Retail Banking:
Portal Protection

In the world of retail banking, competition is fierce. Not only from the traditional high street, but also from new challenger banks and technology giants.

As cybercrime reaches an all time high, the importance of data protection in the banking sector is more crucial than ever. Finding a way to ensure cyber protection while maintaining user experience has become the focus for the future of cybersecurity.

CUSTOMER PROFILE:
UK National Bank

INDUSTRY:
Financial Services

HQ COUNTRY:
United Kingdom

PRODUCTS:
› Zero Trust CDR
› ZTCDR for Web Gateways

Improving experience & interaction

To continue to be competitive, this retail bank needed to offer an online portal where customers could apply for a mortgage. Ensuring that the process is fast, simple, and easy to use – but that did not offer a potential point of ingress for cybercriminals.

In particular, the bank needed to find a way to ensure documents and images submitted to the portal couldn't be used to introduce malware.

Zero Trust CDR

For the bank's security team, document uploads represent a particular concern. Overwhelmingly, malware designed to compromise networks and steal assets is initially introduced by being concealed in innocent-looking documents.

This "zero-day" malware routinely evades detection by conventional anti-virus products, so the team needed to find a better solution – one that would guarantee any document or image uploaded via the portal was totally malware-free and would not give the cybercriminals a way into the network.

The challenge was to offer an unbeatable level of experience and interaction via the portal, without compromising security. Instead of relying on detection-based anti-virus, the bank installed Forcepoint's Zero Trust CDR alongside its Web Application Firewall (WAF) to protect the portal.

The WAF acts as both an application firewall and a reverse proxy passing any document or image it receives via the portal to Zero Trust CDR.

Zero Trust CDR uses a unique process called transformation, whereby the valid business content is extracted from the uploaded document, the original is discarded, and a brand-new document or image is created. The document is delivered to the user without the user knowing the process has taken place.

Using this approach, the bank has strengthened its security posture. Every upload is transformed and guaranteed 100% threat-free of both known and unknown or "zero-day" malware.

GCHQ's National Cyber Security Centre (NCSC) recommends the use of transformation technology to counter "zero-day" malware.

Faster, better, risk free home buying experiences

Forcepoint's Zero Trust CDR is a key component in the cybersecurity platform deployed by the bank. It underpins faster, better home-buying experiences for customers together with improved operational efficiencies and cost savings for the bank.

The Zero Trust CDR transformation process is transparent to both the applicant and the bank employee. It is appreciably quicker than the alternative – and inferior – anti-virus scan. Uploaded documents are complete, fully editable, pixel perfect and 100% threat-free.

"Zero Trust CDR has been a key enabler in offering mortgage applicants a truly customer-centric experience. Applicants can quickly and easily upload documents in support of their home-buying journey, while the bank can be certain the documents it receives are completely malware-free."

Challenges

To offer an unbeatable level of experience and interaction via an online portal, without compromising security.

Approach

Installing Forcepoint's Zero Trust CDR alongside its Web Application Firewall to ensure both data protection and user experience.

Results

Using this approach, the bank has strengthened its security posture. Every upload is transformed and guaranteed 100% threat free of both known and unknown or "zero-day" malware.