.

**Sample Use Case Pattern**

Use Optimized algorithmic support for:

- Common stream data processing
- Complex event processing

Created Sensor Data fusions

- Generate Whitelist and policy mapping
- Detect Unusual Events occurring in stream(s) of data
- Post Detection, Isolate & Analyze Root Cause

Anomaly / Outlier Detection using unsupervised machine learning

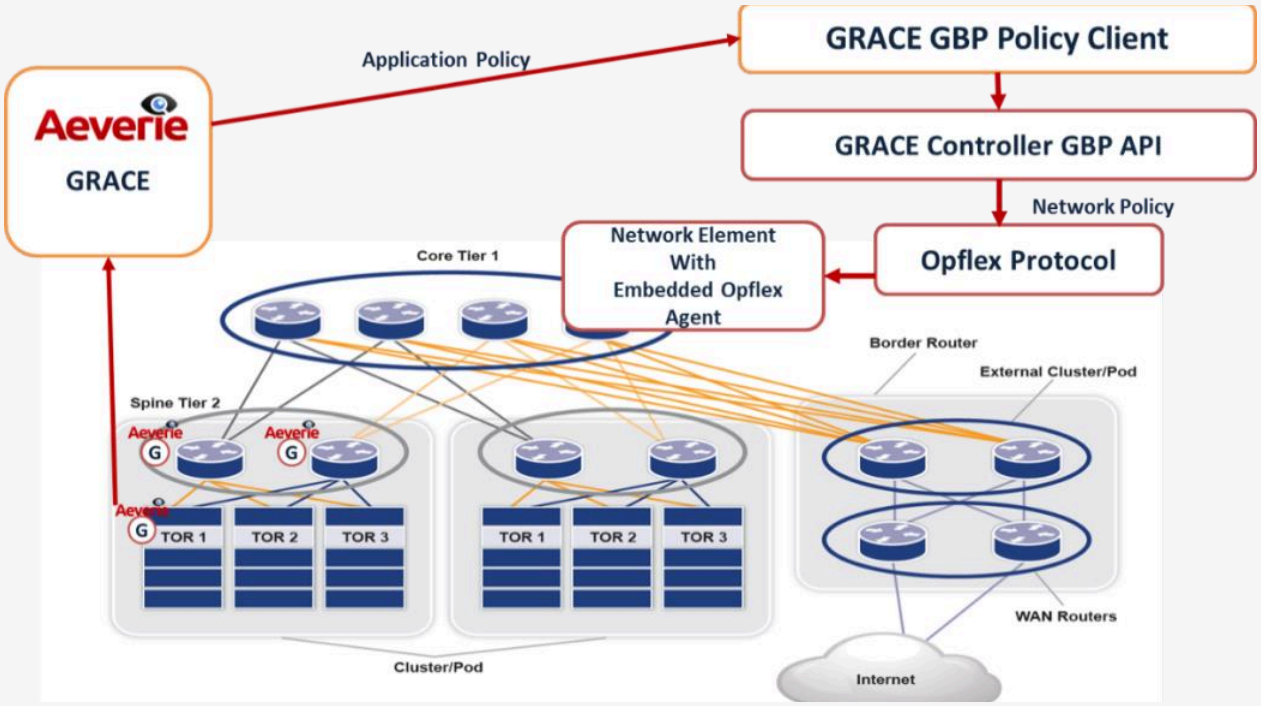
Commonalities / Root Cause Forensics

- Event Chaining
- Prediction / Forecasting
- Actions / Alerts / Notifications

Create Automated Targeted Control Actions

- Distribute Whitelist policy

Create filter specification dynamically when zero-day attack occurs and send it via routing protocol updates to network elements for control action to prevent malicious traffic




Aeverie IoT Security Solutions work together to provide protection throughout the attack continuum and also that can be integrated with complementary solutions for an overall security system:

**Before an attack**: Discover threats, and enforce and harden policies with existing Firewalls, Identity Services appliances, and Network Access Control (NAC) products.

**During an attack**: Detect, block, and defend against attacks that have already penetrated the network and are in progress with existing and next generation intrusion prevention web security systems.

**Post attack**: Scope, contain and remediate an attack to minimize damage in conjunction with deployed malware protection using real time network behavior analysis

## 5. GLOSSARY

**NAC**: Network Access Control
**DOS**: Denial of Service
**TOR**: Top of the Rack
**SDN**: Software Defined Networks