CASE STUDY

Leading European law firm

corrata

Introduction

This leading European law firm has close to a thousand staff and offices across multiple countries and serves the needs of high profile domestic and international clients. The law firm has particular expertise in sectors such as renewable energy, healthcare, software, banking, property and environmental planning.

The firm is committed to the highest standards of information security and complies with a wide range of European, North American and International standards and regulatory frameworks. To achieve these high standards the firm compliments robust information security and risk management processes with best of breed security technology solutions

Security of client data is a core business imperative. Large sophisticated legal services organisations routinely deal with information which is highly sensitive. Investment proposals, merger and acquisition transactions and other large commercial deals are the everyday business of its staff. For this reason legal firms are prime targets for cybercriminals. And, in an increasingly fraught geopolitical environment, nation state actors and their accomplices can also be a threat.

The challenge

Demanding deadlines and staff who travel regularly makes frictionless access to information on the move essential to a modern legal services organisation. This has only become more important since the widespread adoption of remote working.

The firm has a mature security stack in place for traditional endpoints but were concerned that mobile could be a weak point. VMWare Workspace One is used to provide device management for iOS and Android devices but the firm identified that the additional layer of security provided by mobile threat defense was now essential.

Risk levels in mobile are rising. Business usage of mobile has grown as more and more enterprise applications are cloud delivered and, in parallel, cybercriminals have increased their focus on mobile as an attack vector. Phishing attacks, mobile malware and WiFi hacking are key threats. The firm was particularly concerned about phishing attacks delivered over SMS and the emerging evidence that such attacks can now bypass two-factor authentication. They were also concerned by the ease with which public and domestic WiFi networks can be compromised and by reports of sophisticated malware such as Pegasus silently infecting iOS and Android devices.

> **Today securing mobile devices is just as important as securing the corporate network, traditional endpoints or any other part of the enterprise.**
>
> IT Director

The solution

The firm was impressed with the Corrata solution for a number of reasons. Firstly Corrata provides a range of protections which goes well beyond the dns filtering and virus scanning offered by competing solutions. These include a range of unique protections against sms phishing, multiple cutting edge features to detect and intercept sophisticated malware infections and comprehensive protection against Wi-Fi attacks.

The second reason for selecting Corrata was because the solution's architecture provides protection without compromising either employee privacy or company confidential. By operating on-device Corrata avoids the need to collect privacy sensitive data such as location, browsing history, and information about files. This is very important to the firm as it is committed to ensuring that its security solutions minimise the need to collect privacy sensitive information. But it's not only employee privacy which is protected: Corrata's approach also ensures that client confidentiality is maintained.

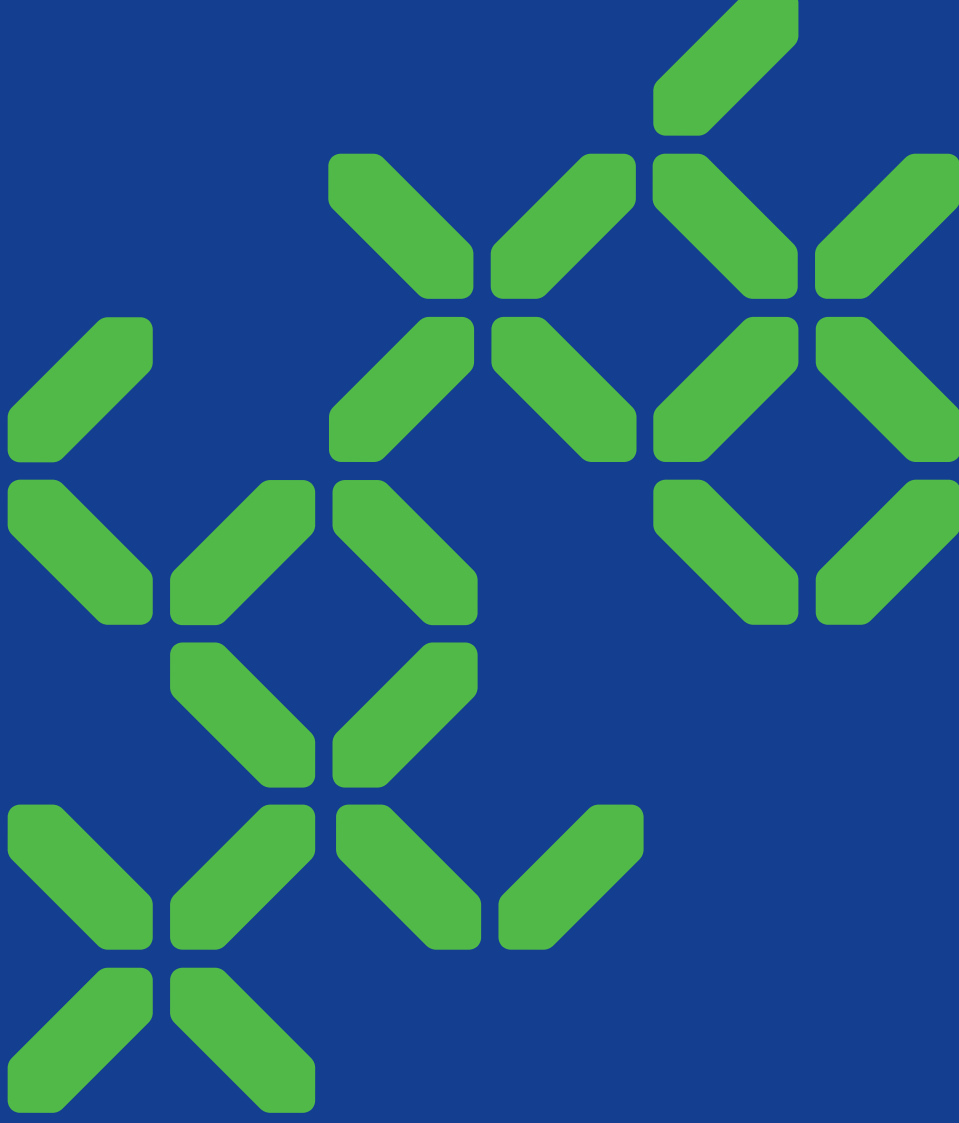
The firm was also impressed by the ease with which the solution was implemented. Integration with Workspace One took a matter of minutes. This enabled quick and simple enrollment of employee devices. Ongoing management has also proven to be straightforward and not resource-intensive. Integration with Workspace One simplifies adding, removing or updating devices. Corrata itself provides comprehensive reporting on threats and the security status of devices and makes it easy to undertake remediation actions where necessary.

> **Corrata goes beyond other mobile defense solutions and provides an unparalleled set of protections against mobile attacks.**

Head of Information Security

> **Corrata has proven easy to deploy and manage. Integration with Workspace One (UEM) was a matter of clicks. Ongoing management is not resource intensive.**

IT Manager



corrata

corrata.com