Forcepoint

Customer Story

Communisis Modernizes Their Forcepoint DLP with Risk-Adaptive Protection

This marketing and communications agency trusts Forcepoint to deliver Zero Trust protection by monitoring risky behavior to gain context into data security incidents.

Communisis provides communications and print management services for some of the UK's largest 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. Communisis has trusted Forcepoint Web Security, Email Security and Data Loss Prevention (DLP) to safeguard its people and data for years. Recently, the company implemented Risk-Adaptive Protection (RAP) as part of DLP to gain better context and understanding of user intent by focusing on users' interaction with data.

Bank statements, insurance documents and credit card bills are staples of our everyday financial lives.

In the past, these paper documents were expected to show up in the post, but today, even the most traditional organizations communicate 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 deliver these one-to-one communications is UK marketing and communications agency, Communisis. They know first-hand that they need the most effective cybersecurity to ensure that the data they interact with is safe everywhere they interact with it.

CUSTOMER PROFILE:

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

INDUSTRY:

Communications

HQ COUNTRY:

United Kingdom

PRODUCT(S):

› Forcepoint DLP with RAP integration

Expanding a Partnership

Communisis started partnering with Forcepoint on its digital transformation a few years ago, and the company hasn't looked back. More specifically, Communisis deployed products such as Forcepoint Web Security, Email Security and DLP Suite.

Communisis was never shy about taking on more Forcepoint products. In fact, Forcepoint helped them break out of a mold they were in with previous security vendors.

In the past, Communisis purchased security products, deployed them and then moved on to a new security vendor when it was time for a change. Their previous security vendors didn't offer the support they needed. On the other hand, Forcepoint offers Communisis a supportive partnership every day.

An example of the Communisis and Forcepoint partnership in action revolves around DLP policies. Communisis recently deployed several DLP polices aimed at employees' email usage. They generally block emails from work accounts to personal accounts, but they might want to allow some exceptions for business units that need more flexibility.

> "Forcepoint helps us understand the full capabilities of their DLP tools. They're always open to a call to walk us through anything."

Michelle Griffey
Chief Risk Officer, Communisis

Walking Communisis through DLP capabilities led to Michelle Griffey learning about one of Forcepoint's cloud-based DLP features: Risk-Adaptive Protection.

Modernizing DLP with Risk-Adaptive Protection

RAP helps organizations add Zero Trust data security through continuous monitoring of data usage. It also helps to uncover insider risk at the earliest point of detection and brings personalized automation to DLP policies.

As soon as Michelle and her team learned about this, they were ready to get on board. They're currently deploying RAP to 1,300 endpoints. Communisis has also started the process of integrating risky behavior analysis to inform DLP policies that help reduce false positives/false negatives and automate policy action enforcement.

A few examples of DLP policies with RAP in place for Communisis focus on employees' interactions with resumes and data related to mergers and acquisitions. Ensuring that employees don't put critical IP at risk is a major goal for Communisis, so protecting data in these areas is a priority.

> "We tend to be risk-averse as a company, so Risk-Adaptive Protection policies can help us verify that one of our developers, for example, isn't sending data that they shouldn't be sending."

Michelle Griffey,
Chief Risk Officer, Communisis

They wouldn't want their software engineers sending data related to banking details. However, an HR rep should be able to send materials like sick notes and resumes. Communisis can change policies based on user roles as needed.

CHALLENGES

- Provide flexible cybersecurity.
- Ensure sensitive end customer personal data is safe in order to maintain client trust.
- Reduce false positives/false negatives and automate policy action enforcement to make IT teams' job easier.

APPROACH

- Added Risk-Adaptive Protection to their Forcepoint DLP.

RESULTS

- Gained better context and understanding of user intent by focusing on user behavior and their interaction with data.
- Enabled safe collaboration on cloud applications by gaining insights into user engagement with data.

Modernizing DLP with Risk-Adaptive Protection (cont.)

Another benefit of Forcepoint RAP is that it offers flexibility in determining critical, high-, medium- or low-risk user behaviors. Continuous user validation makes this possible.

For instance, RAP can limit access based on unusual user activities that could indicate data compromise. RAP can also validate user risk through real-time monitoring of ongoing user and data interaction.

Communisis didn't want a black-and-white, on/off policy approach; they wanted to leverage adaptive, personalized policies that give the right people safe access to the right applications.

By leveraging insights into when users trend toward risky behavior, the policies take action to protect sensitive data. User actions that reach a high or critical risk score initiate an instant block, for instance. Communisis wanted to test these features with a couple policies at first, and they plan on adding more.

What's Ahead for Communisis

What's next for this partnership? Forcepoint is currently helping Communisis determine future RAP policies, including more types of access privileges that won't hurt sensitive IP. The goal is increasing employee productivity with individualized data security, so low-risk users can proceed as usual while limiting high-risk user activity. Identifying anomalous behavior risk from employees is a key part of that process.

> **"We plan to determine more RAP policies by looking at additional risky user behaviors. Monitoring anomalous behaviors that help us identify high-risk users is an incredibly exciting feature and is a huge reason we use RAP with Forcepoint DLP."**

Michelle Griffey
Chief Risk Officer, Communisis

When organizations like Communisis deploy DLP policies with RAP, they gain meaningful visibility into user interactions with critical data.

[FP-Customer-Story-Communisis] 11Jan2024