yubico

Fluidra enhances its global workforce security with YubiKeys

Case Study

FLUIDRA

Industry

- Manufacturing

Benefits

- Higher security and smooth login
- No mobile device required
- Easy integration with Google identities
- First step to passwordless environment

Protocols

- 2FA

Products

- YubiKey 5C
- YubiKey 5 NFC

Deployment info

- Privileged user accounts globally
- Alternative to mobile authentication

Fluidra Group – A global leader in the pool and wellness industry

Fluidra Group is a multinational group of companies, headquartered in Barcelona, Spain and present in more than 45 countries, with 135 sales branches and 36 production centers across the world. Fluidra's 7,000 employees develop, manufacture and distribute innovative products and services for the global residential and commercial pool market.

As the Chief Information Security Officer (CISO) at Fluidra, Ángel Uruñuela is responsible for corporate cyber security across the organization. His remit also includes product security, ensuring that any products controlled using Internet of Things (IoT) networks, for instance machines used to clean pools, are secure by design.

Responding to the growing cybersecurity threat

CISOs today operate in a challenging cybersecurity landscape, explains Uruñuela: "There is a lot of cybercrime, as well as more regulations coming soon from governments in both Europe and North America. Then there is the current economic situation, in addition to rising geopolitical tensions." Cybersecurity leaders like Uruñuela have also had to adapt to the rapid transformation caused by the pandemic: "companies moved many aspects of their operations to digital channels, and the challenge for CISOs is to ensure that every aspect of this new digital reality is secure by design. We must also factor in security fatigue, with employees authenticating onto a growing list of platforms."

For Uruñuela, the number one cybersecurity threat is ransomware. He compares the internet to a neighborhood: "As a wellness manufacturing company we may not be a prime target, but your security has to be at the same level as your neighbors because if not, criminals will break in no matter who owns the house." Fluidra has not had a major incident or data breach, but Uruñuela says, "All companies, and especially IT security & digital teams, have to be prepared."

Ángel Uruñuela
CISO for Fluidra Group

> "Twenty years ago, cybersecurity was something that took place in a dark, closed room. Now it's all over the news, but there is still a significant gap. Cybersecurity has to be in every medium-sized company. CISOs need to be able to implement real controls, because if it's not done properly, you're going to be in trouble."

> YubiKeys are fast, robust and best-in-class: a best-in-class device and best-in-class security. It's very smooth, and saves time compared to the people who have to enter the TOTP because you need to type six numbers, for every account. It's much faster just to touch a key."

Ransomware attacks pose serious challenges

For a CISO responding to a ransomware attack, the first challenge is to maintain business continuity, and swiftly return to operations. Secondly, the business must be able to prevent ongoing Denial of Service attacks, especially on IoT networks. The third task is to limit data leakage. As Uruñuela explains, "Even if you are able to recover from a ransomware attack, you will have a second attempt at extortion, threatening to dump any leaked data online."

Massive data breaches and business operations being suspended in the wake of an attack can devastate businesses. "We have seen companies much bigger than Fluidra having to close factories, which can cost them millions of dollars per day. Of course, this makes companies very motivated to pay a ransom", says Uruñuela. Not all incidents are public: "We see many incidents on the news, but if an attack has no direct impact on the consumer, it will not be visible. As a CISO, I hear about such incidents, at big companies, all the time."

Growing risk requires increased cybersecurity budgets

Awareness around cybersecurity is growing, but not always fast enough. According to Uruñuela, CISOs need to improve at justifying spending to CEOs and CFOs: "We need to start talking more in business language. It's very, very difficult to explain the return on investment."

Uruñuela sees regulations as an important driver of change: "I support the SEC proposal that regulated companies need to have somebody at board level who oversees cybersecurity and not only that–somebody who understands cybersecurity. President Biden's recent Executive Order will push cybersecurity in the federal government and other sectors in the U.S., while NIS2 will also push a similar conversation here in Europe. We're going to have many more regulations coming, and probably they will mention anti-phishing hardware tokens like YubiKeys."

Fluidra sought added protection for privileged identities

To protect Fluidra from ransomware attacks, Uruñuela decided to implement phishing-resistant Multi-Factor Authentication (MFA) for critical accounts and admins. While most of the organization already used mobile authentication to access cloud services, an alternative was also required for employees who didn't have a mobile device, or didn't wish to use one as MFA.

