

UK Communications Firm Communis Relies on Forcepoint to Protect Personal End Customer Data for its Financial, Insurance, Utility, and Government Clients

This marketing and communications agency trusts Forcepoint to secure its digital transformation while providing flexible security to keep its creative team productive and its clients' end customer communications safe.

Communis provides communications and print management services for some of the UK's largest government agencies, financial service firms, and insurance companies, as well as creative and point-of-sale marketing for global brands. These engagements require best-in-class cybersecurity solutions for data, web, email, and cloud. Communis has trusted Forcepoint Web Security, Email Security, and DLP to safeguard its people and data for years. Recently, the company has decided to enhance its security posture with Forcepoint Dynamic Data Protection for risk-adaptive data defense and CASB for visibility into cloud usage—to better align its security strategy with its digital transformation journey.

CUSTOMER PROFILE:

Marketing and corporate transactional communications, creative agency, and POS deployment.

INDUSTRY:

Marketing Communications

HQ COUNTRY:

United Kingdom

PRODUCTS:

- › Forcepoint Web Security
- › Forcepoint Email Security
- › Forcepoint DLP
- › Forcepoint DDP
- › Forcepoint CASB

Bank statements, insurance documents, credit card bills, and tax statements are a staple of our everyday financial lives and essential to financial service and government agency communications with their customers. In the past, these paper documents were expected to show up in the daily mail, but today, even the most traditional organizations are communicating with their clients via the channel that best fits their needs—whether it’s delivered in an envelope to a home mailbox or digitally via email or online portal. Helping top UK banks, insurance companies, and utilities such as British Gas deliver these one-to-one communications effectively and securely is UK marketing and communications agency Communis.

Part of the U.S.-based OSG Group and headquartered in London, Communis has approximately 1,500 employees serving customers across Europe. One side of its business focuses on the design, creation and delivery of those critical customer communications via multiple channels. A second side creates and delivers one-to-many brand communications spanning all sectors, channels, and geographies for global brands. Both sides of the business require the most effective cybersecurity to ensure both end customer PII and client materials are protected, but the sides differ significantly so flexible, risk-based security is key.

“The work we do for our clients means there’s a heck of a lot of personal data flowing through our network. We have to make sure that information is secure, plus protect for example, a proprietary marketing piece that a major brand is about to release,” said Michelle Griffey, Chief Risk Officer, Communis. “Communis has built up our expertise and our clients’ trust that we’ll keep their information safe over the last 10 years. It’s critical to our business.”

Moving to the cloud requires balance, but provides benefits to clients and end customers alike

Recently, Communis has started to take the digital transformation plunge by moving some of its activities and data to the cloud, where this can be done safely.

“It’s a fine balance because we have contractual requirements with a client who may go to cloud themselves, but may be somewhat more reluctant to allow a supplier to do the same, because there’s an element of risk in terms of the control,” said Griffey. “That just means that we have to be cautious and make that decision with our eyes open to both our clients’ requirements and our own needs and security.”

The clients and their end customers are driving this shift as well. “Historically bank statements or credit card statements may have been delivered in a printed format, but many of these organizations ideally would like their customers to review documents online for any number of reasons,” Griffey explained.

“Having a partner who can output communications via whichever channel the end customer wants is actually critically important for our clients. If an individual calls up their insurance company to make a policy change, they can request confirmation via whichever channel they prefer: print, email, etc. We can push it out, and if the email bounces for any reason, we’ll be notified and initiate a print and traditional mail send. This ensures that our clients are meeting their regulatory requirements.”

COVID-19 has expedited this move to offering more innovative services for Communis. Since clients may not be in a position to produce materials from multiple offices across multiple locations as more employees are working from home due to shut-downs, the company has recently begun offering a Hybrid Mail service. This can combine all of those documents from multiple employees under a same brand, batch it up, and send it to either print centers or out via email, negating the need for an employee to pick it up from an office printer.

CASB and Dynamic Data Protection deliver more visibility and flexibility to enable both sides of the business

The agency has relied on Forcepoint Web, Email, and DLP to ensure secure web traffic, email communications, and data



Challenges

Provide flexible cybersecurity to protect both sides of the business.

Ensure sensitive end customer personal data is safe in order to maintain client trust.

Support digital transformation and a move to the cloud.



Approach

Add Forcepoint DDP and CASB to the existing security infrastructure.



Results

- › Enabling creative productivity on one side of the business while safeguarding sensitive personal data on the other.
- › Built a strong partnership to overcome cybersecurity challenges.

visibility and control for several years, but the move to more cloud-based services drove a new direction for Communisis's security strategy. The company decided to expand its relationship with Forcepoint with the addition of Forcepoint Cloud Access Security Broker (CASB) and Dynamic Data Protection (DDP).

"We need CASB to start working through strategically how we can protect that cloud-driven future world, which is where we're all going," Griffey said. And Forcepoint DDP brings the ability to deliver a more flexible security posture—very helpful when the two sides of the business almost require two different approaches to data security.

"It's almost like there is a sliding scale of security need," Griffey said. "The creative for a new advert or marketing piece is just as important to that client as the hundred thousand individual personal records belonging to a bank. But, those records do need a different level of protection, because the details that you might find within a bank statement, which will go down to your pay, your mortgage, your spending habits, your bank account details, and where you live, can be really quite dangerous in the wrong hands. So, the protection around that data naturally needs to be higher up on the sliding scale."

"I find DDP incredibly exciting by virtue of the fact that we can start to be much more targeted in our security."

MICHELLE GRIFFEY, CHIEF RISK OFFICER, COMMUNISIS

"I find DDP incredibly exciting by virtue of the fact that we can start to be much more targeted in our security, rather than almost putting a wall up and saying, 'We're not going to let anybody do anything,'" Griffey said. "We can make the differentiation between

the one-to-one communication side which requires that higher security level and the one-to-many marketing side where they may be working on a bit of creative and need more freedom to collaborate. And I just think it's going to allow us to enable our teams to work better to their own role in their own job."

Fighting the same fight in the cyber world—where people are the biggest risk and the biggest opportunity

Forcepoint and Communisis have worked closely together to overcome any hiccups and challenges, to the point that when Communisis was considering adding a CASB and looking at the possibilities of DDP, the collaboration they'd built with Forcepoint gave them the confidence to move forward with those solutions and at the same time upgrade their support package.

"Over the last few months, we've had a real opportunity to work directly with Forcepoint to smooth out any issues in our environment and discuss how we can drive continuous improvement," said David Perkins, Communisis, Information Assurance. "Across the Information Security and IT teams, we feel that we have the best solutions for us."

"I look at this as a partnership," Griffey said. "I think we can work together when we have a unique implementation challenge to come up with a solution. And then, we can feed that information back into Forcepoint to share with your other customers. I can bet, if we're having the issue, then several other clients probably are also. Ultimately you benefit and other Forcepoint clients will benefit as well."

"That's why it's important that we work as partners with security firms like Forcepoint. We're all actually fighting the same fight when it comes to the cyber world," Griffey said. "And Forcepoint's human-centric approach to cybersecurity is critical, because ultimately, it is people who are potentially going to be our biggest risks, but they're also our biggest opportunity to protect ourselves."



"It is people who are potentially going to be our biggest risks, but they're also our biggest opportunity to protect ourselves."

MICHELLE GRIFFEY

CHIEF RISK OFFICER, COMMUNISIS