# Eyecon Infrastructure and Services Overview

# PREFACE

## PURPOSE

The purpose of this document is to provide a high-level IT infrastructure overview for Eyecon solutions.

This design document describes a set of requirements such as availability, security, scalability and performance, along with the monitoring, manageability and cost of ownership of Eyecon solutions.

All the architectural rules in this document are mandatory. All changes to the rules must be executed through a specific project that will validate the changes against business requirements.

The document itself is not intended to be a deployment or configuration guideline.

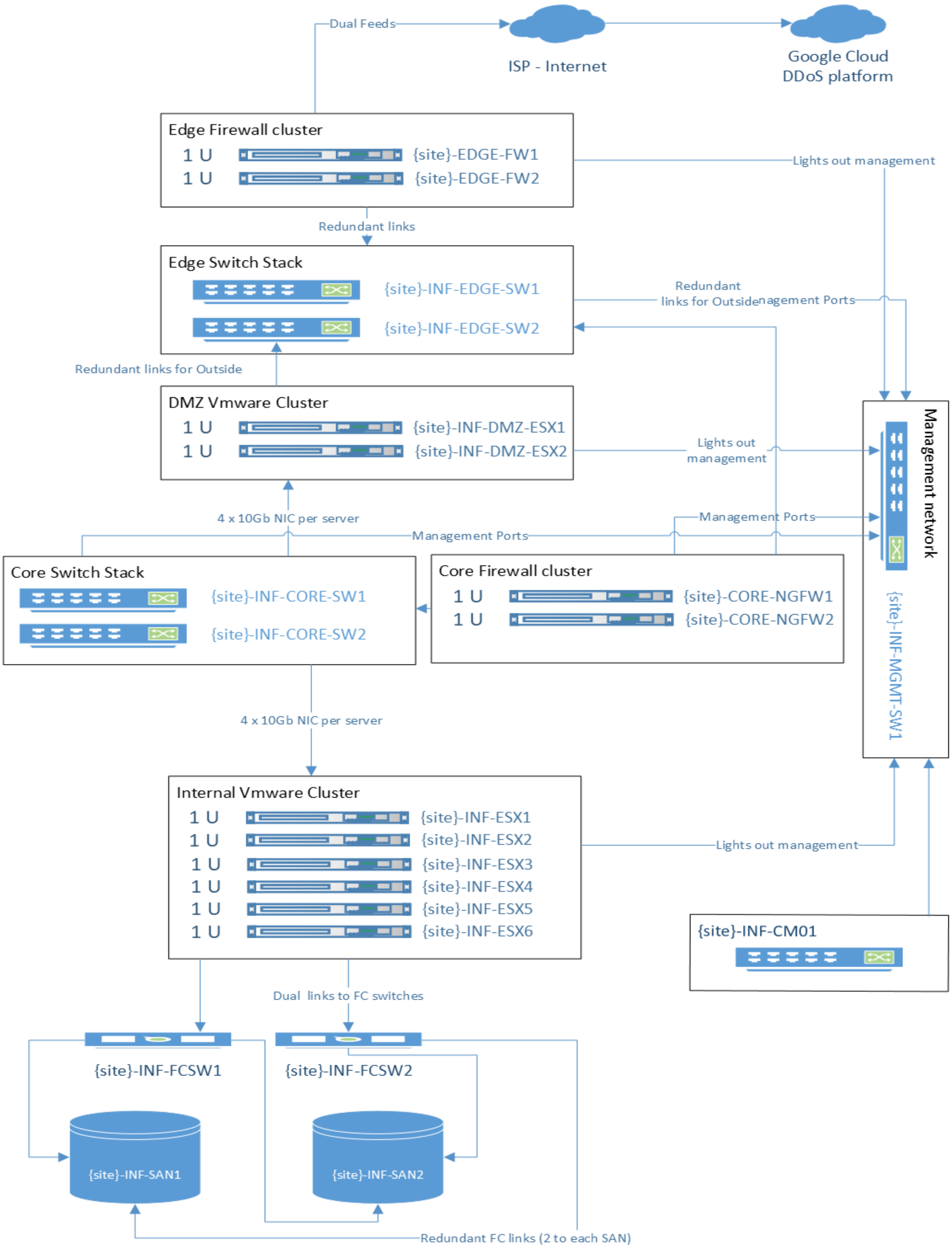
## DESIGN

Below presents the illustrations of design, both physical and logical, for a generic Eyecon solution.

