# PROTECT YOUR DOMAINS FROM FRAUDULENT EMAILS

## and phishing attempts

### BACKGROUND:

**Why email authentication matters for businesses**

For more than two decades, Agilent Technologies has been a leader in the life sciences, diagnostics, and applied chemical markets. Agilent's expertise and trusted collaboration give customers confidence in the company's solutions. With phishing attacks on the rise and email as the backbone of the company's communications, Agilent wanted to adopt DMARC enforcement so it could extend this emphasis on confidence and trust to the safety and security of its email.

Agilent's goal of implementing and maintaining DMARC enforcement was a tedious journey that required significant overhead, effort and time from the IT team.

> "In hindsight, our journey to DMARC could've been so much faster if we'd adopted Valimail from the start. Valimail lets you get to DMARC "reject" within months. The solution made it easy to stop the risks of unauthorized senders and to get our email to a state of trust that emails received from our domains are legitimate."

**Scott Moore**
Messaging Service Manager,
Agilent Technologies

| | |
|---|---|
| **PRODUCT:** | ENFORCE |
| **INDUSTRY:** | Life Sciences, Diagnostics, and Chemical Markets |
| **LOCATION:** | Global |

TRUST YOUR EMAIL

## CHALLENGE:

### Finding an automated way to streamline email authentication efforts

With a diverse set of products and services, as well as global operations, Agilent had deployed a significant number of email domains and subdomains throughout the years. In the midst of this environment, Agilent was also experiencing phishing attacks that were becoming increasingly worrisome. “We had a handful of incidents where employees received an email that appeared to be an urgent wire transfer request from an executive. To the untrained eye, they looked like legitimate emails coming from an Agilent email address. We knew we needed a way to stop people from sending email attacks to our employees and to our customers that appeared to come from Agilent,” said Scott Moore, Messaging Service Manager, Agilent Technologies.

## SOLUTION:

### Providing employees and customers with confidence that emails from your company domain are legitimate

In its search for a solution, Agilent also wanted to prioritize an approach that worked well with its Microsoft 365 investment. “We knew by looking at options within the Microsoft security ecosystem, we would get a better end-to-end security suite of services,” said Moore. “I showed our leadership team the daily process we had been managing and, in contrast, how fast and simple Valimail makes things.” Within the first 30 days of adopting the solution, Valimail identified approximately 200,000 suspicious emails sent from more than 100 countries, all “from” Agilent domains. Valimail made it fast and efficient to stop these unauthorized senders, while also avoiding inadvertently blocking legitimate emails when Agilent moved to DMARC enforcement.