Logbot

CHAT WITH YOUR MACHINE

Security concerns

Logbot security concerns

- ✓ **Logbot** security concept is based on the leading cyber security standards: ISO 27001 (Information Security Management System Framework) and IEC 62443 (Industrial communication networks – Network and system security) and follows a holistic approach covering several protection controls
- ✓ Data classification and ownership:
  - **Logbot** treats all data stored in **Logbot Cloud** as confidential
  - The customer controls authorization levels and is the data owner
- ✓ Security mechanisms of **Logbot clients** follow best practices to protect ICS (Industrial Control System) systems:
  - Are in line with the leading security standard for industrial systems (IEC 62443)
  - Provide a secure on-boarding process to connect to **Logbot**, using a UUID and providing logical separation between the automation and transmission grids
- ✓ Communication and network security controls, amongst others:
  - Internal communication in **Logbot** platform is encrypted (HTTPS)
  - Data in rest is located on DigitalOcean datacenters that comply to cyber security best practices and state-of-the-art requirements
  - Data in motion is 256 bit SSL/TLS encrypted
  - Network segmentation
  - Redundancy
  - System integrity controls like malware protection, patch and vulnerability management in place

More information on Logbot user manual

Service provider security (DigitalOcean)

Physical Security
Our datacenters are co-located in some of the most respected datacenter facility providers in the world. We leverage all of the capabilities of these providers including physical security and environmental controls to secure our infrastructure from physical threat or impact. Each site is staffed 24/7/365 with on-site physical security to protect against unauthorized entry. Security controls provided by our datacenter facilities includes but is not limited to:

- 24/7 Physical security guard services
- Physical entry restrictions to the property and the facility
- Physical entry restrictions to our co-located datacenter within the facility
- Full CCTV coverage externally and internally for the facility
- Biometric readers with two-factor authentication
- Facilities are unmarked as to not draw attention from the outside
- Battery and generator backup
- Generator fuel carrier redundancy
- Secure loading zones for delivery of equipment

Infrastructure Security
DigitalOcean's infrastructure is secured through a defense-in-depth layered approach. Access to the management network infrastructure is provided through multi-factor authentication points which restrict network-level access to infrastructure based on job function utilizing the principle of least privilege. All access to the ingress points are closely monitored, and are subject to stringent change control mechanisms.
Systems are protected through key-based authentication and access is limited by Role-Based Access Control (RBAC). RBAC ensures that only the users who require access to a system are able to login. We consider any system which houses customer data that we collect, or systems which house the data customers store with us to be of the highest sensitivity. As such, access to these systems is extremely limited and closely monitored.
Additionally, hard drives and infrastructure are securely erased before being decommissioned or reused to ensure that your data remains secure.

