Security Through eNlight

eNlight has been designed to address all security requirements and face the threats existing in today's online ecosystem to ensure smooth functioning of your operations. With eNlight cloud you can be assured that your application / website / information / database is protected against security threats. We make sure that our customers' data is kept highly confidential; to reinforce the trust and confidence our customers have in us. We adhere to rules and regulations by taking adequate security measures. We are certified and competent to ensure total security against data theft and information leakages, to diminish risks and simplify server security.

1. Secure Cloud Infrastructure

eNlight Cloud stores data on enterprise storages having multiple security layers. These security layers are further strengthened by the best practices followed to store eNlight data, including **Isolation of storage** from public network and **thick provisioning** of storage to negate sharing. eNlight is based on **hardware virtualization technology** isolating cloud servers at the **hypervisor layer** for additional data security. This explicit virtualization of the physical resources leads to a clear separation between guest and hypervisor, resulting in additional secure separation between the two. Customer instances have no access to raw disk devices, but instead are presented with virtualized disks. The eNlight Virtualization layer automatically resets the chunk of storage used by a customer, thus preventing exposure of one's data to the other.

2. Server Isolation & Security

Inside eNlight' secure environment, the isolation layer replicates cloud resources (processors, memory, storage, etc.) to match the execution requirements of the original server. Using this approach, servers and applications run on eNlight cloud **"as is"** without requiring modification or redesign, and without any disruption. eNlight's tightly integrated modules easily expand to ensure server, application, and data security across physical, virtual, and cloud servers, as well as virtual desktops. eNlight Cloud offers a comprehensive, centrally managed platform to help you simplify security operations.

3. Storage Security

Our employees are prohibited from viewing the content of the files you store in your eNlight account, and can only view file's metadata (file names and locations). Storage Servers are Isolated from the Public Network, and safely nestled into a Private Network, thus eliminating all the threats & attacks that the Internet poses. Traffic to and from eNlight Cloud stays within the corporate firewall without crossing the Internet. Our regulated routing policies also specify the users that are actually allowed to reach the Cloud resources.

4. Network Isolation

eNlight Cloud deploys Network virtualization techniques that separate different networks on the same hardware and therefore, partition resources accordingly. This ensures excellent isolation along with regulated network resource sharing within different users. Network Isolation boasts of multiple advantages,

some of which are:

- viruses and worms cannot propagate into eNlight Cloud's isolated network,
- malicious users and external applications are unable to attack eNlight servers as they lack the authentication credentials required to establish communication within eNlight's Isolated Network.

5. Network Security

Every customer is kept in a VLAN with L3 Switch in the backend. This reduces trivial network vulnerabilities and provides significant protection against traditional network security issues such as Distributed Denial of Service (DDoS) Attacks, Man in the Middle (MITM) Attacks, IP Spoofing, Port Scanning and Packet sniffing by other tenants. Security is provided on multiple levels: the operating system (OS) of the host, the virtual instance OS or guest OS and firewall. Some of the features of eNlight' Network Security are:

- Private VLANs.
- Optional hardware firewall or load-balancing.
- Anti-spoof / anti-sniff firewall technology.
- Customer isolation in public cloud.
- ARP access list used to avoid man-in-middle kind of attacks and IP thefts.
- On request dedicated Firewall Provision with SSL and IPsec VPNs.
- High end Cisco anomaly detector with sophisticated algorithms to analyze the traffic.
- High end Cisco anomaly Guard, capable of handling 1Gbit/s traffic, to protect network from DDoS attacks.
- Out of Path Traffic filtering system to block malicious traffic without affecting normal traffic.

6. Protection Against IP Spoofing & Theft

We take security very seriously; hence all systems and applications have been protected against all known and potential threats. To protect against IP Spoofing, eNlight Cloud has implemented IP-MAC-Binding policies to ensure "zero" IP thefts Thus IP addresses get bounded with the MAC address of the VM they have been provisioned on. Similar policies are implemented on routers so that if MAC gets spoofed, the router still does not forward traffic on unknown MAC address. In addition, eNlight interface does not accept addresses within the internal range as the source. eNlight ensures that proper authentication measures are in place and carried out over a secure (encrypted) channel. eNlight's host-based firewall infrastructure does not allow an instance to send traffic with a source IP other than its own.

7. Security Against Internet Threats

eNlight cloud is protected against various threats over the internet by multiple protection mechanisms, which are:

a. Default Firewall - Enabled on all servers by default.
b. An IDS connected in parallel to the router which continuously monitors traffic and blocks known threats such as application and network virus(es). It also helps detect and eliminate possible DDoS attacks.
c. 24 x 7 NOC teams keep a close watch on aberrant behaviours of network.

8. Uptime Monitoring

A team of highly experienced NOC engineers monitors every activity of Network 24x7. There is a higher and a lower limit set for all ISP. In case of any attack from a single ISP, a warning message is automatically generated for in-shift engineers. Our R&D team has also developed an in-house tool which simplifies the monitoring aspects. The concept is called GRID monitoring where every switch is representing a rack is displayed in GRID and it turns RED in case any of the servers within the RACK is malfunctioning. This way the health of entire datacenter is visible at a glance along with the longs in case of any problems. Also with the change request policy in place, all the major changes are tracked, tested and backed up before implementation.

eNlight's automated monitoring tools offer high level of performance and availability. eNlight system has been specially designed to monitor key operational metrics including notifications to alert management. Alarms are configured to notify operations and management staff when thresholds are crossed on key operational metrics. Documentation is maintained to aid effective handling of incidents, as well as for future reference.

eNlight Cloud monitors the servers continuously and provides resources within a very short span from load detection timestamp. These changes are logged in real time and are provided to the clients with a maximum of 90 seconds cycles. The usage and amount utilized can be monitored on hourly, daily, monthly and yearly basis.

9. Secure VM Management

Identity of every client is verified by our billing staff and his / her email address is kept as the primary access parameter for cloud account. Client gets access to all geographically configured clouds using the same access credentials. Different Access Control Lists are maintained for staff members involved in providing eNlight support and services.

10. Security Against Privileged Users

All privileged users involved in eNlight operations have to sign strict privacy policies with heavy penalties & legal implications in case of the breach. Additionally, the entire facility is physically protected with 7 layers of security along with 24x7 surveillance monitoring. The floors are free from personal items like bags & electronic gadgets. To ensure protection from online threats, every device connected to internet is placed behind a firewall. These firewalls store logs of all activities carried out by any privileged user on associated terminals. Most operations are automated to eliminate human errors and Access Control Lists are maintained for privileged users. Network, nodes and storages are handled separately with independent rack biometric authentication.