

## leading legal firm implements the fidelis platform to protect clients from advanced attacks



### customer profile

Domański zakrzewski palinka sp. K. (Dzp) the leading law firm in poland, has been providing expert legal services on behalf of major global organisations since 1993. The firm includes 9 practices, 40 specialisations, 30 partners and offices in warsaw, poznan, wroclaw, london and is part of a preferred business network of legal firms that spans 70 countries. Dzp has also been acknowledged as one of the top law firms in international specialist rankings: chambers & partners, legal 500, iflr1000, itr worldtax and wtr1000. The team specialises in all aspects of commercial, energy and natural resources, pharmaceutical and healthcare, technology, media and telecommunications law and other — their clients place their trust in dzp because of their access to information, know-how and ability to deliver complex solutions. The internal it department currently employs two security analysts who provide internal it services and support core the dzp business 24/7.

### business challenge

The increase in large scale ransom ware attacks — including wannacy and petya — have resulted in the rise of the level of risk of attacks. Dzp, which has visibility into client information relating to company mergers and acquisitions, company financial results, executive changes, power of attorney for representation in court and other market- impacting information before it is publicly released, is a prime target for advanced threat actors seeking lucrative inside information.

This led dzp, whose business model is highly reliant on the use of digital technology, to the decision that their traditional security solutions were inadequate to protect their client information from advanced threat actors.

Due to that dzp decided that with the ever-increasing sophistication of cyber attacks, it needed to ensure that client data was safe. The biggest security challenge was to figure out how to simultaneously compare historical security activity on the network against the current real-time data. The only way to do this, was to implement a modern solution that provided a superior ability to rapidly detect, investigate and resolve advanced attacks, enabling the company to detect both known and unknown threats.

### solution

Dzp was looking for a single integrated advanced solution that enabled them to both see and respond to advanced attacks, rather than a patchwork of systems, software and appliances that had to be purchased separately and strung together. Fidelis provides this capability in one single platform as well as easy scalability in future.

Dzp knew that the fidelis platform was recognised as an enterprise solution, trusted by major global organisations and many financial institutions in poland, across europe, and around the world. Also after further recommendations by key clients, dzp invested in fidelis.

Following a rigorous on-site assessment, dzp was pleased to find that fidelis provided them with a new depth of visibility, enabling them to analyse packets and sessions on the network, both in real-time and historically; spanning all ports, protocols and operating systems 24/7.

Not only this, but with two full-time analysts at dzp, fidelis has enabled them to automate the actions and insight of a much larger skilled team by consolidating alerts and helping them to mitigate risks. This leaves the executive board and partners at dzp free to run day-to- day business, confident in the knowledge that its clients' data is protected by fidelis.

## business benefit

---

The primary benefit that dzp receives from fidelis is the ability to detect, investigate and stop attackers at every stage of an attack.

"We chose fidelis because we wanted to partner with expert consultants who specialise in identifying and stopping advanced attackers" said dzp's it director marek laskowski. "For dzp to be the safest platform for our clients, we needed the strongest cyber- security partner in the business. Our business is branching out rapidly, so we have to have a security solution that can scale accordingly. The fidelis platform provides us with this capability."

Some of the specific benefits dzp has realised with the fidelis platform are:

- Reduce the time it takes to detect and resolve incidents: fidelis enables security analysts to move from alert to investigation using a simple interface, quickly receive relevant information and apply threat intelligence to network data.
- Correlate seemingly unrelated network activity and behaviour: by applying automated hunting and security analytics to retrospective metadata gathered on every network session, analysts can correlate seemingly unrelated network activity.
- Identify and stop advanced targeted attacks as they are beginning: by quickly identifying malicious behaviour including activity in network metadata, command and control activity and lateral movement, analysts can stop data theft before it takes place.

"The team at fidelis and its partner eversys sp.Z.O.O. Are absolutely professional. The expert advice and knowledge provided during implementation as well as on a day-to-day basis is outstanding. Fidelis helps us mitigate the risks to our business and reduce the overall cost of response. I use and would recommend fidelis every day," concludes marek laskowski, it director, domański zakrzewski palinka sp. K.

## vision

---

Through its partnership with fidelis and continued development of its security infrastructure, dzp is responding to the growing security concerns of companies by providing the safest information services platform available for its partners and clients around the world.