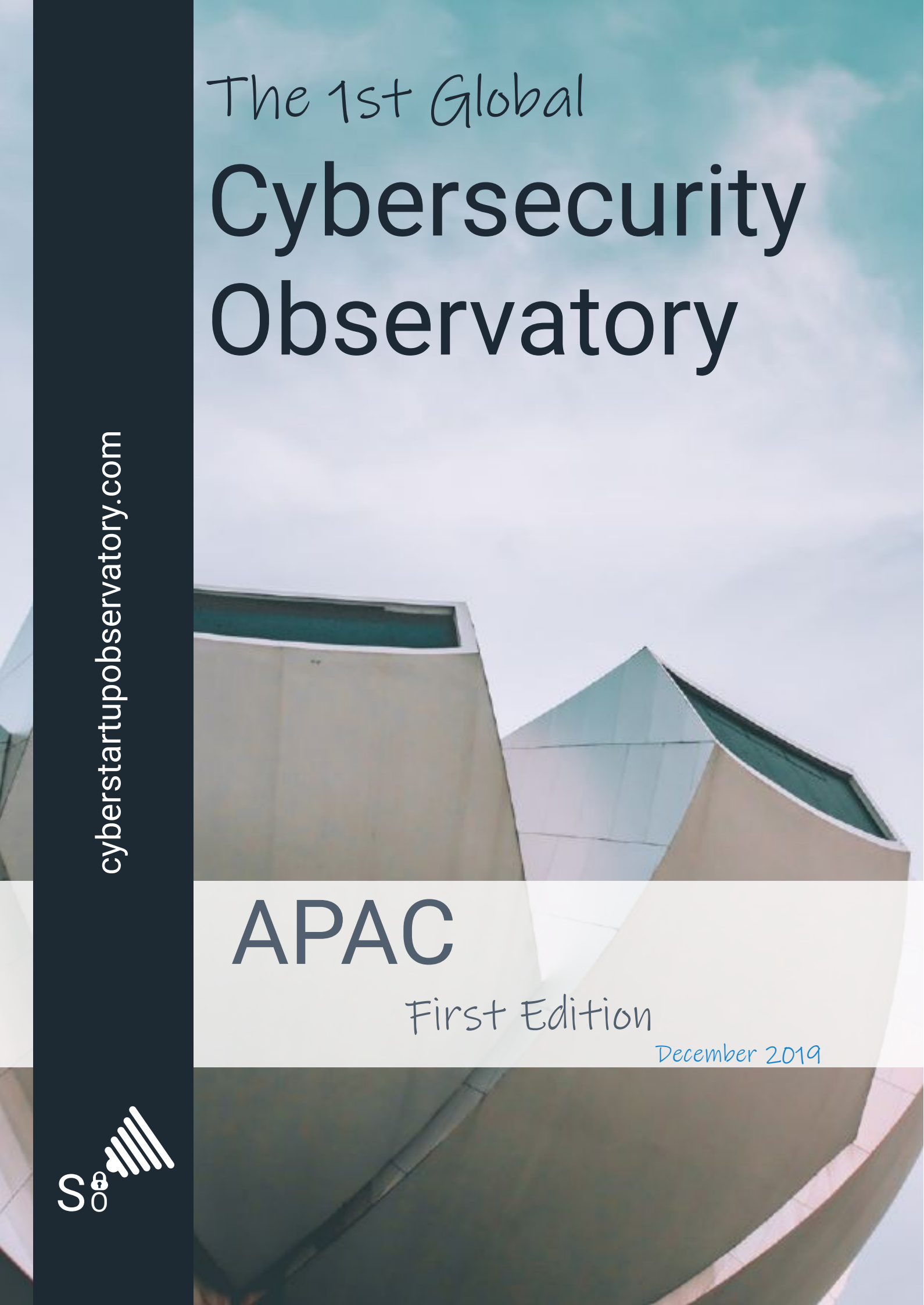


The 1st Global

Cybersecurity Observatory

cyberstartupobservatory.com

APAC

First Edition

December 2019

Insight

Blu5 Group

Digitalization of the Energy Sector: Innovative approach to reduce the risks of cyber attacks

Digitalization of the Energy Sector: Innovative approach to reduce the risks of cyber attacks

