![FireEye logo]

# Email protection for World-Leading Particle Physics Research Facility

## FireEye Email Security at CERN

**CERN supplier**

### FACTS AT A GLANCE

**INDUSTRY**

Technology and Research

**SOLUTIONS**

- FireEye Email Security

**BENEFITS**

- All email traffic efficiently examined for malicious content

- No perceived impact on end users

- Full compatibility with existing security stack

### CUSTOMER PROFILE

Headquartered in Geneva, Switzerland, the European Organization for Nuclear Research, also known as CERN is a world-class laboratory for particle physics research. Established in 1954, CERN provides the infrastructure needed for high-energy physics research as well as housing the world's most powerful particle collider, the Large Hadron Collider (LHC). Run by 23 member-states, CERN brings together a community of more than 17,500 experts that are collaborating to advance the boundaries of human knowledge.
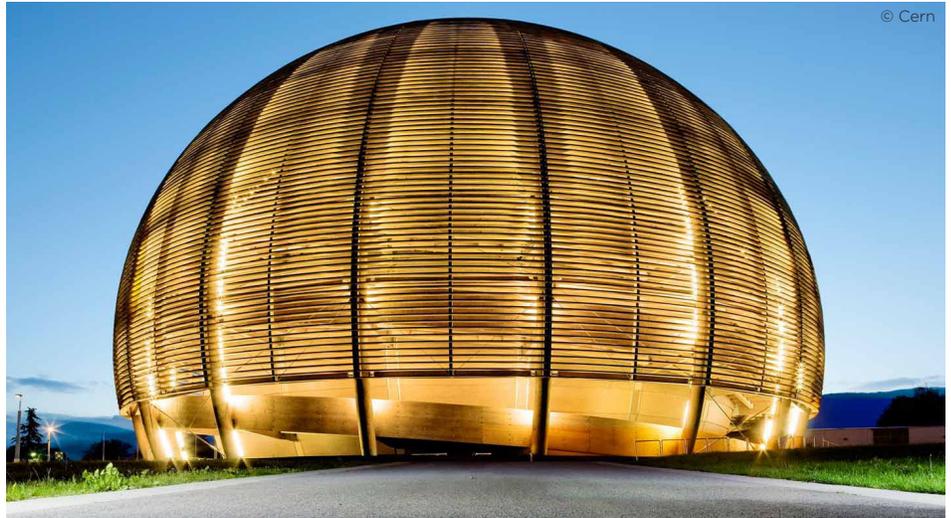


© Cern

At its core, CERN is all about matters of the universe. Dr. Stefan Lüders, computer security officer for the world-renowned organization, summarized the research as, "Trying to figure out what happened right after the Big Bang occurred and how this influences the way our universe works today."

To support its mission, CERN has created a massive IT infrastructure that facilitates collaborative research among thousands of global scientists. The LHC project alone generates over 80 petabytes of data annually. The organization's environment includes seven computer centers—comprising more than 10,000 servers and in excess of 330 petabytes of data—supplemented by the Worldwide LHC Computing Grid (WLCG). The Grid—the largest computing grid available today—is a global collaboration of more than 170 computing centers located in 42 countries that connects thousands of remote researchers.

On average, there are over 40,000 devices connected to the CERN network each day, two-thirds of which are owned by individual users. In addition to the in-house email system, a recent CERN study estimated that users are responsible for approximately 30,000 active personal email accounts in the environment, collectively accounting for over one million messages daily.

Considering the enormity of CERN's operations and volume of endpoints, end users constitute one of the organization's biggest vulnerabilities. Dr. Lüders elaborated, "At CERN we strongly encourage personal and academic freedom, so researchers are very accustomed to connecting their own computers to our network. This means they use their preferred operating systems and programming languages, and invariably give their devices full administrative rights."

# "FireEye Email Security provides us with an excellent solution protecting CERN against malicious email attachments."

— **Dr. Stefan Lüders,** Computer Security Officer, CERN

CERN's bring-your-own-device practice is a core focus of Dr. Lüders' security team. He commented, "As we have no direct control over how these laptops, smartphones and tablets are configured, we constantly inform end users that they are responsible for security on these devices. Protection starts with them taking ownership for the security of their own equipment."

Nevertheless, given the organization's widespread dependency on email, the plethora of inconsistently protected endpoints connected to CERN's network gave cause for concern. "Email can provide a dangerous foothold for malicious attacks against the organization," cautioned Dr. Lüders. "Being pragmatists, we knew that we needed a robust solution to secure this highly exploitable attack vector and implement it in a way that didn't feel overly restrictive to our users."

## Preventing Email-Borne Attacks

CERN has a very stringent selection process for goods and services selection. The security team investigated multiple options before ultimately deciding FireEye Email Security was the best match for CERN's needs. "We wanted a solution that could not only cope with the organization's email volume without causing delays but that would also integrate into the existing security stack," explained Dr. Lüders.

FireEye Email Security was deployed inline—delivering instant blocking of any malicious emails—and configured with redundancy to ensure continuous enterprise-wide coverage. "With imperceptible overhead, FireEye Email Security automatically and confidentially opens every attachment entering our environment in a detonation chamber to identify any malicious intentions. If nothing suspicious occurs, we confidently deliver that message to the intended recipient," remarked Dr. Lüders.

FireEye Support helped CERN successfully integrate FireEye Email Security into its infrastructure. FireEye Support provides CERN with immediate hotline access to trained professionals, 24 hours a day, 365 days a year. "Direct access to FireEye experts has been very important to our team. We appreciate knowing we'll be able to connect with a professional with the technical knowledge to quickly answer our questions. We've also established close relationships with the developers at FireEye, which helps assure us our needs and feedback are being heard and considered," enthused Dr. Lüders.

## Being Prepared for the Ongoing Demands of Cyber Security

Discussing the challenges and responsibilities of being in a CISO-level role in today's highly dynamic, volatile threat landscape, Dr. Lüders shared, "In cyber security, the advantage is with the attacker. A hacker only needs to find and exploit a single vulnerability in our infrastructure to be successful. For us to be successful, we have to defend the entire attack surface at all times."

To face this enormous challenge, Dr. Lüders forges forward defending CERN's environment. He concluded, "Working with FireEye, we've developed a strong mutual understanding of the unique nature of our environment and how to defend a typically highly vulnerable threat vector. FireEye Email Security provides us with an excellent solution protecting CERN against malicious email attachments."

To learn more about FireEye, visit: **www.FireEye.com**

**FireEye, Inc.**
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

**About FireEye, Inc.**
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™