BlackBerry
Intelligent Security. Everywhere.

Case Study

# BlackBerry Empowers Jouve To Achieve Unified Endpoint Security Transformation

## Jouve

**Industry:**
Digital Transformation

**Employees:**
1,800 worldwide

**Location:**
Paris, France

**Product:**
BlackBerry® Protect

**Website:**
https://www.jouve.com/en/

JOUVE

If you ask the average Frenchman about the role that digital transformation plays in their daily life, you're likely to elicit little more than a shrug. Yet, digital transformation is quietly changing how French citizens interact with their government, their doctors, and their banks, among others, thanks to the information processing experts at Jouve.

For more than 30 years, Jouve has been one of Europe's digital transformation leaders. The company helps clients across the globe optimize their digital transformation and data management processes at every stage of the value chain, from acquisition to deployment. In addition to developing digital platforms, applications, and websites, the firm also offers a comprehensive portfolio of business process outsourcing infrastructure services. Jouve clients include France's six largest banks, 30 government departments and agencies, the publications department of the European Patent Office, and the top provider of learning solutions in the United States. Each year, Jouve produces and distributes content to 500 million Europeans in 23 languages. Currently, the company has a strong development in the health sector, conducting digital transformation for hospital and patient on-boarding.

## Digital Transformation Challenges

One of Jouve's greatest strengths is its ability to design applications that enable clients to streamline their business operations and create user-friendly experiences for their customers. For example, Jouve developed an application for the CPAM health insurance fund in Paris that utilizes handwriting recognition, video coding, data quality control, and secure data communications to automate the workflow and processing of more than four million medical claims each year. The system benefits healthcare providers by expediting reimbursements and integrating seamlessly with their electronic medical records systems. Patients also benefit, submitting claims simply by swiping a smart card at the provider's point of sale terminal.

Many firms that embark on similarly ambitious digital transformation projects soon discover the pitfalls of developing complex applications like these on their own. A Couchbase survey[1] of 450 IT decision makers in the U.S., U.K., France, and Germany found that 81% of respondents had a digital transformation project fail, suffer significant delays, or get scaled back. Another 86% said their firms had been prevented from pursuing such projects due to "reliance on a legacy technology, complexity of implementing technologies, and lack of resources and skills". According to the Harvard Business Review[2], an estimated $900 billion of the $1.3 trillion spent in 2018 on digital transformation projects went to waste.

## Jouve's Endpoint Security Transformation Begins

The individual responsible for cyber risk management at Jouve is Sébastien Drouin, whose roles include serving as chief information officer, chief technology officer, and member of the board. According to Sébastien, "We recognize that Jouve occupies a special position of trust in French society due to the sensitive nature of the data we manage for our customers. Therefore, as part of our ongoing security program, we decided to replace our signature-based legacy AV product with a solution that is more efficient, effective, and easier to manage."

The solution Sébastien envisioned would meet a number of key criteria. First, it would be transparent to end-users, especially the 250 developers that design and build Jouve applications. According to Sébastien, "Our developers often complained that their work was being interrupted by forced reboots during scans and signature updates by our legacy AV. This caused a 15% annual reduction in their productivity."

Sébastien also wanted to eliminate the administrative burden imposed on his team by the need to download, install, and audit a constant stream of signature update files. "Upgrading our endpoint defenses would enable us to focus on more strategic security initiatives," he says.

Most importantly, Jouve's new endpoint protection solution would have to be effective against advanced persistent threats and zero-day exploits. Sébastien knew this would require artificial intelligence (AI), a technology Jouve was already using effectively in its fraud detection product. Consequently, he and his team focused exclusively on short listing next-gen products as they prepared to begin a formal proof of concept (POC) evaluation. According to Sébastien, "BlackBerry was one of the first companies we invited to participate based on their sterling reputation and advanced AI technology."

"BlackBerry was one of the first companies we invited to participate in our proof of concept based on their sterling reputation and advanced AI technology."

*— Sébastien Drouin, Jouve CIO/CTO*

## Solution Testing and Deployment

During the subsequent POC, Sébastien and his team stress tested the candidate solutions on a wide variety of endpoint devices. CPU and memory usage were measured as systems were exposed to both commodity and advanced attacks. Metrics of protection, detection, and response effectiveness were captured and compared. When the POC ended, Sebastien selected BlackBerry as Jouve's new endpoint security partner. According to Sebastien, "BlackBerry Protect was not only the most effective solution at preventing malware infections, it was also the most economical in consuming system resources."

The deployment that followed proceeded efficiently and without incident. According to Sébastien, "We had no difficulties optimizing BlackBerry Protect for our environment. The whole process went extremely smooth. All of our endpoints were soon operating in a state of prevention."

## Transformation Achieved

Today, Sébastien's enthusiasm for BlackBerry and its security solutions remains undimmed. "BlackBerry Protect is performing exactly as expected," he says. "Our developers are happy because they're no longer contending with the performance and reboot issues caused by our legacy AV. Our security team is happy because they're no longer spending hours each week installing and auditing signatures updates. The board and I are happy because we've dramatically improved our cyber risk management profile. And our sales teams are happy because BlackBerry's stature and reputation help them close deals. All in all, our partnership with BlackBerry has proven to be an unqualified success."

> "BlackBerry Protect was not only the most effective solution at preventing malware infections, it was also the most economical in consuming system resources."
>
> *— Sébastien Drouin, Jouve CIO/CTO*

1 Digital Transformation Projects Continue to Be at Risk, Couchbase Research Finds

2 Digital Transformation Is Not About Technology.

## About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 150M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

*For more information, visit BlackBerry.com and follow @BlackBerry.*

BlackBerry
Intelligent Security. Everywhere.



BB20-0271 | 200609