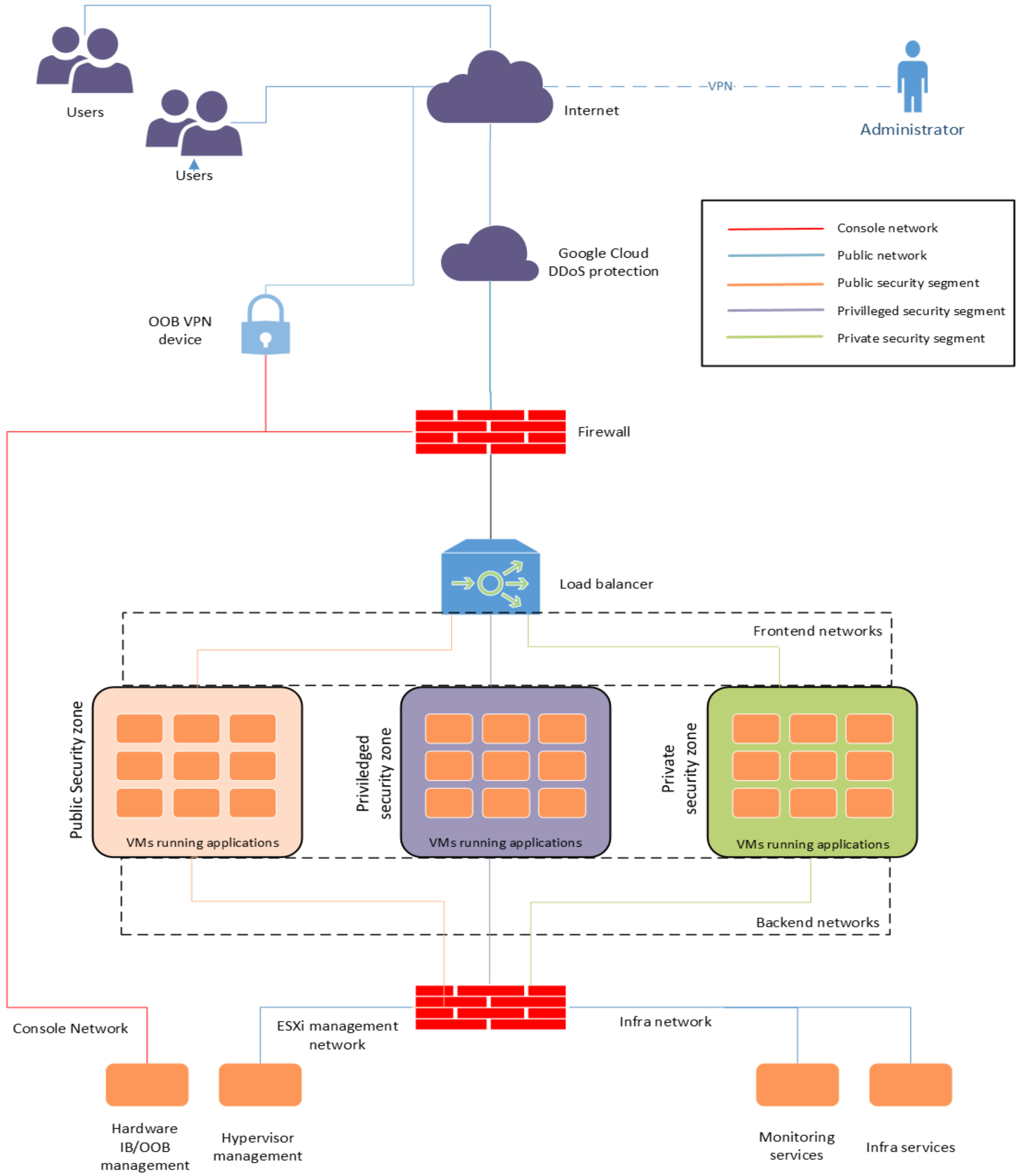
An actual implementation will have its design augmented to accommodate the specific Eyecon products deployed, and the actual number of physical and logical components needed. However, all the main design principles will remain the same.

Architectural goals and concepts are described in the following sections.

The diagram below illustrates the generic physical site layout.