Authors: Antonio Varriale, Giorgia Somma, Blu5 Group

At a glance

- 5 minute read
- IT/OT Isolation
- Plants' networking security
- Isolation and security
- Seamless cryptography and user experience

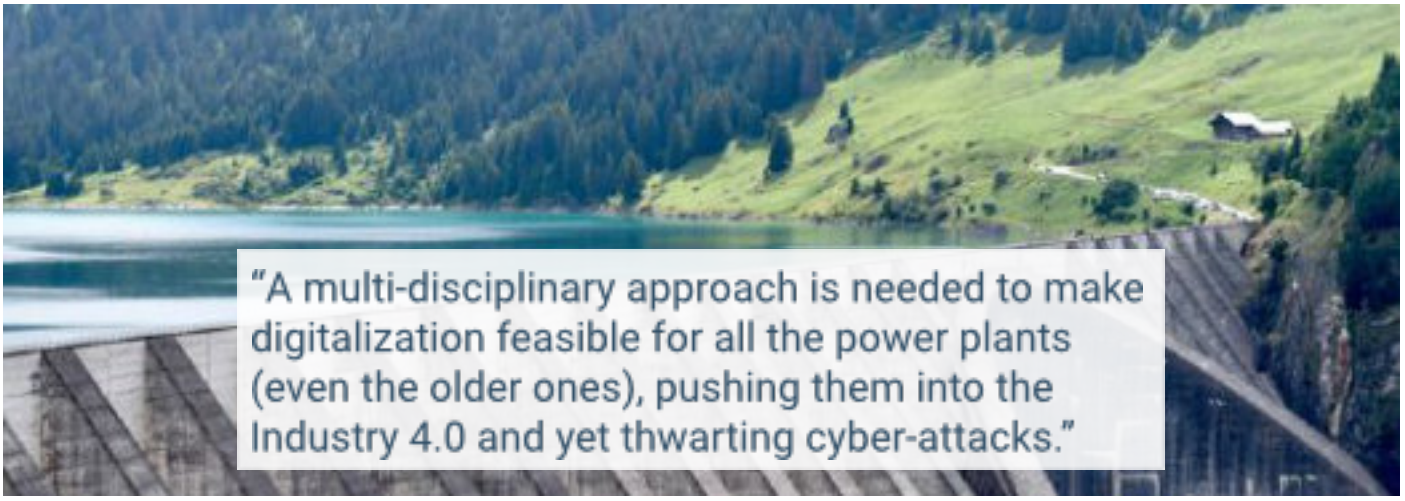
IT/OT Isolation

Initially, Industrial Control Systems (ICS) were isolated systems running proprietary control protocols using specialised hardware and software. The Internet of Things (IoT) and digitalization have been reshaping the energy landscape over the past few decades: billions of physical devices are now connected to the internet, collecting and sharing data.

The technology advancement makes feasible the Big Data Analysis, which brings enormous opportunities: performing predictive maintenance, optimizing operation costs, reducing outage time, turning raw data into useful business information and many others.

This said, however, many power plants, especially the larger ones, which are considered critical infrastructures for the electrical grid, still use the approach of completely isolating the IT and OT domains, missing out on opportunities.

Due to increasing need from OT system vendors to monitor and control sensors and connected systems as well as easily analyse, manage and monitor Big Data from remote, this separation model has been increasingly compromised.



Collection and analysis of data is key to improving efficiency in power plant operation.