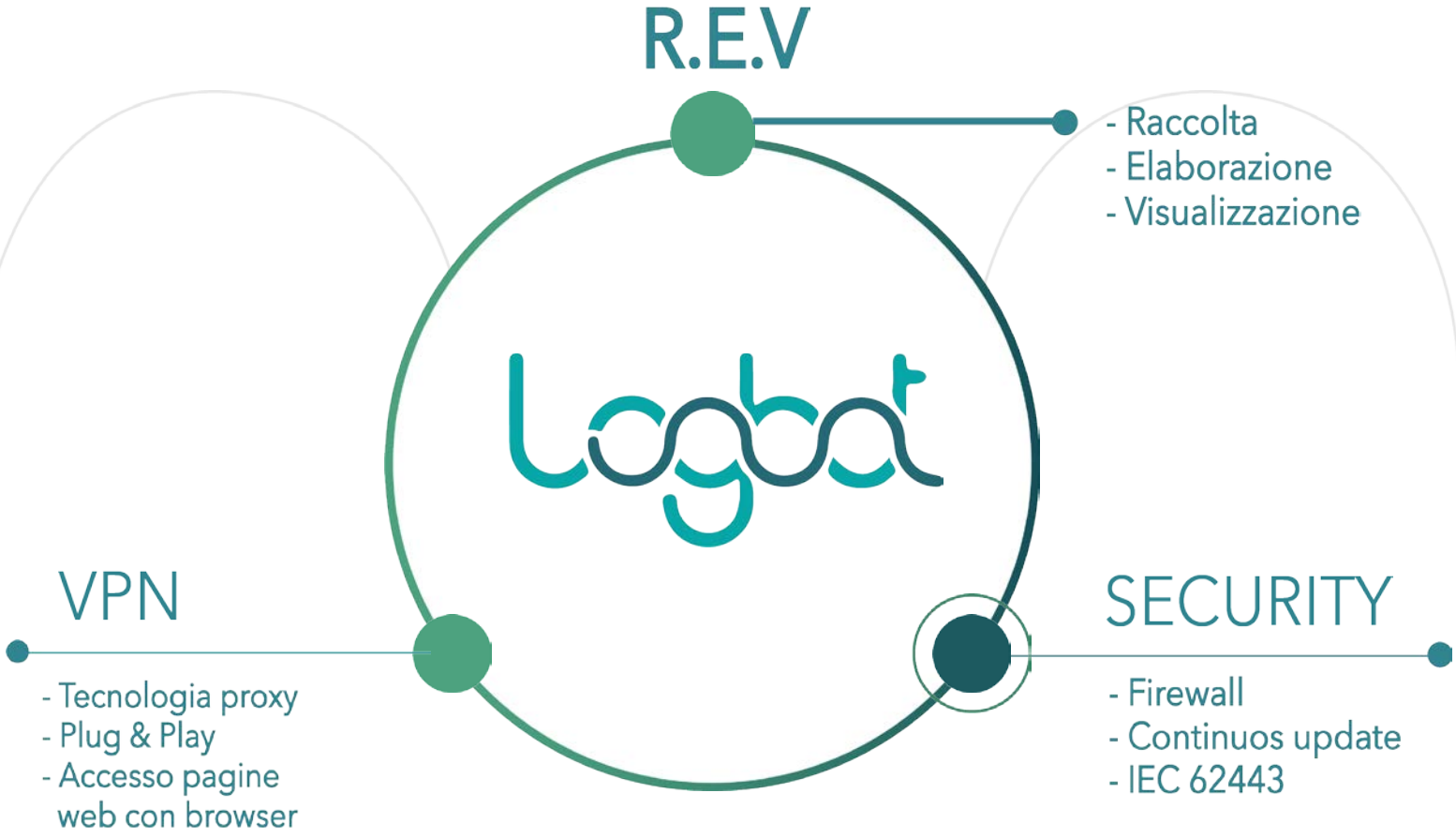
Access Logging
Systems controlling the management network at DigitalOcean log to our centralized logging environment to allow for performance and security monitoring. Our logging includes system actions as well as the logins and commands issued by our system administrators.

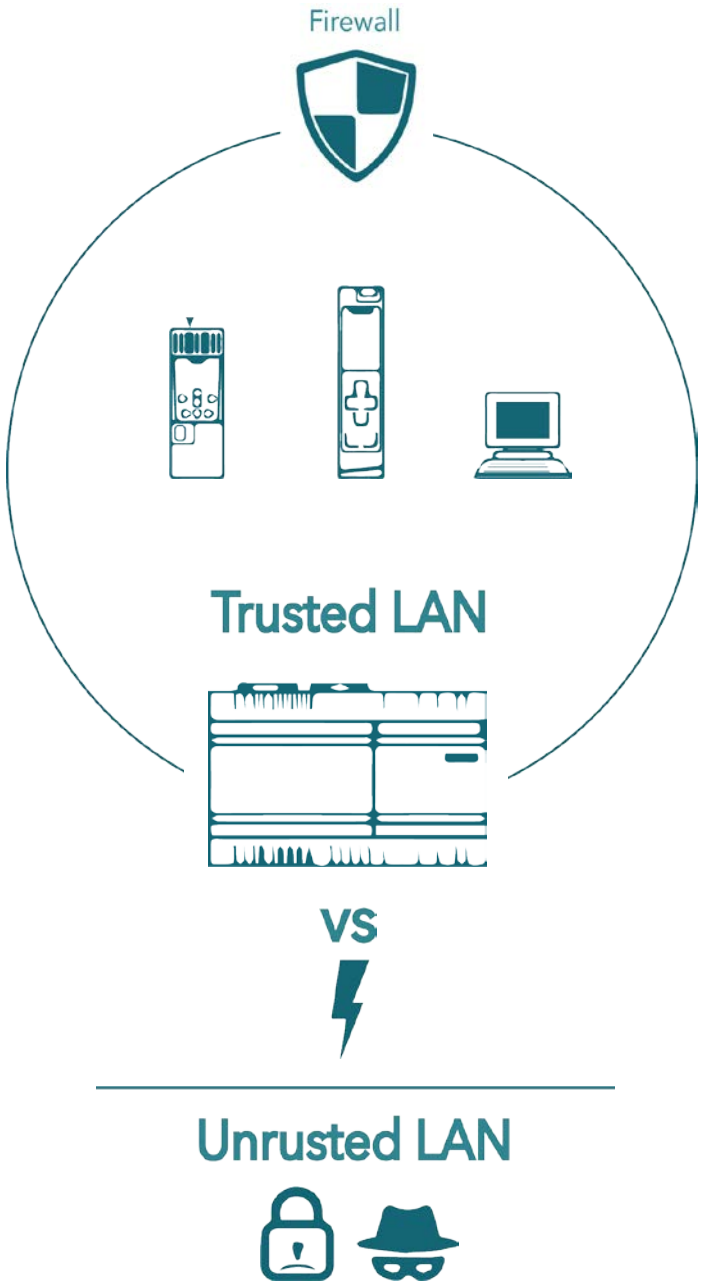
Security Monitoring
DigitalOcean's Security team utilizes monitoring and analytics capabilities to identify potentially malicious activity within our infrastructure. User and system behaviors are monitored for suspicious activity, and investigations are performed following our incident reporting and response procedures.

