UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

NETWORK FORENSIC ANALYSIS IN THE AGE OF CLOUD COMPUTING.

The old mantra of "trust but verify" just is not working. "Never trust and verify" is how we must apply security in this era of sophisticated breaches. (Anthony Burke)

César de la Torre,
UFA-ESPE

Marco de la Torre,
Wroclaw University of Technology.

INTRODUCTION

- In the past, the principal ideas of IT security had focused on perimeter defenses; for example, firewalls, proxies, and content filtering.
- The idea of cloud computing has dramatically changed from the last mentioned concepts, due to new ideas to implement corporate IT services over the Internet.
- The process generated by virtualized applications, running in hosted servers and accepting network connections, are denominated cloud services.
- Clouds are classified in publics and privates, it also exists hybrid clouds as a mixed of the before mentioned. A public cloud sells services to anyone on the Internet and the administration is out of enterprise´s control; on the other hand, a private cloud is a proprietary data center or network infrastructure that supplies hosted services to a limited number of users.

DISTRIBUTION OF SOFTWARE AND HARDWARE IN A INFRASTRUCTURE

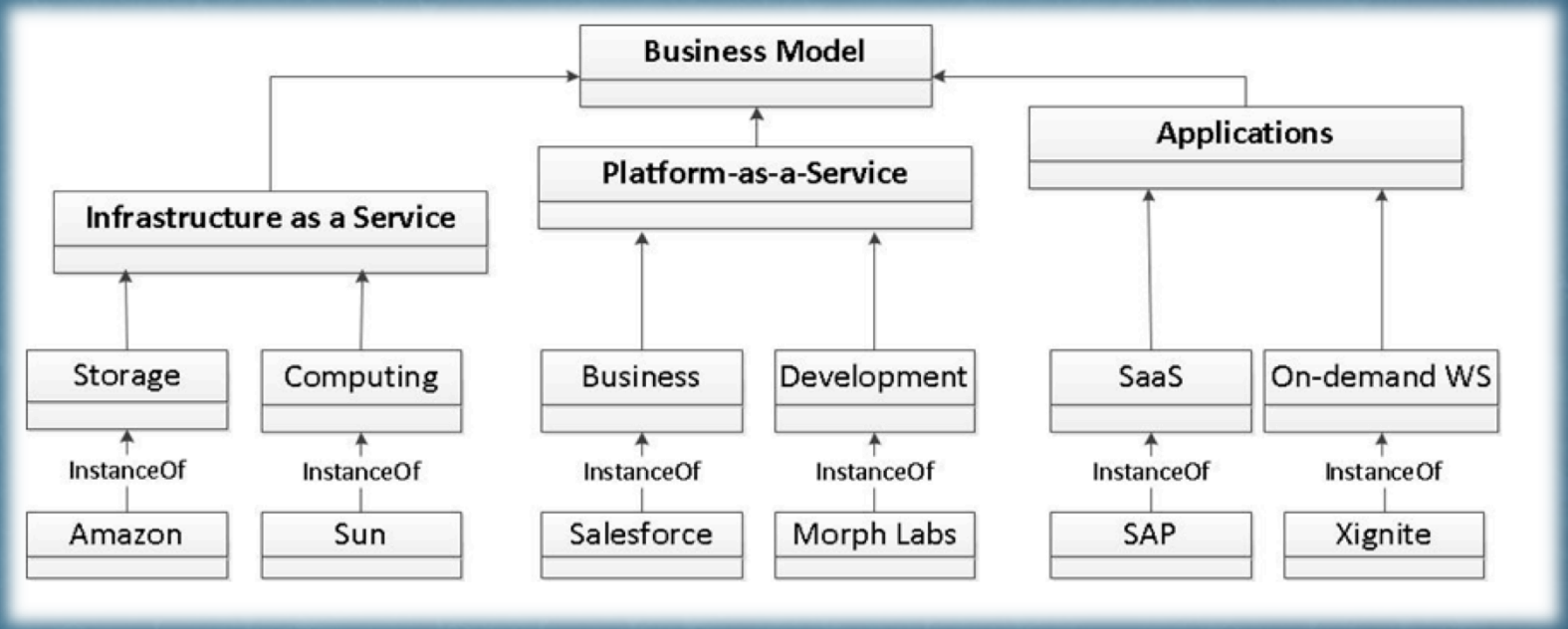
CORPORATE LOCATIONS			EXTERNAL ADMINISTRATION
User office/Desk	**Remote office**	**Data center**	**Third-party location**
Desktop Computing	Department Servers	Consolidated Servers (Private Cloud)	Public Cloud
Client Agents	Local services	Virtualized applications and services	Cloud services

Private or public, the principal goal of cloud computing is to offer an easy and scalable access to the applications in real time, at the lowest possible cost and enforcing the security paradigms.

Basically a cloud allows:

- the dynamic scale-in and scale-out of applications by the provisioning and de-provisioning of resources, e. g. by means of virtualization.
- the monitoring of resource utilization to support dynamic load-balancing and re-allocations of applications and resources.