Dual Feeds
ISP - Internet
Google Cloud
DDoS platform
Edge Firewall cluster
1 U
{site}-EDGE-FW1
1 U
{site}-EDGE-FW2
Lights out management
Redundant links
Edge Switch Stack
{site}-INF-EDGE-SW1
{site}-INF-EDGE-SW2
Redundant
links for Outside
nagement Ports
Redundant links for Outside
DMZ Vmware Cluster
1 U
{site}-INF-DMZ-ESX1
1 U
{site}-INF-DMZ-ESX2
Lights out
management
Management network
4 x 10Gb NIC per server
Management Ports
Management Ports
Core Switch Stack
{site}-INF-CORE-SW1
{site}-INF-CORE-SW2
Core Firewall cluster
1 U
{site}-CORE-NGFW1
1 U
{site}-CORE-NGFW2
{site}-INF-MGMT-SW1
4 x 10Gb NIC per server
Internal Vmware Cluster
1 U
{site}-INF-ESX1
1 U
{site}-INF-ESX2
1 U
{site}-INF-ESX3
1 U
{site}-INF-ESX4
1 U
{site}-INF-ESX5
1 U
{site}-INF-ESX6
Lights out management
{site}-INF-CM01
Dual links to FC switches
{site}-INF-FCSW1
{site}-INF-FCSW2
{site}-INF-SAN1
{site}-INF-SAN2
Redundant FC links (2 to each SAN)

The logical site layout is illustrated by the following diagram



Note: Load Balancers do not allow routing between different front-end networks, they force that traffic to Firewalls. Public, privileged and private security zones are described in later sections

## CONNECTING TO PRODUCTION SYSTEMS

Access rights to Eyecon systems are controlled via our strict security groups within directory services. Access is granted on the principle of least privilege.

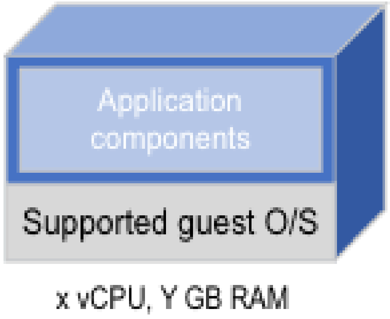
Administrative access to production systems for managing the infrastructure platform is only possible via site-to-site VPN to Eyecon's office. SSH and similar administrative access from Eyecon's internal networks into production networks and systems is only allowed from Production Gateway VMs (Virtual Machines).

Not all Eyecon employees can access Production Gateways, it is limited only to members of the operations team and enforced by network restrictions and security groups.

## VIRTUALIZATION

The infrastructure platform is designed as a fully virtualized architecture. Each software component is contained within its own Virtual Machine. These containers are orchestrated by a central system that allows for granular resource assignment and orchestration.

- From the infrastructure perspective, a virtual machine container is the smallest logical component deployed.
- It consists of the operating system, third-party components, and Eyecon application components. Each Eyecon product has specific rules concerning the components that can be combined into one virtual machine. This is done to meet requirements for the sizing and security of virtual machines.
- Virtual machines are only connected to networks required by the services deployed on them.
- Supported Guest Operating Systems (OS) are listed in Appendix A