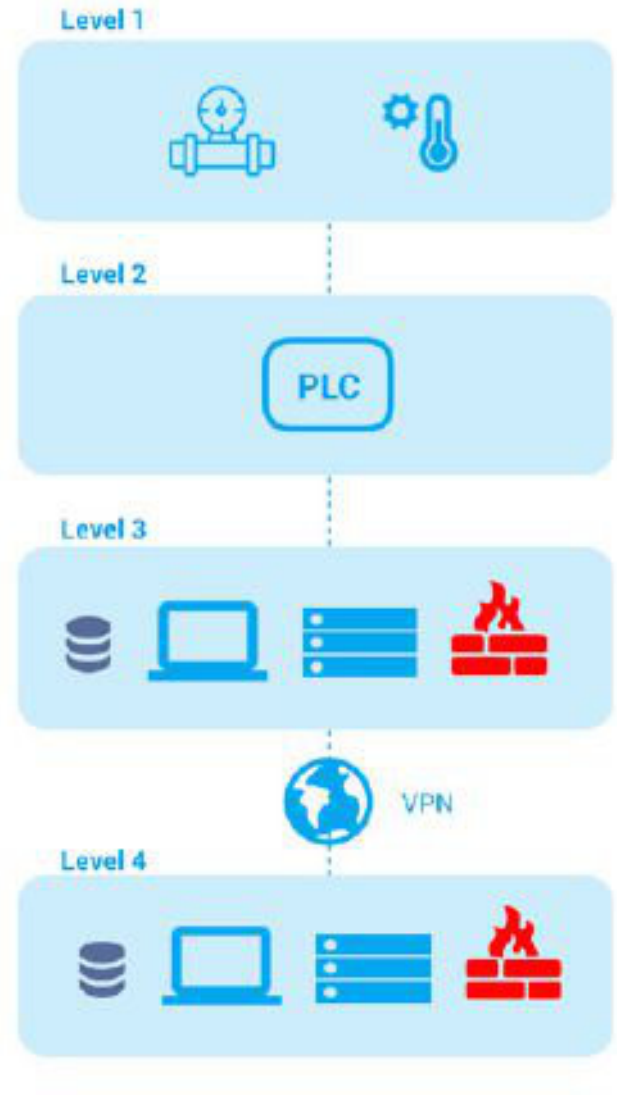
The fast-growing amount of power plant data collected and stored in large and numerous data repositories has far exceeded human beings' ability for comprehension and optimization of information without powerful tools. The easiest way to perform efficient Big Data Analysis is therefore to integrate all the information in a unique platform.

Automated processes that are connected to the Internet, however, provide an attack vector. Power plants' Monitoring and Control Systems use computer hardware that can be exploited, while legacy supervisory computers can be hacked by exploiting known vulnerabilities in older operating systems, such as Windows XP. Older networked sensors and actuators also pose a threat; first and second-generation Industrial Internet of Things (IIoT) devices were manufactured with zero security measures.

A multi-disciplinary approach is needed to make digitalization feasible for all the power plants (even the older ones), pushing them into the Industry 4.0 and yet thwarting cyber-attacks.

Plants Networking Security

The monitoring and control of power plant devices can be achieved with different network architectures. However, they all share a multi-layered architecture.



Power Plant Network Architecture

It can be noticed that, up to level 3 facility, management takes place within a local network - the so-called LAN - bound by the perimeter of the plant itself. With the advent of level 4 and the subsequent "connection" of the power plants to the internet, it is necessary to ensure an adequate level of security for the data involved in the transmission.

The most common way, in a power plant connected to the internet, is to provide a dedicated hardware device to the connection itself, which is a firewall. Through the firewall, acting as a gateway for all devices accessible from the outside, you can remotely reach the system. The most exploited solution involves the creation of a Virtual Private Network (VPN) tunnel between the Control Centre and the power plant, to ensure protection of exchanged data from unauthorized access.

Firewalls are used to verify the access to control networks. However, misconfigurations are common and usually not tested, thus enabling security weaknesses. Complex passwords, two-factor authentication and user awareness are good practices that help mitigate a successful cyberattack.

Many power plant operators do not want complex passwords or passwords that change periodically. Dictionary passwords such as "Password" can be exploited in a few minutes to gain access to a network.

A lot of power plants are using virtual private network (VPN) connections for remote starting and operation. VPNs can provide the ability for someone to hack into the plant and manage. If the attacker understands how to operate, damage can be significant.

Currently, the energy sector consists of both legacy and next generation technologies. New technologies mean new intelligent components (e.g. electricity or gas meters, digital valves or pumps) to the energy infrastructure that are highly interconnected. These new components are typically based on information and communication technology (ICT) interconnected to local networks.

According to RISI's (repository of industrial security incidents) latest update the number of cyber incidents against power plants has increased significantly since year 2000 and become more powerful. High-profile attacks on power grids have been unveiling the vulnerabilities of traditional security solutions. In the case of old legacy systems, patches do not exist or are prohibitively costly and difficult to implement. Patches for next generation technologies are constantly being issued, but are not enough and are particularly not effective against zero-day attacks.

"Attacks on critical infrastructures have increased and become more powerful....unveiling the vulnerabilities of traditional security solutions. In the case of old legacy systems, patches do not exist or are prohibitively costly and difficult to implement. Patches for next generation technologies are constantly being issued, but are not enough and are particularly not effective against zero-day attacks."