Droplet Security & Employee Access
The security and data integrity of customer Droplets is of the utmost importance at DigitalOcean. As a result, our technical support staff do not have access to the backend hypervisors where virtual servers reside nor direct access to the NAS/SAN storage systems where snapshots and backup images reside. Only select engineering teams have direct access to the backend hypervisors based on their role.

Snapshot and Backup Security
Snapshots and Backups are stored on an internal non-publicly visible network on NAS/SAN servers. Customers can directly manage the regions where their snapshots and backups exist which allows the customer to control where their data resides within our datacenters for security and compliance purposes.

LOGBOT è il sistema operativo per **SIMATICOS**





Protezione della cella di automazione con Logbot:

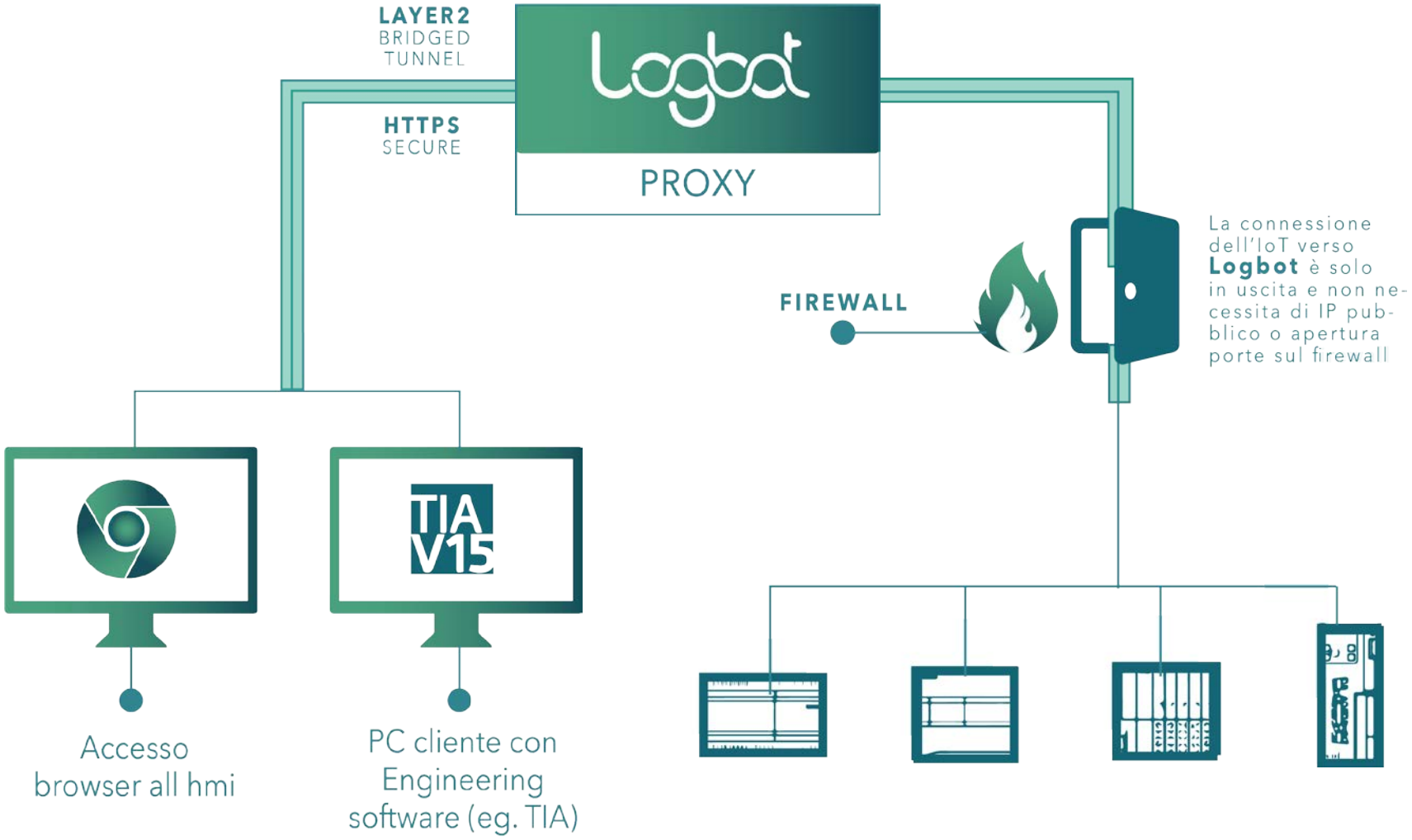
- Segmentazione di rete attraverso interfacce di rete separate da Firewall