For Uruñuela, YubiKeys had clear advantages: "Everyone agrees that SMS is not as good as the rest. Time-based One-time Passwords (TOTP) can be a good balance as a backup or lower-cost solution, but are less secure, with a wide range of threat vectors that you don't have with a physical security key. Hardware security keys with FIDO protocol are far more advanced."

YubiKeys also offered an advantage when searching for cyber insurance: "It's going to be additional points, the more keys you have. If you can say that some part of your organization is using hardware security keys with FIDO, it'll give you a higher score, and a lower cost."

Personal use showed benefits of YubiKeys

As a cybersecurity veteran, Uruñuela has long used YubiKeys in his private life: "I bought my first YubiKey 12 years ago, and it still works. I have been in the industry for 22 years, with an offensive security-minded approach. When I first started hearing about hardware security keys with anti-phishing protection, new protocols, and two slots, it was the right device for me to buy. I remember I initially used one slot for my password manager, and the second for cloud services."

Ever since he bought his first YubiKey, Uruñuela has been a fan: "It works very well. It has best-in-class security. I like Yubico's vision and how it has evolved into new products like the YubiKey Bio with fingerprint reader." When choosing MFA for Fluidra, it was a simple choice: "YubiKeys checked all the boxes. We wanted security keys and contacted Yubico right away."

> Every day when I go to the IT department or I go to the physical areas, I see employees have their YubiKey hanging around their neck. It's part of their day-to-day life and day-to-day operations, and how they connect to systems. I don't think they even think about it."

YubiKeys give Fluidra employees higher security at work and at home

Fluidra chose a mix of YubiKey 5Cs and YubiKey 5 NFCs. All privileged accounts were given YubiKeys, while all other employees were offered a choice between mobile authentication and YubiKey as a second factor authentication for the corporate network, both on-site and remote.

Deployment was simple, explains Uruñuela: "The project went faster than we thought it would. YubiKeys work very well in our technological landscape. As a Google-centric company, the SaaS solutions we use most often are integrated with Google identities. Other non-integrated SaaS solutions are also compatible with YubiKeys."

Fluidra supports employees using their YubiKeys at home, too. Uruñuela explains that "In addition to the corporate scenarios where they are forced to use YubiKeys, they know they can also use them with multiple cloud services in their private lives. We encourage them to use it because if you protect your personal life and your personal devices, you are also protecting the company."

YubiKeys have enhanced Fluidra's security posture while saving time

Uruñuela is confident that YubiKeys have improved Fluidra's security: "Return on investment in cybersecurity is a very complicated matter, but I would say the return is very good. We have a key that ensures maximum security for access to certain systems. That was the goal: we achieved it, easily and painlessly. And the product works very well – that's all I can say."

For CISOs considering implementing robust MFA, Uruñuela has this advice: "Choose your methods wisely. Make sure you know your landscape, and that the methods you use are compatible with your landscape. Make sure you have a plan B. Choose something like hardware security keys which are multi-platform, for multiple devices, and work in many different scenarios."

The right onboarding for users is also important: "Have a great manual for newcomers so they know how to onboard a key. We created manuals in five different languages, using professional translators. Show employees that it's easy to carry around the key, and that it'll save time."

> Return on investment in cybersecurity is a very complicated matter, but I would say the return is very good. We have a token that ensures maximum security for access to certain systems. That was the goal: we achieved it, easily and painlessly. And the product works very well."

For Fluidra, the future is passwordless

Uruñuela sees the current deployment of YubiKeys as just a first step: "I envision in the next three years that everyone in the organization should have YubiKeys. My dream scenario would be one employee one key, with adaptive multi-factor authentication, to avoid security fatigue. That way, they don't use the key all the time, but only when additional authentication is required."

Ultimately, Uruñuela hopes for a passwordless environment: "I would like to see how two-factor authentication (2FA) becomes passwordless, combining this with the different identity and access management solutions we manage. In the future, everything is going to be 2FA and, depending on budgeting and cost, it's going to evolve into a passwordless situation in certain areas, I would say. It may take a few years, but in some cases regulations may even enforce it."

It may also be necessary for Fluidra to mandate YubiKeys for external vendors: "Third-party access has to be as secure as our internal access. It looks like digital supply chain attacks are going to grow in the future. Some people are also starting to talk about fourth-party risk, the third-parties of your third-parties. Critical vendors who have significant access to applications and data will have to be subject to the same security measures as internal employees."

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
5201 Great America Pkwy, #122
Santa Clara, CA 95054, USA
844-205-6787 (toll free)
650-285-0088