Nowadays the probability that cyberattacks have the ability to shut down power stations is very real.

ISOLATION AND SECURITY

In a scenario where power grids are fast becoming digital jungles, traditional network perimeter security solutions struggle to keep up with the complexity of hyper-connected systems. Organizations are shifting attention towards alternative solutions to perimeter security as they are gradually gaining awareness that a perimeter breach will give the hacker access to the entire Intranet. So, the starting point is recognizing that the network is always hostile and a zero-trust approach is required. In a zero-trust environment, all hosts are treated as if they are connected to the internet and the network is compromised. Organizations should therefore not automatically trust anything inside or outside its perimeters and instead grant access to its systems to authorized entities only.

Today Cyber Security solutions have to deal with the ever-growing variants of attacks and vulnerabilities having to screen multiple attack vectors. Next-generation technologies have in fact dissolved the corporate perimeter causing the attack surface to grow exponentially.

This increases the workload of Cyber security systems hence reducing the efficiency thereof. In the panorama of Cyber Security solutions to protect Critical Infrastructures, a gap is there in the provisioning of new network perimeters restricting inbound traffic to reduce opportunities available to cybercriminals.

The proposed solution is the security foundation of the zero-trust model: **SEdesk™.**

A hardware-based security solution is presented as the right combination of application and network layer protection by isolation.

By defining a controlled perimeter, the solution provides fine-grained access control as well as data protection leveraging a proprietary technology applied both at network level and on endpoints.

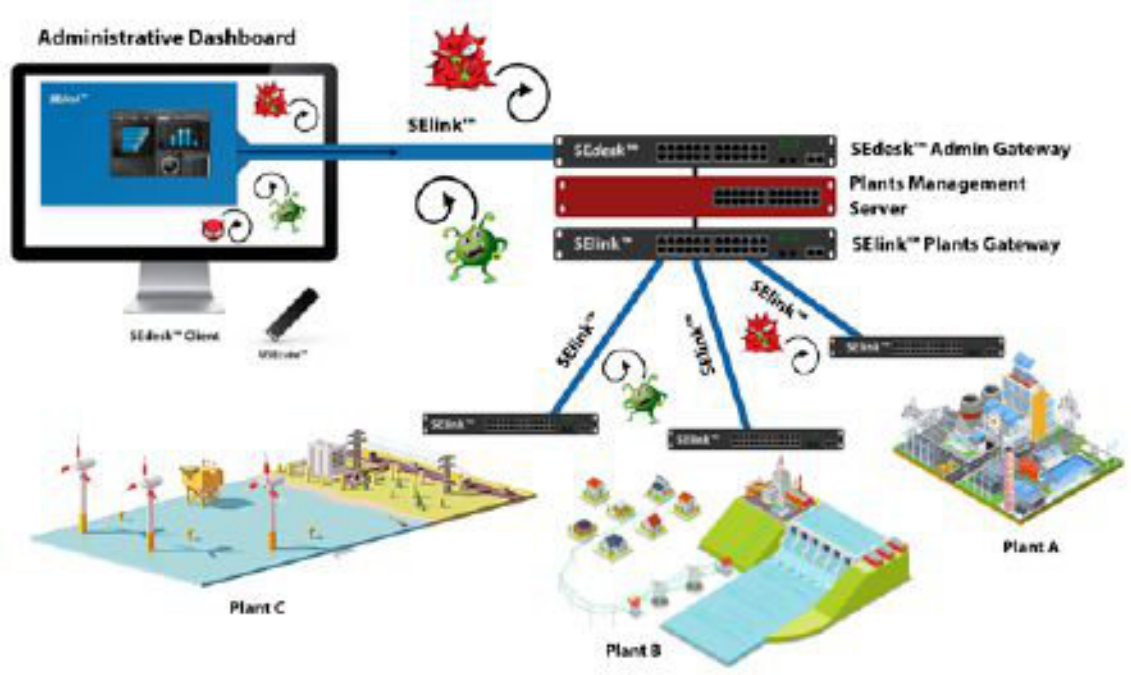
A multilayer and VPN-free approach is considered to control access privileges and secure data exchange between the central servers and the remote power plants, minimizing the impact of attacks.

All services of the energy provider (i.e. monitoring and management applications), whether web or legacy applications run in a secure and isolated environment: a unified workspace.