CLOUD BUSINESS MODEL

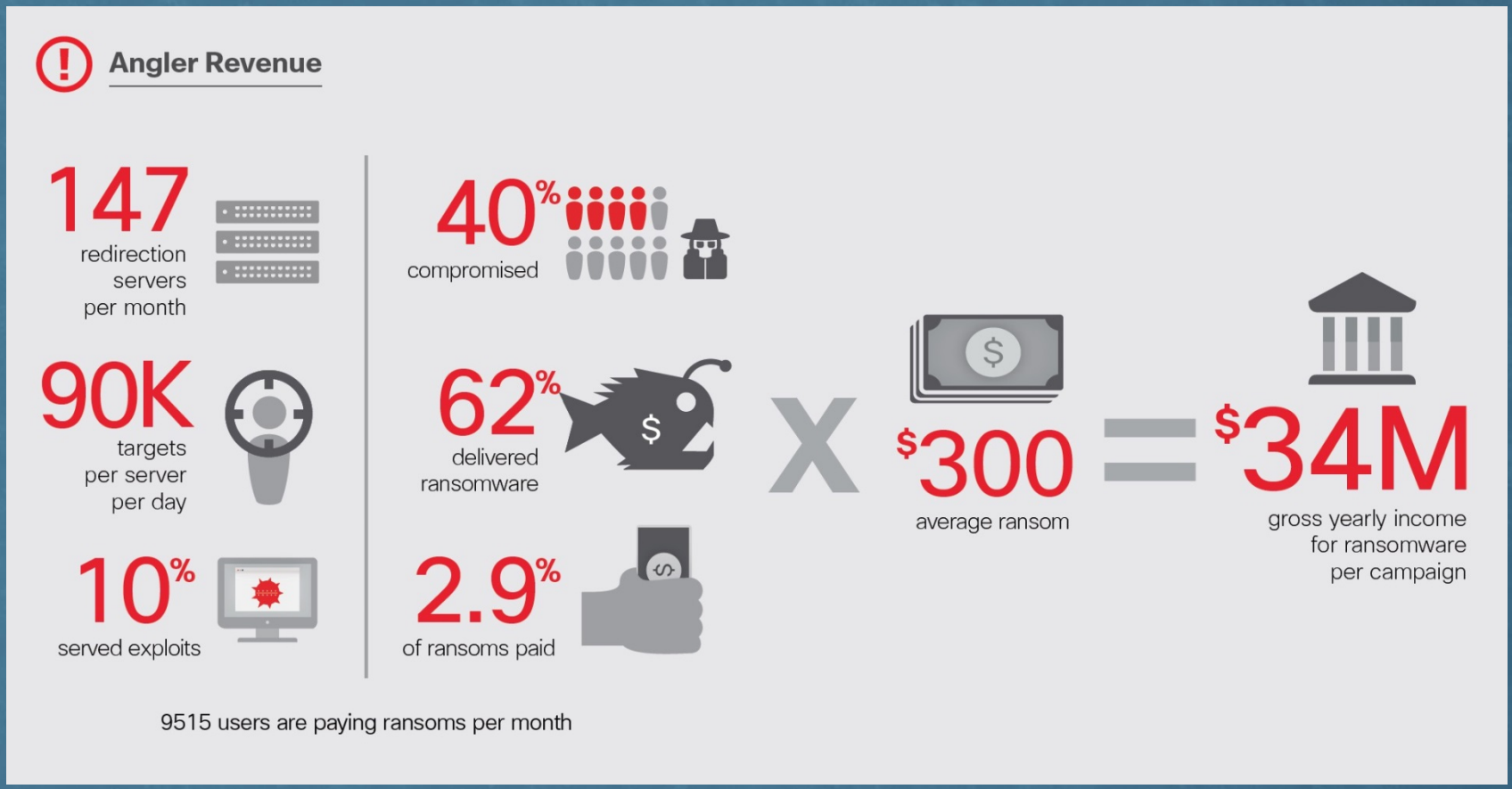


- The Cloud Business Model Framework analyzed is mainly categorized in three layers:
  - *Infrastructure as a Service (IaaS)*
  - *Platform as a Services (PaaS)*
  - *Applications commonly known as Software as a Service (SaaS)*

CLOUD APIs

- Cloud APIs are application-programming interfaces (APIs) used to build applications in the cloud computing market.
- APIs allow software to request data and computations from one or more services through a direct or indirect interface.
- The principal benefits of using Cloud APIs are the ability to leverage cloud resources into Cloud Providers.
- Several organizations provide cross-platform based Cloud APIs, the principal goal of these organizations is to bring uniformity and/or standardization to Cloud APIs.