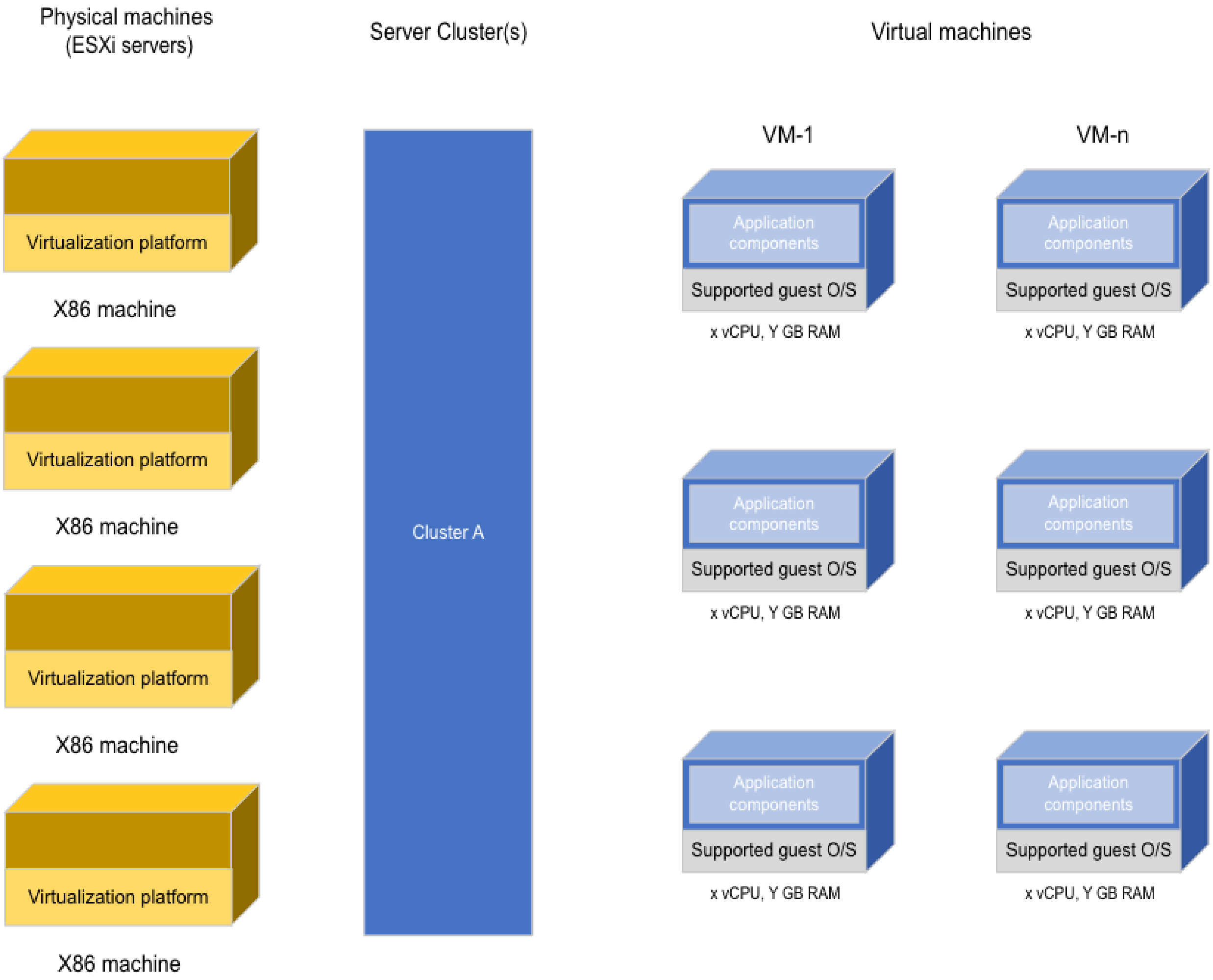
### VIRTUALIZED APPLICATION INFRASTRUCTURE AT PRODUCTION SITES

The diagram below illustrates the deployment model for the virtualized application infrastructure.

Physical servers are combined into a single cluster (resource pool) running VMWare ESXi. Virtual Machine instances are deployed on top of it, created from standard approved image. Playtech applications are deployed on top of the VMs by respective product's devops engineers.

VM containers are continuously load-balanced between all physical machines in a cluster.

The supported models of physical servers are listed in Appendix A.



## FAULT TOLERANCE

Hardware will occasionally fail. This is a fact, and an assumption that must always be considered in software development. The infrastructure architecture must provide the means to minimize the impact and recovery time for a failure of any infrastructure component. In most cases, the solution uses component redundancy with failover mechanisms. At least n+1 instances of each component are deployed, even when not required according to existing load. The health of all Eyecon's hardware devices is being monitored via our central monitoring platform (covered in more detail later)

## MANAGEABILITY

Eyecon uses as few vendors as possible. The number of different building blocks is kept at an absolute minimum. Limiting the number of vendors and used hardware models allows Eyecon to implement centralized management tools, keep the technical knowledge focused, and keep the maintenance overhead at an optimal level.

## SUPPORT

Eyecon collaborates with world-class managed, secure and certified datacenters. Deployed hardware solutions have support in the locations where Eyecon operates. It is crucial to have vendor service available once something malfunctions. This ensures the malfunction will be fixed in a proper time frame with minimum impact to the system. The current requirement for existing and new hardware solutions is 5 years of support with a minimum NBD (Next-Business-Day) reaction time.

## DATA STORAGE INFRASTRUCTURE

Eyecon uses high-availability storage infrastructure configurations that are compiled according to the vendor's best practices and recommendations to achieve the required SLA (Service-level agreement) for Eyecon solutions. All critical storage infrastructure components are fully redundant, either via multiple physical nodes or internal redundancy within a node (such as with drive arrays).

All storage infrastructure components have central administration, monitoring, and performance analysis tools. All deployed components conform to Eyecon's centralized management practices and procedures.

## DATABASE INFRASTRUCTURE

Percona MySQL RDBMS is used as the database engine for all mission-critical deployments, running on a virtualized x86 platform.

Databases are deployed in a Hot-Cold type of cluster – multiple nodes of which the database is running on only one at a time. The database servers can be deployed in an optimal configuration and scaled vertically with minimal impact on the services.

Data partitioning is used to maintain the efficiency of data storage usage and data lifecycle management.

Eyecon Databases are covered by central Database Activity Monitoring, which is part of our standard security strategy for databases and data protection.

## APPLICATION SERVER INFRASTRUCTURE VIRTUALIZATION

Eyecon uses a VMware stack on enterprise-grade x86 machines to provide a virtualized platform for all application servers and supporting functions (such as infrastructure services and monitoring). Virtual Machine containers, middleware, and Eyecon's own application components are deployed and managed using a centralized management system.