Restricted access to specific services is enforced on all users by means of fine-grained access policy rules, regardless of whether users are internal or external to the organization.

Access control of device, user and services is granted based on mutual multi-factor authentication with the Gateway following a negotiation of security and access policies.

Back-to-back connections to the Gateway are encrypted and signed, replacing obsolete VPNs, lacking the ability needed to protect digital organizations.



SEdesk™ network architecture

Services are made accessible, simultaneously, from different plants through single-port forwarding thus avoiding multiple port opening for each and every service, with the primary goal of reducing the surface of attacks.

Following changes in the network elements, policies are enforced automatically, involving zero-configuration efforts from the users. From an administrator perspective, an integrated user-friendly interface is required reducing the burden on the administrative tasks.

All data collected from the remote assets is stored in encrypted form at all times. This multi-layer approach protects both the network and the endpoints from data exfiltration.

Seamless Cryptography and User Experience

Although security is one of the biggest necessities in the digitalization era, most of the users refrain from including it in their processes either because it involves a change in their habits or because they do not really understand and control it.

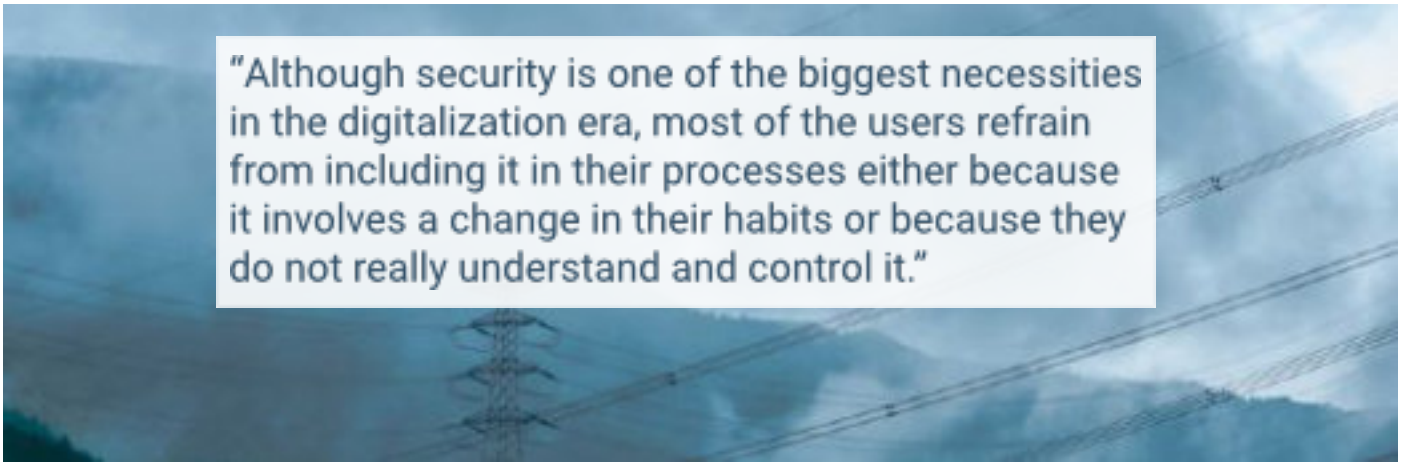
Traditional security technologies require complex installation and configuration procedures on both the client and the server side. For example, VPN clients require specifying several technical parameters to be installed, making the process very complex for standard users. Besides, the fragmentation of security techniques and protocols creates even more trouble for the final users creating a fast track to the company LAN for malwares and attackers residing on the client (Zero Trust).

A balanced trade-off between security and usability is one of the most valuable features of SEdesk™.

All the military-grade security mechanisms adopted by SEdesk™ are executed in a transparent way without any knowledge on the user side.

The level of control and flexibility provided by SEdesk™ also prevents user/operator mistakes. For example, in case of multi-plant management systems, the SEdesk™ client is connected to multiple plants at the same time showing the right control application for each plant, without any margin of error.

Compatibility and conflict issues between the control applications and the operating systems are solved, since the SEdesk™ gateway converts any service (including native remote applications, remote desktops, ...) to HTML5/Javascript secure web applications which are locally rendered solely by the authorized SEdesk™ client.



The Cybersecurity Observatory

APAC - First Edition