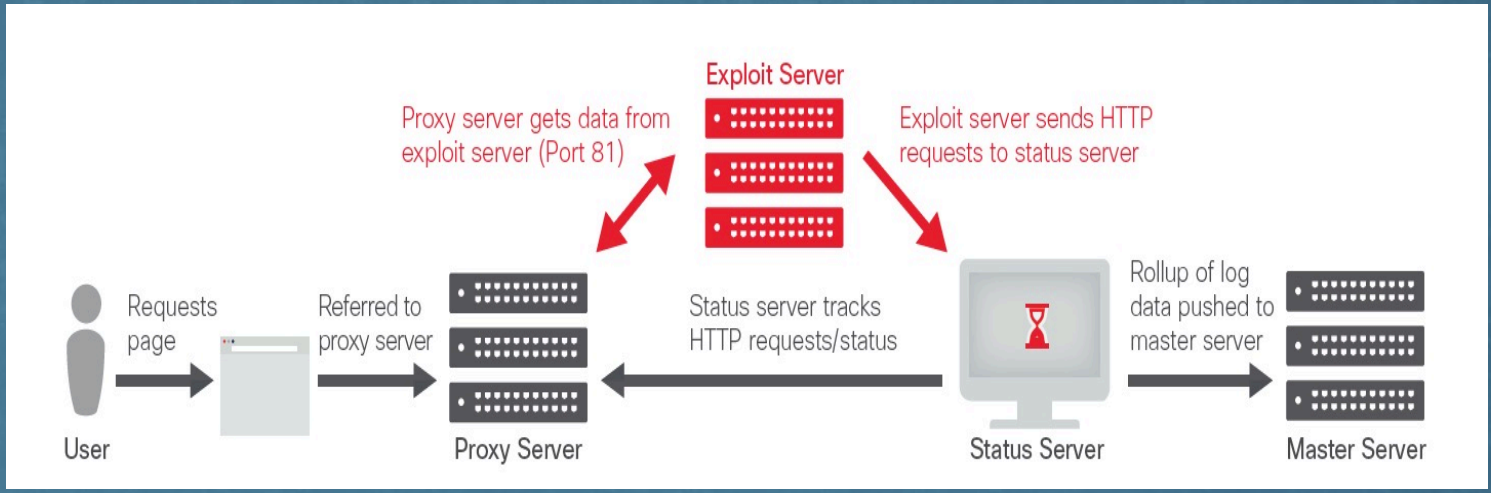
ANGLER EXPLOIT REVENUE



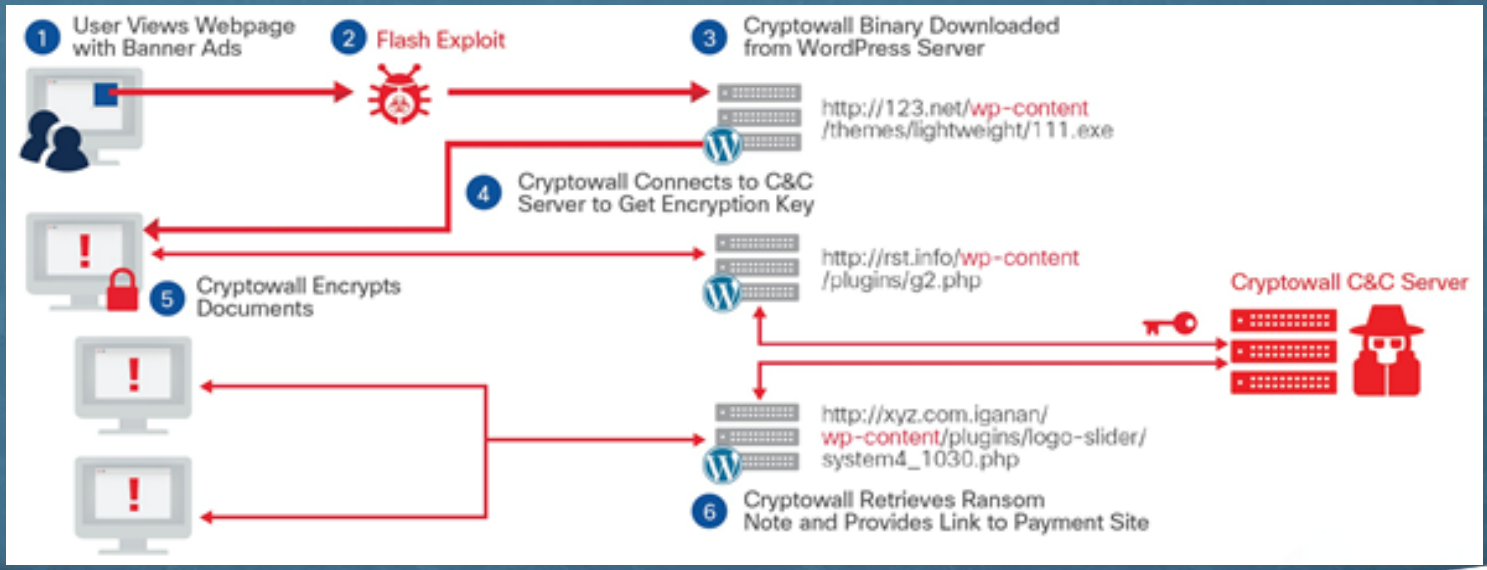
The Angler exploit proceeds to exploit security holes, commonly known as vulnerabilities, in order to infect the users with malware.

The entire process can occur completely invisibly, requiring no user action.

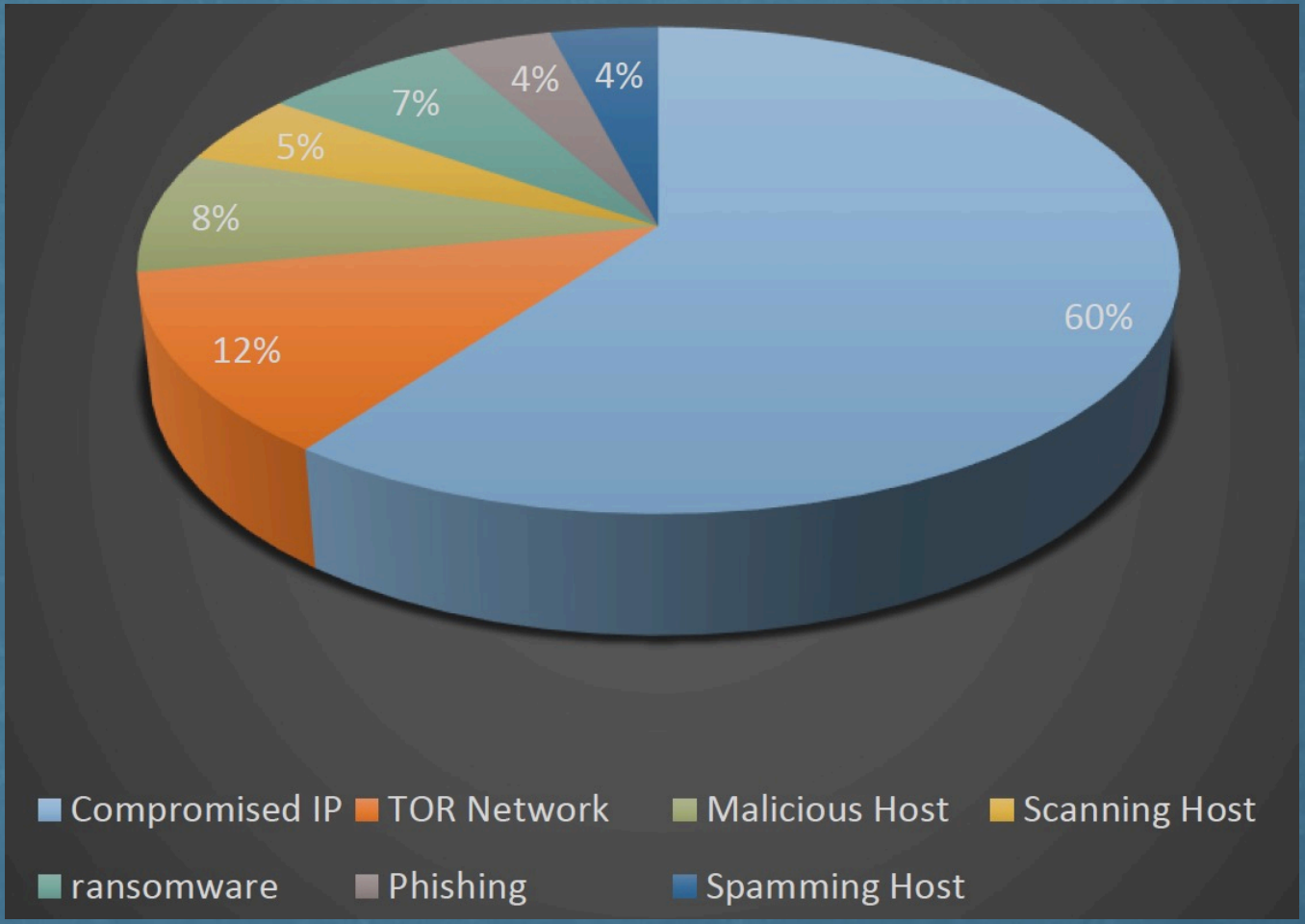
HOW THE RANSOMWARE ACTS



Wordpress site compromised by Criptowall



STATISTICS OF OUR NETWORK



Compromised IPs are currently the biggest threat, creating security breaches in the network.