The virtualization platform used provides support for the high availability and manageability requirements – controlled failover in case of physical host failure, moving working VM containers between physical hosts. All physical servers are directly connected to the central storage device, to meet high availability, recovery and management efficiency requirements.

All production sites use the same licensing and physical application server model wherever possible. Physical servers are maintained as clusters (common resource pools) under VMware ESXi. It is possible to have several clusters within the same site, but as a matter of best practice, the number of clusters is kept to a minimum. The minimal cluster size is three physical hosts.

All servers are managed via a centralized management system, hosted at Eyecon's on-premises datacenter. The management system is set up in a high-availability cluster.

## NETWORKING LAYER

Google cloud DDoS proxy and protection is deployed in front of all production sites for preventing and mitigating DDoS attacks.

An Nginx H/A proxy / load-balancer is deployed in a dual cluster. This improves the efficiency of infrastructure usage through load balancing. It also ensures the transparency of component maintenance or failures. In addition, the load balancers are used for SSL (Secure Sockets Layer) offload, with SSL private keys stored in a secure encrypted manner within the devices.

For each site we have 2 internet links for redundancy. Two routers with active-passive setup have one cable from both internet links.

To follow the industry's best practices, Eyecon solutions have the following layers:

- Network security layer – firewall clusters, where access to all other layers and components is controlled. Each layer makes up a separate network segment.
- Public application components layer – application components that require access from the public internet to enable gaming activities.

- Privileged application components layer – application components that can only be accessed by components in the public security zone, specific IP addresses and/or via VPN. For example, the backend UI used by the licensee staff.
- Private application components layer – application components that are not directly accessed by any publicly available components, usually connecting to application components from other layers.
- Data layer – databases are separated into a separate network. Like all other layers, access to application components is controlled on the IP address/service port level through firewalls.
- Management layer – a management network that can be accessed only through VPN for infrastructure administration purposes.
- Data storage layer – the Eyecon solution uses storage devices connected via fiber-optics. Storage area network is physically separate from data network.
- Eyecon collaborates with best-of-breed vendors and solution providers to offer DDoS mitigation solutions. However, these solutions are dependent on the location of the services being offered, no generalizations have been made.

## MONITORING PLATFORM

Eyecon is monitoring its platform and services via centrally implemented monitoring tools. Our holistic monitoring solution covers the following layers:

- Infrastructure layer (servers, network devices, etc.).
- Virtualization layer (Virtual Machines).
- Application layer (Eyecon application services).
- Business metrics behavior (pattern analysis to detect abnormal behavior).

Our monitoring platform uses five main approaches which are chosen based on technical needs and business requirements for the services to be monitored:

- Agent based monitoring – every server hardware and virtual machine has a standalone monitoring agent that keeps track of all necessary metrics.
- Remote monitoring – all critical services and applications are regularly checked remotely for their health statuses. The same approach is used to verify service quality metrics (response times, memory usage, etc.).
- Real time trend and pattern-based business metrics analysis (spins per minute, launches per minute, etc.).
- Time-series based health metrics from applications and operating systems are collected and monitored in real time to detect signs of problems before they materialize.

All alerts are gathered into the central management system where these are correlated and forwarded either to Eyecon operations support, different dev support teams or go directly to jira service desk tickets based on the alert criticality level.

## APPENDIX A - LISTING OF THE STANDARD COMPONENTS

Efficiency requires automation, and automation requires standardization. Eyecon’s Infrastructure Operations department uses only a specific set of infrastructure components. All new components are tested before being used in production. The component’s suitability to the overall solution is verified.

The standard, approved and supported components for new setups are:

### A.1 - HARDWARE

- Storage – Fujitsu AF series, Brocade fiber-optic switches
- Network switches and routers – Brocade ICX series, Cisco catalyst devices
- x86 application servers and firewalls – Fujitsu RX series, Dell R-series
- Database servers – Fujitsu RX series, Dell R-series
- OpenGear - remote management device

### A.2 - SOFTWARE

- CentOS Linux operating system
- Oracle Enterprise Linux
- VMware vSphere vCenter
- Cisco Nextgen firewall platform
- Third-party components – Nginx, HA Proxy, Java, Tomcat, Kafka
- Monitoring components - Nagios, InfluxDB, GrayLog, Grafana, Python

| Document Revision History | | | |
|---|---|---|---|
| Date | Revision | Author | Description of Change |
| 19.02.2024 | 1 | GF | Collated existing content to single document |
| 21.02.2024 | 2 | PC | Review and minor amendments |