CASE STUDY

bell¿ngcat

Industry

Non-profit

At a glance

An independent collective of researchers, investigators and citizen journalists who have a passion for open source research

Staff and contributors in 20+ countries

Partnerships with news organizations and NGOs around the world

Key results

Faster time to authenticate

Fewer account lockouts and resets

Successfully thwarts highly targeted phishing attacks

Protocols

FIDO U2F

Yubico solutions deployed

YubiKey 5C NFC

Secure It Forward Program

Bellingcat secures high stakes investigative journalism with the Yubico YubiKey

> “As a security officer, you always look for the sweet spot between convenience and security. The YubiKey hits the mark really well because it’s very easy to use and very intuitive.”
>
> **Information Security Officer** | Bellingcat

An unyielding pursuit of the truth can result in being a target

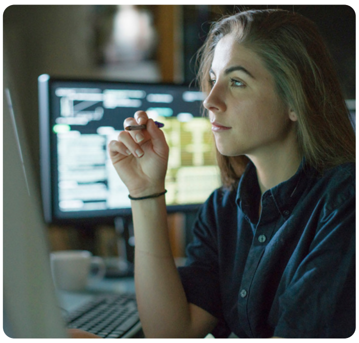
Bellingcat is based in the Netherlands, but the impact of its work touches every corner of the globe. Founded in 2014, this non-profit is an independent collective of researchers, investigators and citizen journalists brought together by a passion for open source research—whose pioneering methods shine a light on war zones, human rights abuses and the criminal underworld. Instead of focusing on breaking news, Bellingcat’s researchers take time to deeply analyze vast open source data and collaborate with an extended team of researchers and technologists.

Bellingcat have won awards and recognition for investigations ranging from the downing of Flight MH17 over eastern Ukraine to police violence in Colombia and the illegal wildlife trade in the UAE. Their work is regularly cited across international media as well as courts and investigative missions. It’s not just about in-depth storytelling, though—it’s also about more transparent journalism. Bellingcat holds tailored training sessions on ethical digital investigation and open source research for journalists, human rights activists and members of the public.

Bellingcat’s commitment to transparency and accountability makes them a prime target for bad actors who seek to prevent their story being told. This threatens not only their ability to pursue truth, but the security of their employees and extended team. Much of the responsibility of ensuring that the team is safe and secure falls to the Information Security Officer, who wishes to remain anonymous due to the sensitive nature of his work.

Bellingcat faces a myriad of threats, often state-sponsored, including highly targeted and sophisticated phishing, social engineering, malware and even infiltration and espionage. Many attacks aim to damage Bellingcat’s reputation.

> “We make some powerful people pretty angry, sometimes, with our stories. We try to challenge the official narratives in conflict zones, and sometimes it has a direct impact on the propaganda or the story that those governments are trying to project.”
>
> **Information Security Officer** | Bellingcat



"They try to find any way that can discredit our work," says the Information Security Officer. "That includes threats that could result in exfiltrating the personal data of our staff and where they live."

The organized crime networks and repressive states who seek to discredit Bellingcat have a variety of increasingly sophisticated tools at their disposal, thanks to a burgeoning industry of electronic spying tools available for purchase. Meanwhile, generative AI allows for even opportunistic criminals to create hard-to-detect phishing attacks. Like any non-profit, Bellingcat is constrained by limited budget and resources, and so must make complex decisions on how best to counter the risks they face.

> "It's a cat and mouse game. It has become more sophisticated, much harder to detect. Unfortunately, what I've seen over the last four or five years is an electronic spying industry that's ready to offer technology to the highest bidder."
>
> **Information Security Officer** | Bellingcat

YubiKeys chosen over Legacy MFA for global team

When the Information Security Officer arrived at Bellingcat, his first threat modeling exercise exposed high risks due to phishing and weak passwords. As an immediate response, stronger passwords were mandated, and a password manager was deployed. However, this was deemed insufficient in the long-term, and many potential alternative methods of multi-factor authentication (MFA)—such as SMS, phone calls or outdated mobile authentication—were also seen as too easily bypassed and so quickly ruled out.

Bellingcat required "robust" phishing-resistant MFA that would be effective globally, even for reporters located in countries where networks are insecure. "If you lose your phone, or your phone is compromised, then any two-factor authentication is kind of moot. We decided we needed a physical key that is completely disconnected from the internet, that cannot be hacked, that you physically have with you at all times," says the Information Security Officer. The YubiKey was the natural choice for this task. The Information Security Officer already used the YubiKey for his personal security, and had been an early adopter, discovering the device in 2014 as part of the internet freedom community and quickly identifying it as a "must-have".

The YubiKey enables Bellingcat to require hardware-based MFA for all accounts, significantly reducing the risks associated with phishing, compromised phones and weak passwords. All users were required to upgrade to the Google Advanced Protection Program, which mandates security keys for authentication into Google Workspaces, while the YubiKey will in future also secure Single Sign On to Bellingcat's CRM, Slack and other critical platforms.

Bellingcat was quickly able to mandate the use of YubiKeys across the entire global team. "We gave everyone a grace period," says the Information Security Officer, "and now it's the only MFA method they can use—no SMS, no calls, no Google Authenticator, only the YubiKey."

> “Everybody loves their YubiKey. We all have them on our keychain. I think it’s really perfect.”
>
> **Information Security Officer** | Bellingcat

That ease is critical because Bellingcat’s team has differing levels of tech-savviness, yet their work depends on being able to authenticate securely and quickly, without account lockouts and resets slowing down the progress of important investigations. Today, every new addition to the Bellingcat team receives two YubiKeys on day one—a primary key to put on a keychain and a backup to keep at home. The team is highly encouraged to use YubiKeys for their personal accounts, just like their Information Security Officer still does.

Looking ahead to passwordless authentication in the cybersecurity journey

Rather than operate in a silo, Bellingcat’s Information Security Officer is in daily contact with peers at media organizations and NGOs to share information and discuss best practices. Through these conversations Bellingcat learned of and successfully applied to Yubico’s Secure It Forward program, which donates YubiKeys to non-profits, election campaigns, journalists and humanitarian workers around the world. These collaborations bolster cybersecurity across diverse sectors, ensuring that organizations like Bellingcat can continue their critical work with enhanced protection against digital threats.

> “A password is not enough. You need something else, and that something else can only be the YubiKey.”
>
> **Information Security Officer** | Bellingcat

The added layer of security that YubiKey delivers helps Bellingcat continue its investigative work without compromising staff or data security, reinforcing the organization’s mission and operational integrity in a high-threat landscape. The Information Security Officer is confident that the YubiKey has made the organization more secure, and is now considering how Bellingcat can take the next step on their cybersecurity journey—going fully passwordless, with the YubiKey as a primary method of authentication.

Learn more | yubi.co/customers | yubi.co/contact

yubico

Yubico (Nasdaq Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA). The company is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries. For more information, visit: www.yubico.com.