SECURITY AND TRUST

- Crucial point of cloud technology into a business is the safety of critical data, both in transfer and as in storage.
- The idea of perimeter-centric network security strategy, in the age of Cloud Computing, is obsolete because every day exists a major number of mobile devices that are connecting to our network resources from places out of the perimeter.
- The continuous demand of information located in a private or public cloud has changed the vision of perimeter security.

✓ **Cloud Security Architecture is effective only if the correct defensive implementation is divided into smaller, and more protected zones. This process is known as micro segmentation of security.**

ZERO TRUST MODEL

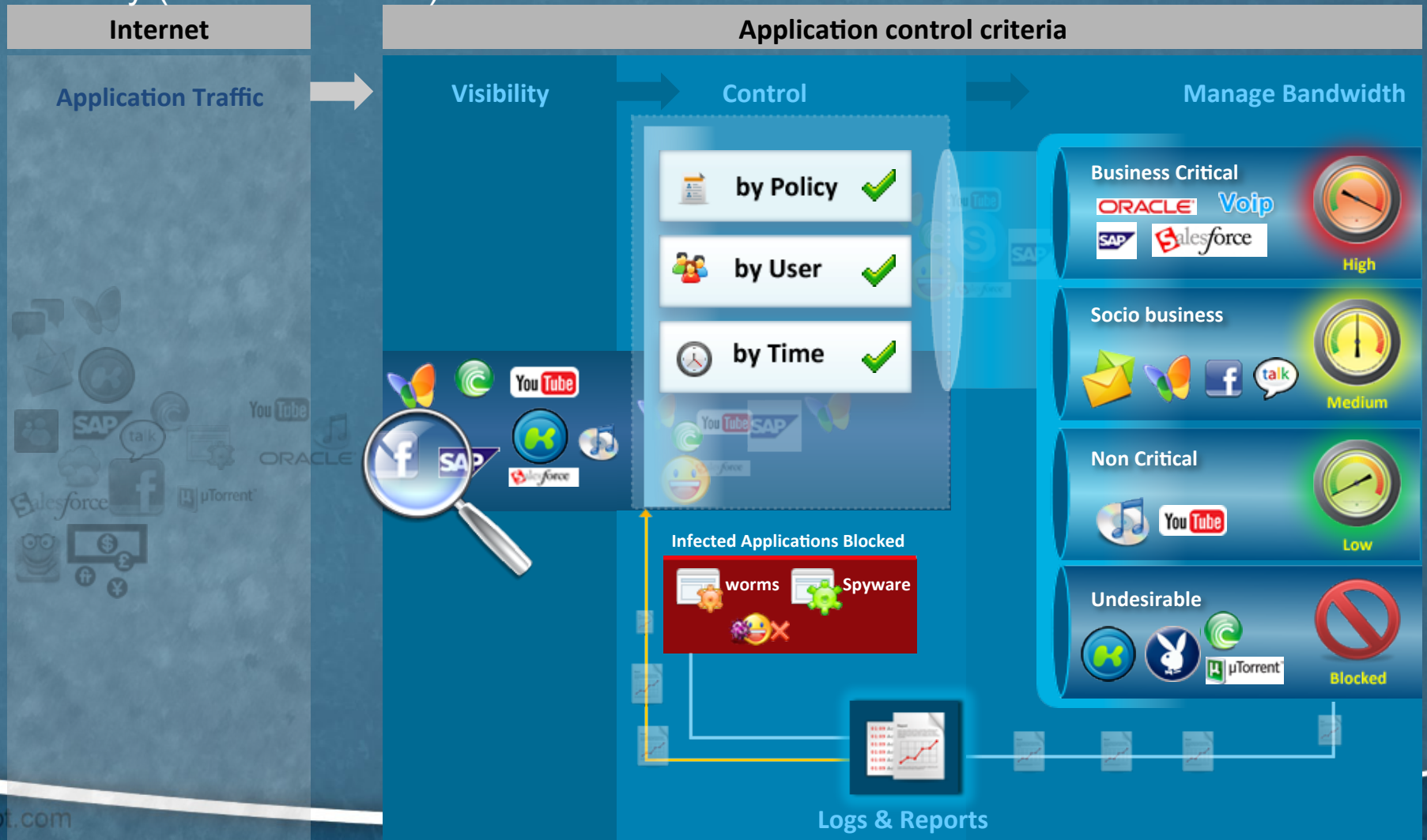
The theory is that even if one small zone is compromised, the breach will be contained to a smaller fault domain, and finally will compromise critical enterprise data. However, the correct distribution of defensive devices must be correlated with the right recognition of security issues that will arise with security management.