- Comunicazioni cifrate mediante protocollo TLS/SSL a 256bit(vpn e trasmissione dati)

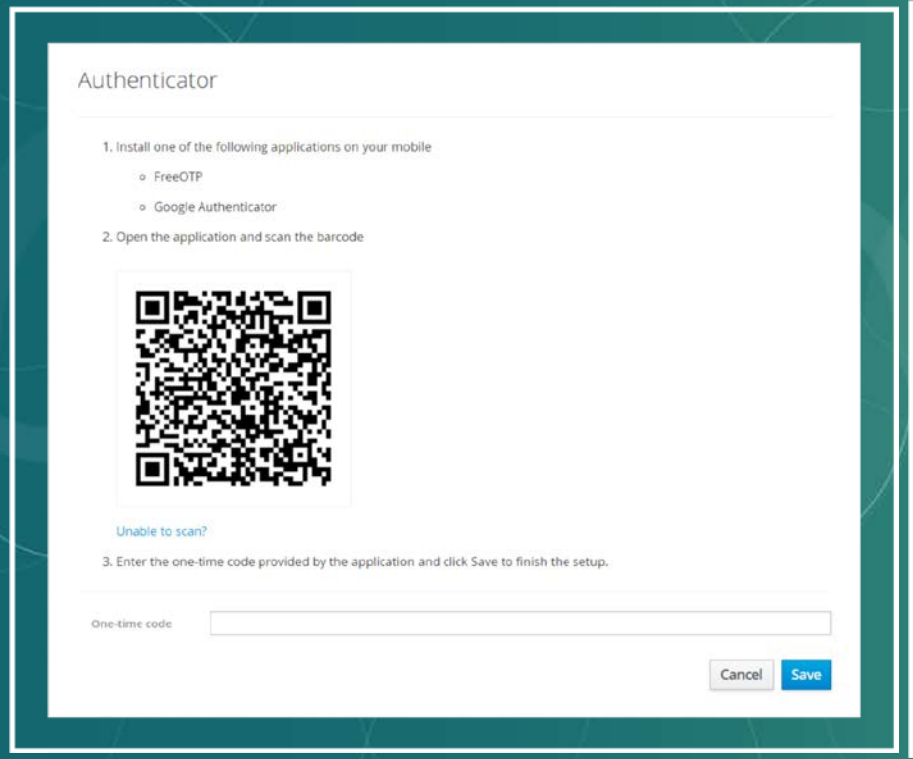
- Aggiornamento continuo di security patch e nuove funzionalita tramite tecnologia docker

