

Web Document Upload with Zero Trust Content Disarm & Reconstruction

1 Customers, suppliers, etc. upload information such as CVs, invoices or ID documents providing attackers with a threat channel into a network.

2 The attacker uploads a malicious document via the corporate web portal which contains malware designed to evade detection.

3 The document is forwarded by the Application Delivery Controller, Reverse Proxy, Web Application Firewall or Firewall to Zero Trust Content Disarm & Reconstruction (CDR).



Extract
Content from Original Data,
Discard Unwanted Content

UNSAFE DIGITAL CONTENT

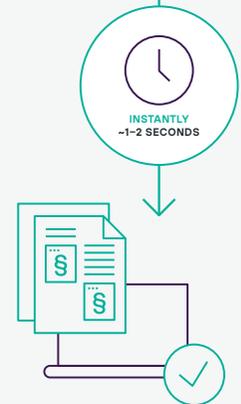
Verify
That the Information
is Safe

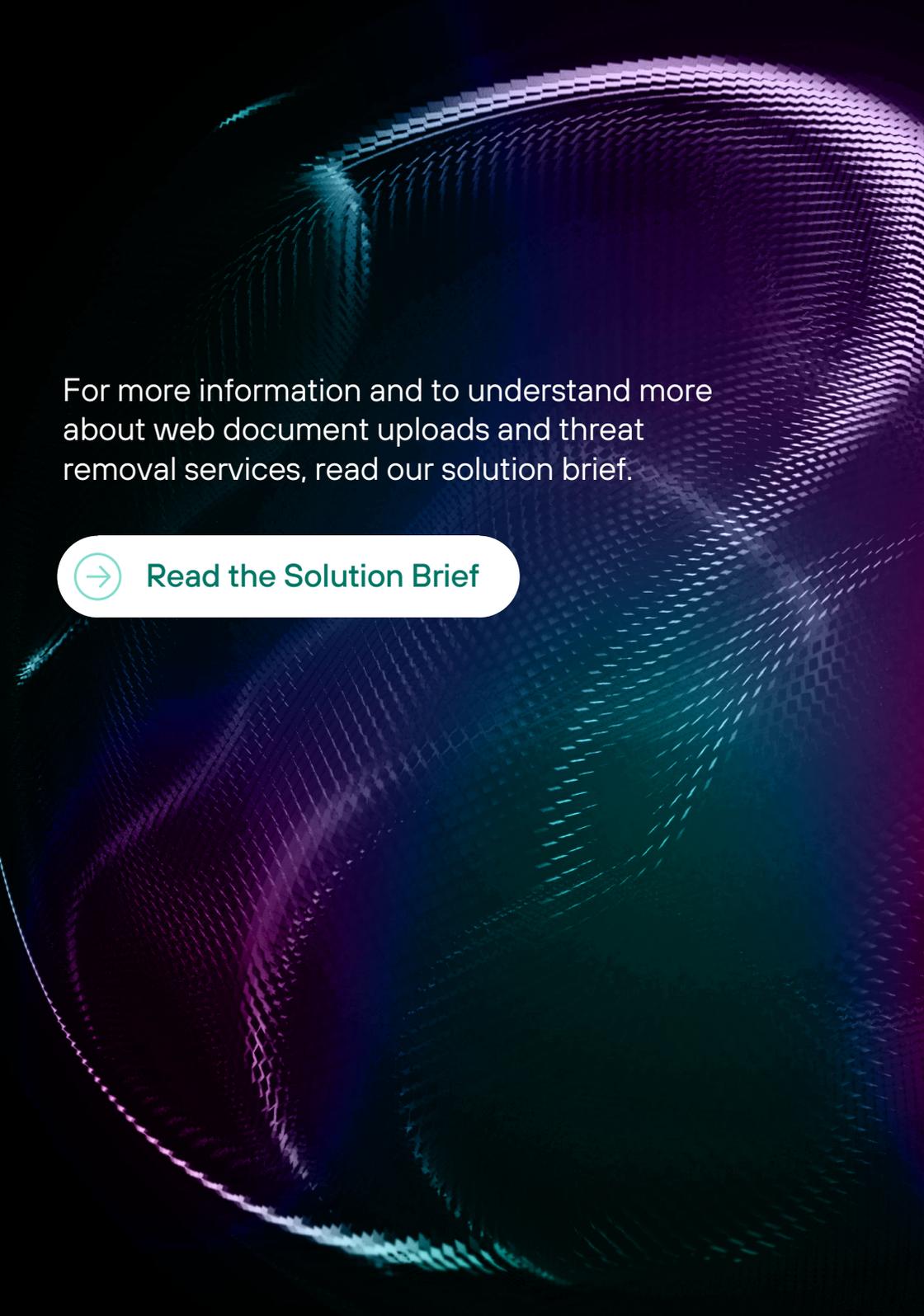
SAFE DIGITAL CONTENT

Build
And Deliver Safe
Information and Data

4 Forcepoint's Zero Trust CDR platform receives the document, extracts the valid business information, verifies it, discards the original, and builds a new file. Populated with the valid business information and hands it back to the application, Delivery Controller, reverse proxy, web application firewall or firewall for onward delivery.

5 The document is risk-free, fully revisable and in near real-time.





For more information and to understand more about web document uploads and threat removal services, read our solution brief.

 [Read the Solution Brief](#)

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, [Twitter](#), and [LinkedIn](#).

Forcepoint

forcepoint.com