The *major benefits of segmentation is the viability to apply the Zero Trust Framework into Cloud Computing Technologies* that introduce the following characteristics :

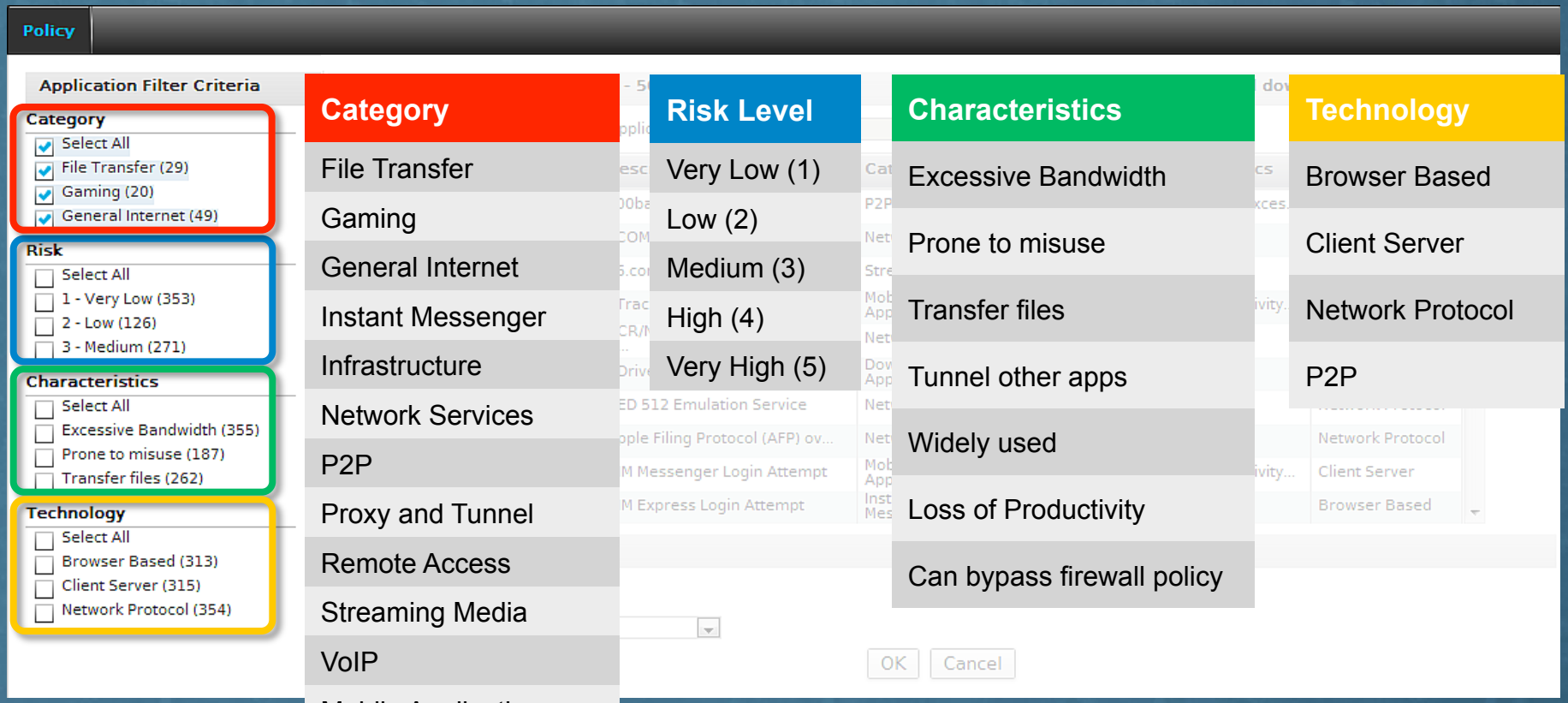
- Zero Trust is applicable across all industries and organizations.
- Zero Trust is not dependent on a specific technology or vendor.
- Zero trust is scalable.
- There is no chance of violating Civil Liberties

REQUIREMENTS FOR A NETWORK FORENSIC SOLUTION

Network forensic solutions must provide three essential capabilities: capturing and recording data, discovering and analyzing data; obtaining network analyzes and visibility (Zero Trust NAV).



CRITERIA TO IDENTIFY AN APPLICATION AND ITS IMPACT ON THE NETWORK



Category
File Transfer
Gaming
General Internet
Instant Messenger
Infrastructure
Network Services
P2P
Proxy and Tunnel
Remote Access
Streaming Media
VoIP
Mobile Applications
Social Networking
Web Mail
And more…

Risk Level
Very Low (1)
Low (2)
Medium (3)
High (4)
Very High (5)

Characteristics
Excessive Bandwidth
Prone to misuse
Transfer files
Tunnel other apps
Widely used
Loss of Productivity
Can bypass firewall policy

Technology
Browser Based
Client Server
Network Protocol
P2P

CLOUD SECURITY OPTIMIZATION TECHINIQUES

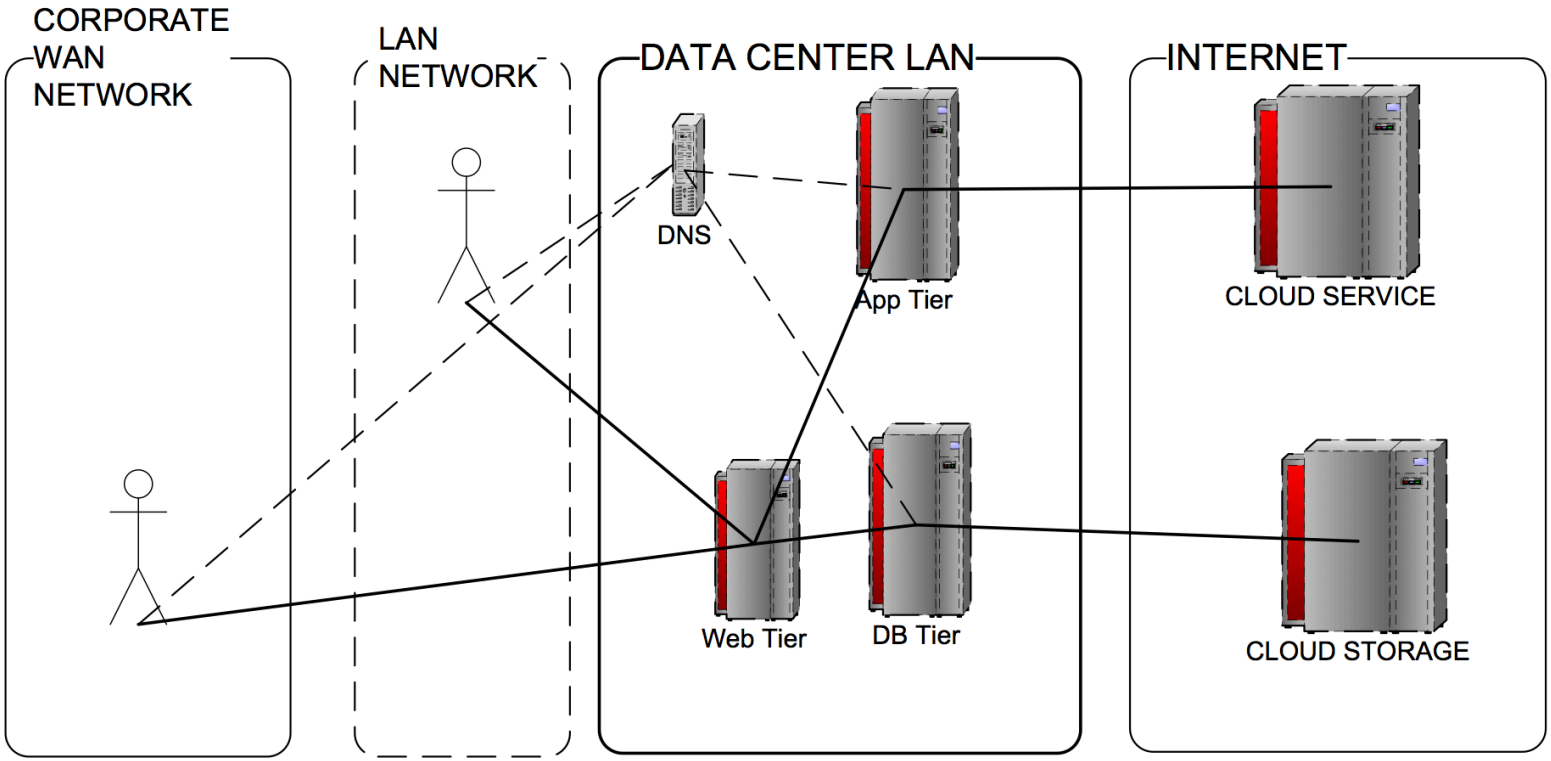
The principal goal of our study is to analyze efficient methods that maximize the network flow; identifying threats in network traffic, increasing average network security and optimizing the throughput assigned to *Cloud Services.*

