Security Whitepaper

September 2017

V1.0

Introduction

Business applications delivered from the cloud should be compelling for all companies–no matter their size or geographic spread. The cloud offers on-demand services, 24x7 support, a pay-as-you-go/ pay-as-you-use pricing model, and will effortlessly scale to meet spikes in demand. So while service availability, high-performance, and security are key considerations, the real benefit of the cloud is a financial one. Placing infrastructure, the system core, in the cloud at geographically dispersed Points of Presence (PoPs) provides access to its rich functionality over the Internet. For end users this means that there is little or no capital investment in on-premise infrastructure. Costs are reduced further with no management burden placed upon internal IT resources.

However, when considering cloud services for business critical media files and video streams the security, performance and reliability must be assessed.

In this paper, we look at some of common security principles and the areas of risk that exist today. We explain some of the controls Yella Umbrella use to manage these risks, to ensure an open and secure environment for all media and business critical data

Overview

Yella Umbrella's Nebula is a platform and toolset for manipulating media files and streams in the cloud, on premise or hybrid. Nebula platform management and control is always cloud based while the tools and the media can be located anywhere the customer chooses.

Nebula automatically delivers tools to run and process media at the chosen location, this will inevitably create security concerns. Before the cloud, a business would purchase and run software or hardware systems at their own site to process media also stored on site. Users could validate new software and any software updates but there was still a strong trust element between the client and software vendor.

With cloud services and automatic software delivery both that trust and the security of that infrastructure become even more important.

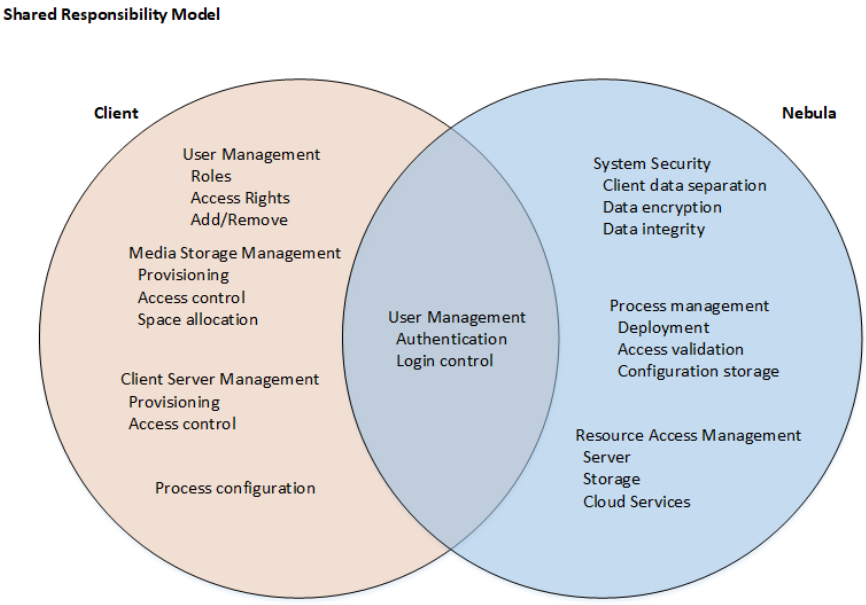
Security Highlights

Nebula has been build using a Secure by Design approach using the OWASP security implementation guidelines as a controlling principal. Our software and platform are audited against OWASP ASVS 3.0.1[1].

Secure by Design means that security considerations have been at the heart of the design and implementation phase resulting in a strong and secure platform that users can trust.

