Menlo Security

CASE STUDY

Protecting Gösgen Nuclear Power Plant from Web- and Email-Based Cyberattacks

Menlo Security Isolation Secure Web Gateway allows users to browse the web and access email as needed without putting the organization at risk.

Gösgen Nuclear Power Plant

Operational since 1979, the Gösgen Nuclear Power Plant in Switzerland provides 1,020 megawatts of electricity to the Swiss power grid.

Challenges

- Need to allow Internet access for employees without putting the organization at risk
- Existing homegrown Internet isolation solution was complex and time-consuming to keep updated
- Needed a solution that protected users without adding maintenance burden

Solution

- Menlo Security Internet Isolation Cloud
- Moves the fetch and execute commands off the end device and into a closed virtual browser environment
- Strips out active content and renders safe content to the user's browser

Client-Based Isolation Added Maintenance Burden

Needless to say, cybersecurity is critical for a nuclear power plant. One misstep, one infected computer, and power can be shut off across an entire region, putting lives at risk. And today, the risk of a cybersecurity breach has never been greater. It is easier than ever, for an attacker to spin up a phishing email, create a bogus web form, or infect a popular website with dangerous malware. In fact, according to the 2019 Verizon Data Breach Report, 99 percent of cyberattacks in 2018 originated from web and email.

The cybersecurity team at the Gösgen Nuclear Power Plant on the Aa River in Switzerland understands the risk better than anybody. Knowing that a cybersecurity solution needs to balance risk with employee productivity, the team originally focused on maintaining reliable yet secure Internet access for its users by *creating a homegrown isolation solution based on VMware ThinApp*. The proprietary solution essentially isolated all Internet traffic in a virtual browser far from the user's device—effectively shutting down malware access to the endpoint.

Isolation proved to be a highly secure, highly reliable technology that allowed users to browse the web and access email as needed without putting the organization at risk. The problem, however, was that ThinApp is rarely updated by VMware, transferring much of the regular maintenance associated with the Internet isolation solution to Gösgen's IT team. And even then, the cybersecurity team couldn't reliably guarantee that every client on every user device was up to date.

"We were falling behind more and more," said Manuela Schweizer, Security and Network Engineer for Gösgen. "[Specifically], the workload of preparing Firefox for virtual deployment was considerable. That is why we looked for a new solution that would keep up with browser development and reduce [IT] workload."

> ***Before, we had to manually examine every single potential malware problem. Now, my job is much easier. We enjoy the security we have achieved with the Menlo Security Internet Isolation Cloud.***
>
> **François Gasser**
> IT Security Officer,
> Gösgen Nuclear Power Plant

Menlo Security Internet Isolation Cloud

Schweizer and François Gasser, Gösgen's IT Security Officer, worked with BOLL Engineering and BNC Business Network Communications AG, the power plant's IT consulting and implementation partner, to find a reliable Internet isolation solution that would enable a native browsing experience for users while protecting Gösgen from all email- and web-based cybersecurity threats. The solution would also need to reduce the maintenance burden on the IT staff.

Trials were set up with two solutions, but it was quickly apparent that the Menlo Security Internet Isolation Cloud was the superior option—primarily because of Menlo's ability to generate exceptions directly from log files. This capability is important, Gasser says, because it speeds time to resolution, which matters when it comes to fast-moving cyberthreats.

The Menlo Security Internet Isolation Cloud powers the Isolation Secure Web Gateway and works by moving the fetch and execute commands off the end device and into a closed virtual browser environment while only safe content is rendered to the user's browser. All active code, including JavaScript and Flash, are executed in the virtual browser environment, where it has no access to the user's machine. Instead, users receive a rendered web page that has all the active code stripped out via a proxy service that removes scripts and automatically converts Flash videos to MP4 files. This eliminates the need to install any client software on endpoints, allowing users to surf the web and access links and documents in emails with no impact on speed, performance, or the native experience. The Menlo solution provided Gösgen with a web security solution capable of delivering traditional web filtering control and access, with the added benefit of unparalleled malware protection.

Seamless Rollout

Because of data privacy issues, the Gösgen cybersecurity team elected to deploy the Menlo Security Isolation Secure Web Gateway in a private cloud environment built and maintained by the IT team. In addition to the policy and management server, Gösgen currently operates four isolation nodes, which are responsible for the complex tasks of executing active code and rendering the adjusted version of the web content.

The rollout was seamless thanks to the cooperation between Menlo Security, BOLL, and BNC. Employees were informed about the new platform via intranet news, and training was unnecessary. In fact, users are completely unaware of the underlying technology. No agent or special browser needs to be installed on the end devices, and it was only the conversion from the previous virtualized browser to the Firefox browser installed locally on the clients that took extra effort.

Schweizer is pleased about the time-saving update mechanism that can be operated via a web interface. All other administration tasks can also be done intuitively via this web interface. “If there’s a problem with new firmware, a rollback is done just as easily,” he said.

No Malicious Code Reaches Endpoints

Since the end of February 2019, all 550 employees of the Gösgen Nuclear Power Plant plus a few external partners have been surfing productively via the Menlo Security Internet Isolation Cloud. According to Gasser, his team has the utmost confidence that no malicious code is able to reach endpoints, enabling him to sit back and relax and allow employees to access websites that had to be blocked before.

“Before, we had to manually examine every single potential malware problem,” he said. “Now, my job is much easier. We enjoy the security we have achieved with the Menlo Security Internet Isolation Cloud.”

BOLL
IT Security Distribution

BOLL Engineering AG (BOLL) is one of the leading value-add distributors in the Swiss channel business since 1988. Primarily focused on IT security and open networking products, BOLL offers its customers comprehensive services that go far beyond the usual distribution support.

The Menlo Security and BOLL partnership was key to KKG’s decision-making process to adopting Menlo’s isolation platform and enabling a Zero Trust Internet approach. BOLL’s support and understanding of the KKG business process ensured a smooth deployment of the Menlo solution.

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security has helped hundreds of Global 2000 companies and major government agencies achieve Zero Trust Internet. The company’s cloud-based Internet Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. The company was named a Visionary in the Gartner Magic Quadrant for the Secure Web Gateway.

Contact us
menlosecurity.com
(650) 614-1705
ask@menlosecurity.com