$$\max_{flow} Benefit = \min_{networkThreats} f(givenNetwork, userRisk, matrixFlow, networkThreats)$$

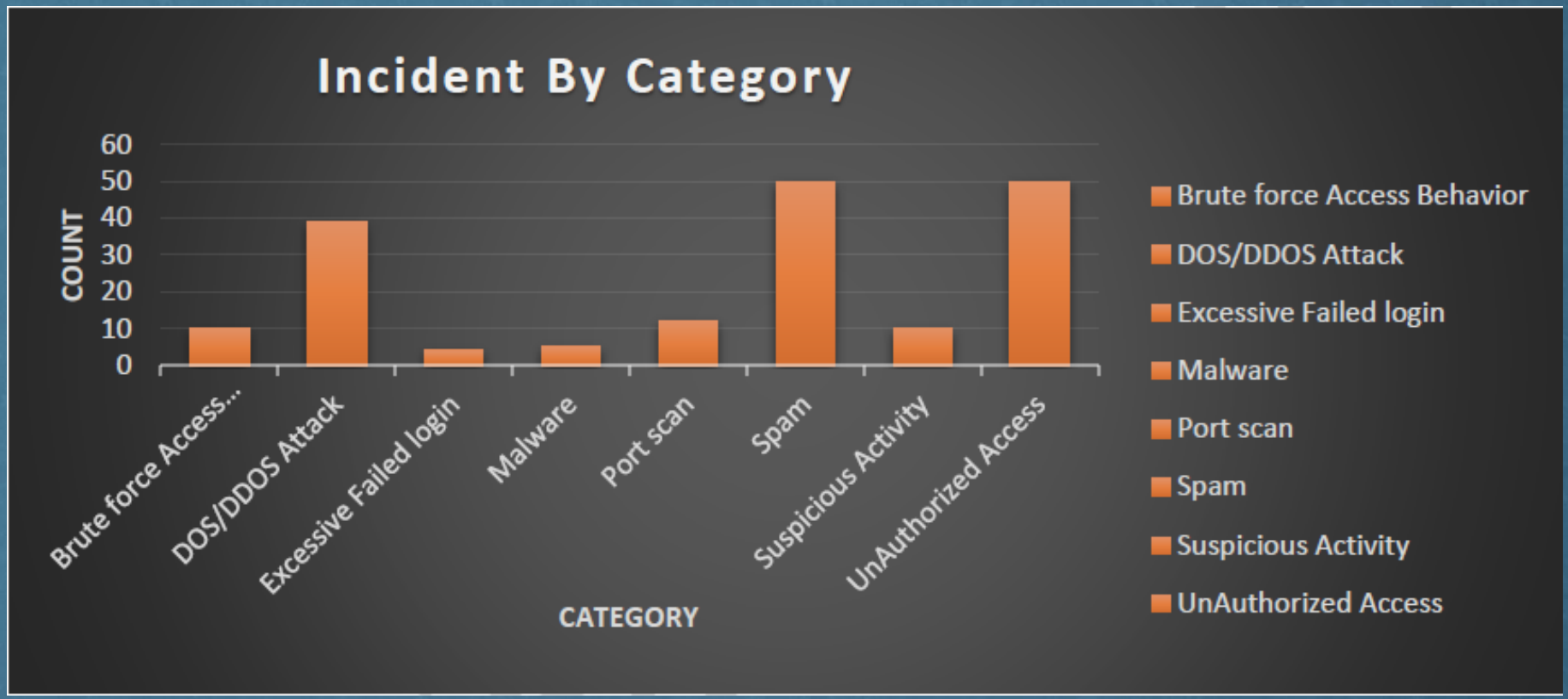
METHODOLOGY

- Design map dependencies among the elements involved in delivering services, which reduces downtime and increase productivity.
- Better utilization of network resources, supported by adequate measures of traffic with respective reporting and planning
- Classify traffic along each service delivery path; contributes for a faster characterization, network analysis and visibility; consequently is possible the remediation of security attacks.