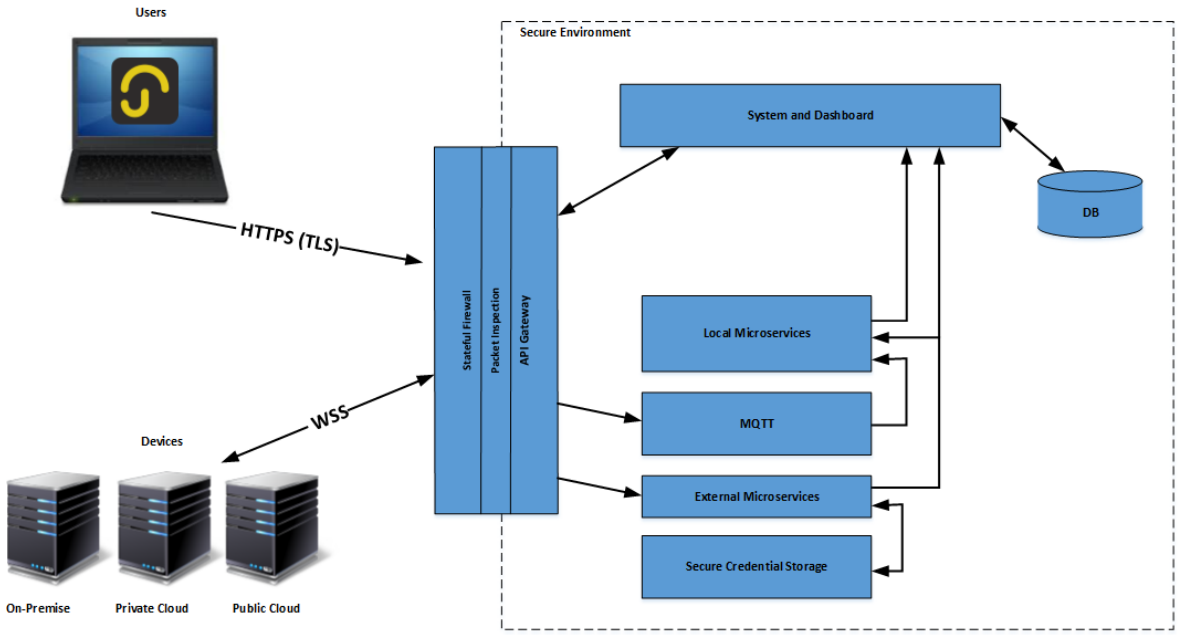
[1] https://www.owasp.org/images/6/67/OWASPApplicationSecurityVerificationStandard3.0.pdf

Yella Umbrella's Nebula system operates on a Shared Responsibility model, similar to that of large cloud providers. Yella Umbrella provide a secure platform with systems and methods that protect data stored in and on the platform and access methods to the system. The client is responsible for using the system to authorize users and allowing access to both data on premises and their in their external cloud storage.



Secure Infrastructure

Nebula provides a secure platform with a strong focus on Security Risk Management (SRM) and ongoing security monitoring supported by regular penetration testing, sandboxing for system component separation and the use of industry standard secure communication protocols.



System Security

The Nebula system utilises JWT secure token exchange extensively.

- Single use JWT tokens, with limited lifetimes, allow extremely secure control of all systems components. Combined with HTTPS Transport Level Security (TLS) communications the short lifetime JWT tokens (for critical access as short as 10 seconds) provide very high protection against interception attacks.
- All session authentication and configuration is via secure JWT tokens. All downloads are Virus checked before delivery.
- User security and authentication is supported by JWT tokens, two-factor authentication, hashed password storage, enforced password format and rollover as well as CAPTCHA login protection against brute force attacks.

All access to the Nebula server(s) is through a API Gateway with stateful firewall and packet inspection.

Use of a third party payment processor provides conformity to PCI-DSS.

Media and data Security

Client media access credentials are stored in Vault by Hasicorp and accessible only via single-use tokens.
Access to client media files can be time limited and data volume limited.
Depending on Process configuration, high value files never leave the clients own storage or control.

Cloud Security

Where possible, data centres selected by Yella Umbrella will adhere to the relevant local standards for compliance.
For example:

- Payment Card Industry Data Security Standard (PCI DSS)
- FIPS (Federal Information Processing Standard) 140-2 Encryption
- SOC3 Systrust for Service Organizations
- BS EN ISO 9001:2008
- ISO/IEC 27001:2005

Contact Us:

Sales@yellaumbrella.tv

www.yellaumbrella.tv