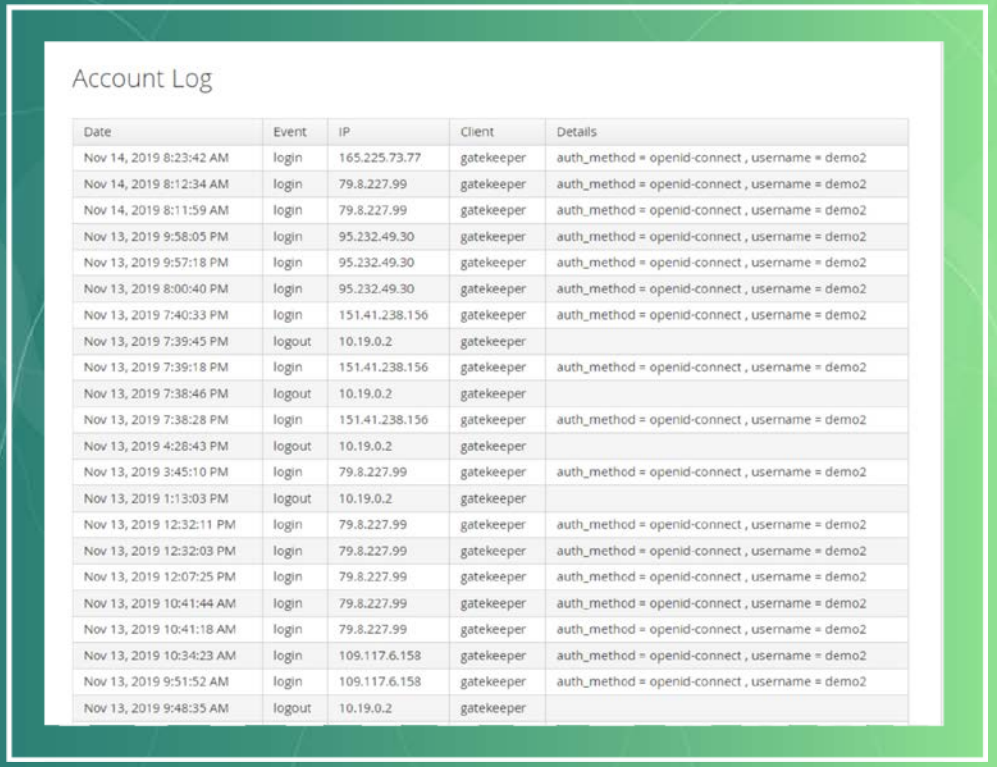
- Audit degli accessi e delle attivita` e autenticazione sicura a due fattori (2FA)

VPN proxy di nuova generazione



AUTENTICAZIONE A 2 FATTORI E AUDITING DI SICUREZZA





Account Log

Date	Event	IP	Client	Details
Nov 14, 2019 8:23:42 AM	login	165.225.73.77	gatekeeper	auth_method = openid-connect , username = demo2
Nov 14, 2019 8:12:34 AM	login	79.8.227.99	gatekeeper	auth_method = openid-connect , username = demo2
Nov 14, 2019 8:11:59 AM	login	79.8.227.99	gatekeeper	auth_method = openid-connect , username = demo2
Nov 13, 2019 9:58:05 PM	login	95.232.49.30	gatekeeper	auth_method = openid-connect , username = demo2
Nov 13, 2019 9:57:18 PM	login	95.232.49.30	gatekeeper	auth_method = openid-connect , username = demo2
Nov 13, 2019 8:00:40 PM	login	95.232.49.30	gatekeeper	auth_method = openid-connect , username = demo2
Nov 13, 2019 7:40:33 PM	login	151.41.238.156	gatekeeper	auth_method = openid-connect , username = demo2
Nov 13, 2019 7:39:45 PM	logout	10.19.0.2	gatekeeper	
Nov 13, 2019 7:39:18 PM	login	151.41.238.156	gatekeeper	auth_method = openid-connect , username = demo2
Nov 13, 2019 7:38:46 PM	logout	10.19.0.2	gatekeeper	
Nov 13, 2019 7:38:28 PM	login	151.41.238.156	gatekeeper	auth_method = openid-connect , username = demo2
Nov 13, 2019 4:28:43 PM	logout	10.19.0.2	gatekeeper	
Nov 13, 2019 3:45:10 PM	login	79.8.227.99	gatekeeper	auth_method = openid-connect , username = demo2
Nov 13, 2019 1:13:03 PM	logout	10.19.0.2	gatekeeper	
Nov 13, 2019 12:32:11 PM	login	79.8.227.99	gatekeeper	auth_method = openid-connect , username = demo2
Nov 13, 2019 12:32:03 PM	login	79.8.227.99	gatekeeper	auth_method = openid-connect , username = demo2
Nov 13, 2019 12:07:25 PM	login	79.8.227.99	gatekeeper	auth_method = openid-connect , username = demo2
Nov 13, 2019 10:41:44 AM	login	79.8.227.99	gatekeeper	auth_method = openid-connect , username = demo2
Nov 13, 2019 10:41:18 AM	login	79.8.227.99	gatekeeper	auth_method = openid-connect , username = demo2
Nov 13, 2019 10:34:23 AM	login	109.117.6.158	gatekeeper	auth_method = openid-connect , username = demo2
Nov 13, 2019 9:51:52 AM	login	109.117.6.158	gatekeeper	auth_method = openid-connect , username = demo2
Nov 13, 2019 9:48:35 AM	logout	10.19.0.2	gatekeeper	

GRAZIE PER L'ATTENZIONE

Logbat