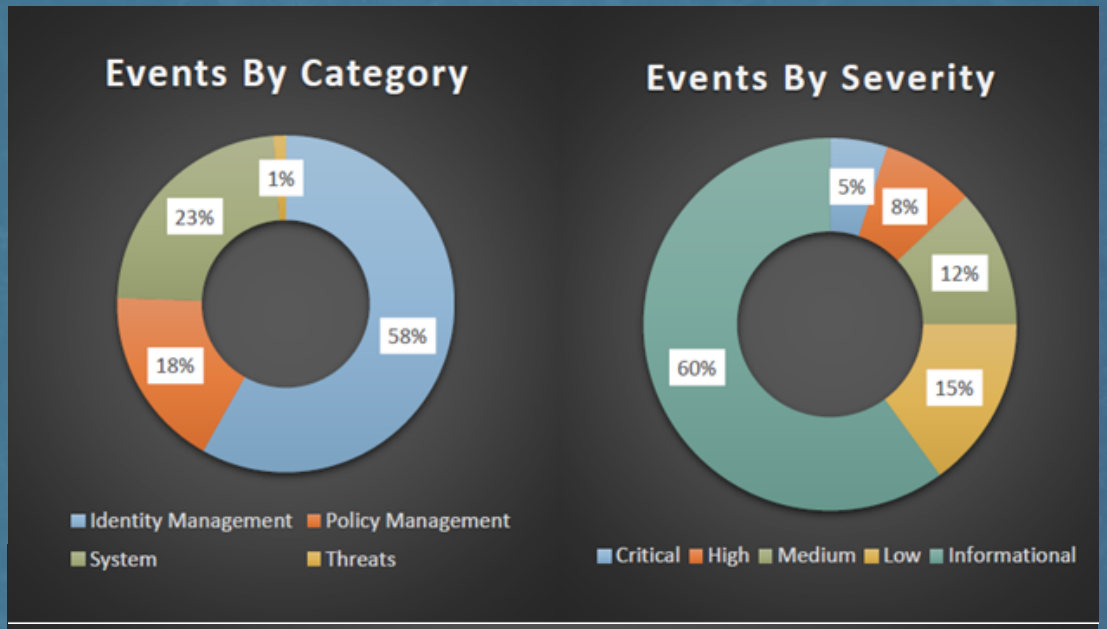
CLOUD SERVICE FLOW MAPPING

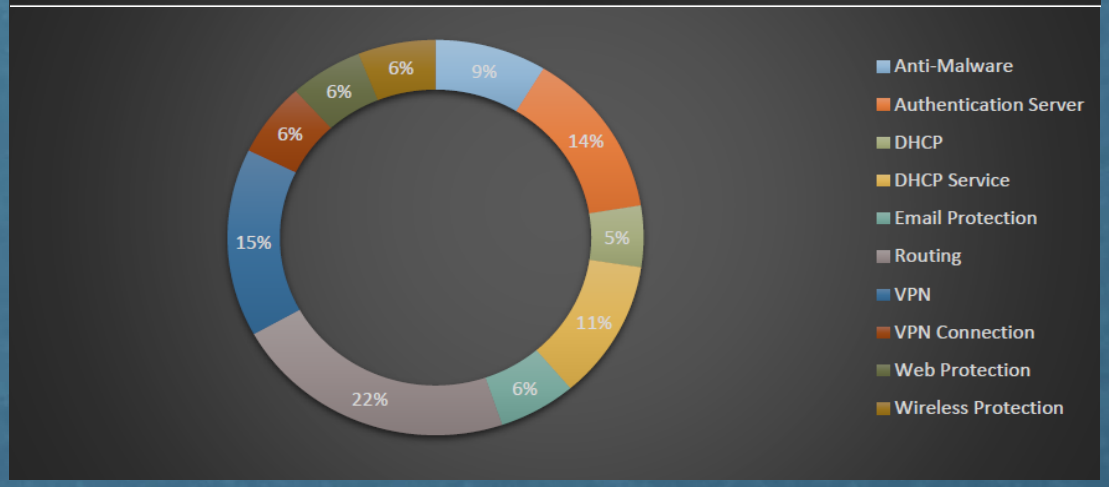


CLASSIFICATION OF INCIDENTS BY CATEGORY



EVENTS

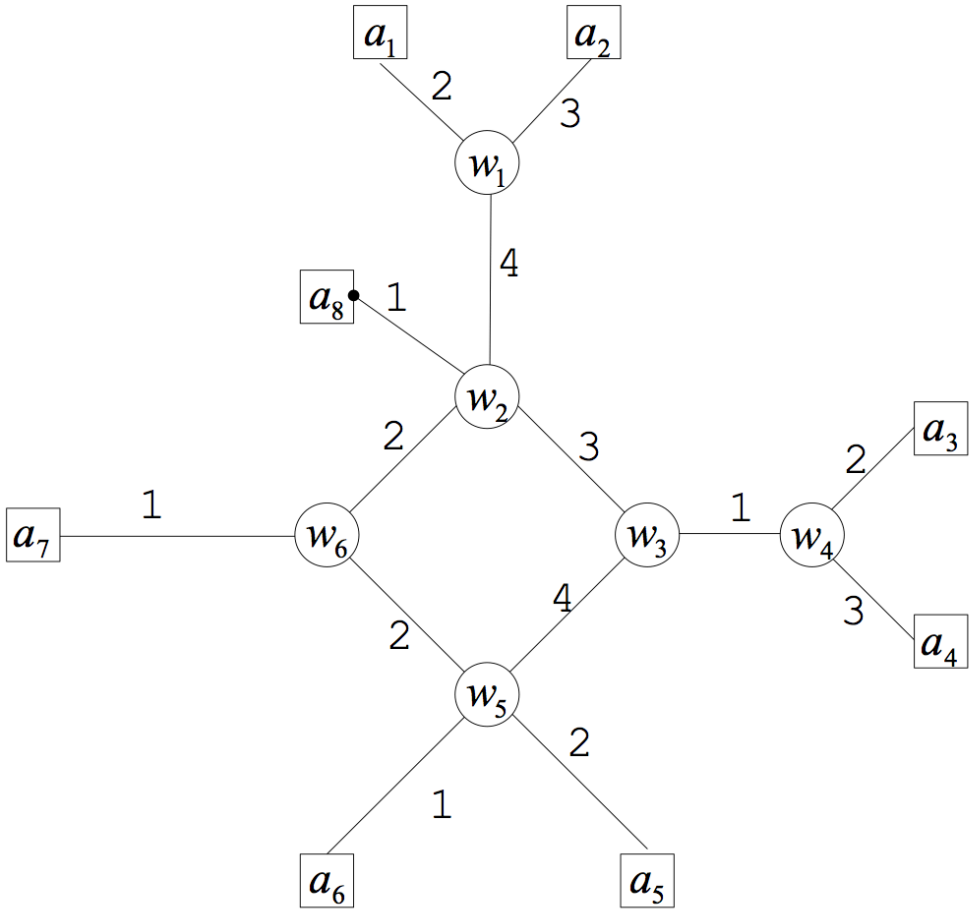




HYPOTHESIS

There exist an algorithm for network segmentation and optimal allocation of *k* security defense elements, to protect cloud services. It increases network security by reducing the time necessary for threat characterization and at the same time warranty the throughput of links required for cloud services; because a deep packet inspection allows to classify traffic in good, malicious and discardable.

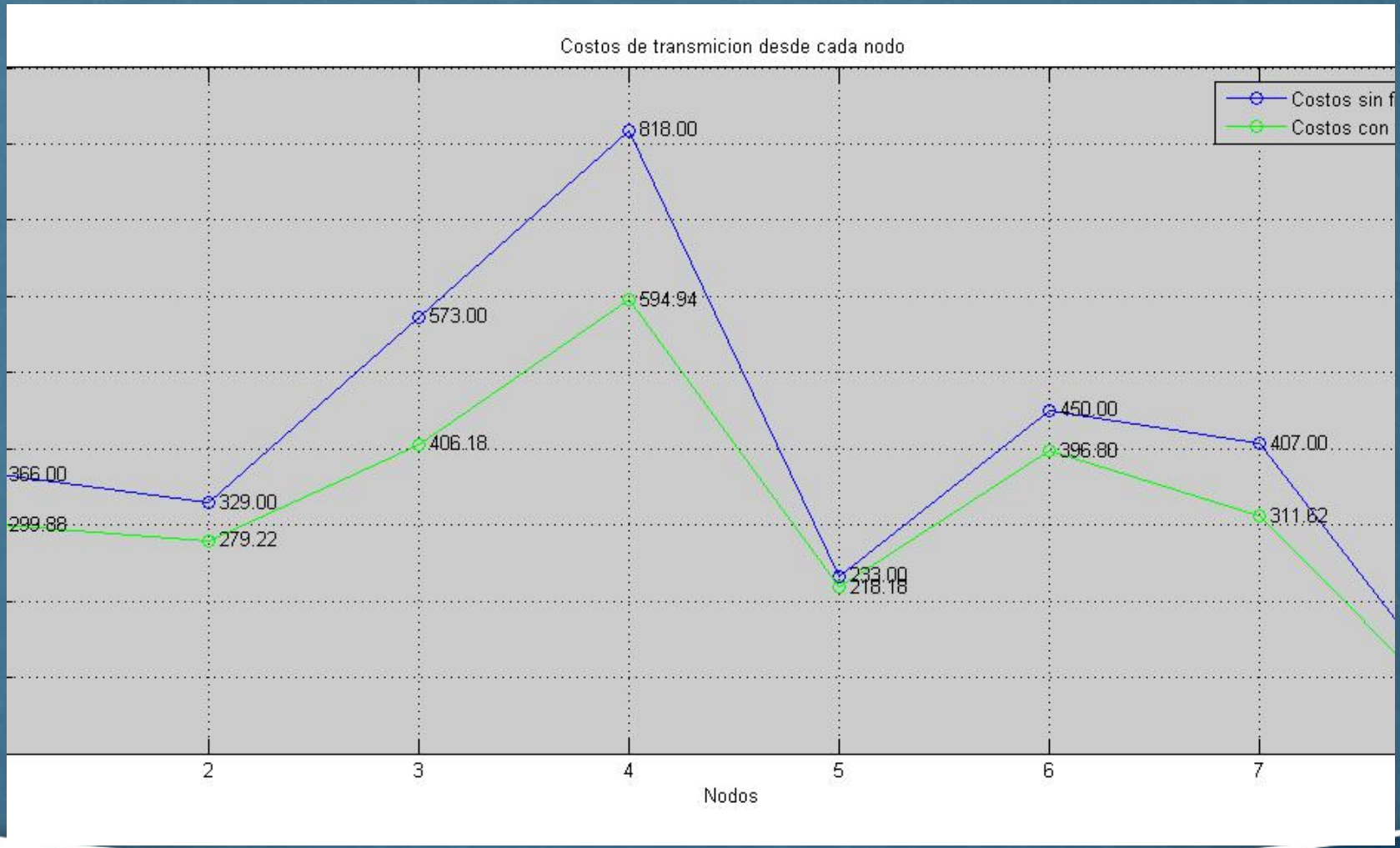
GRAPH REPRESENTATION OF APPLICATION FLOW MAPPING



Where:

- *a_1 - represent the users of corporate LAN*
- *a_2 - represent the users of corporate WAN*
- *a_3 - cloud service*
- *a_4 - cloud storage*
- *a_5 - DB Tier*
- *a_6 - App Tier*
- *a_7 - Web Tier*
- *a_8 – DNS*

SIMULATION OF TRANSMISSION COST IN NODES FOR DATA, WITH SECURITY AND REPORT ELEMENTS INSTALLED IN NODES $\{W_2, W_4\}$ AND WITHOUT DEFENSES



CONCLUSION

- Today, Cloud Service Framework model demands network analysis and visibility of all the traffic, in terms of classification of applications, services and users.

- The respect to user information data, must be seriously warranty in SLA (service legal agreement) because the actual Model of Cloud Computing allows companies to storage information, sensible data and intellectual property in different geographical locations, that may not respect the main Civil Liberties.

- Nowadays, the cloud service security goes further than the corporate network perimeter , it is necessary to develop a new generation of technologies that allows us to protect the data that flows between users and cloud services throw encrypted media.

KÖSZÖNÖM
(THANK YOU)