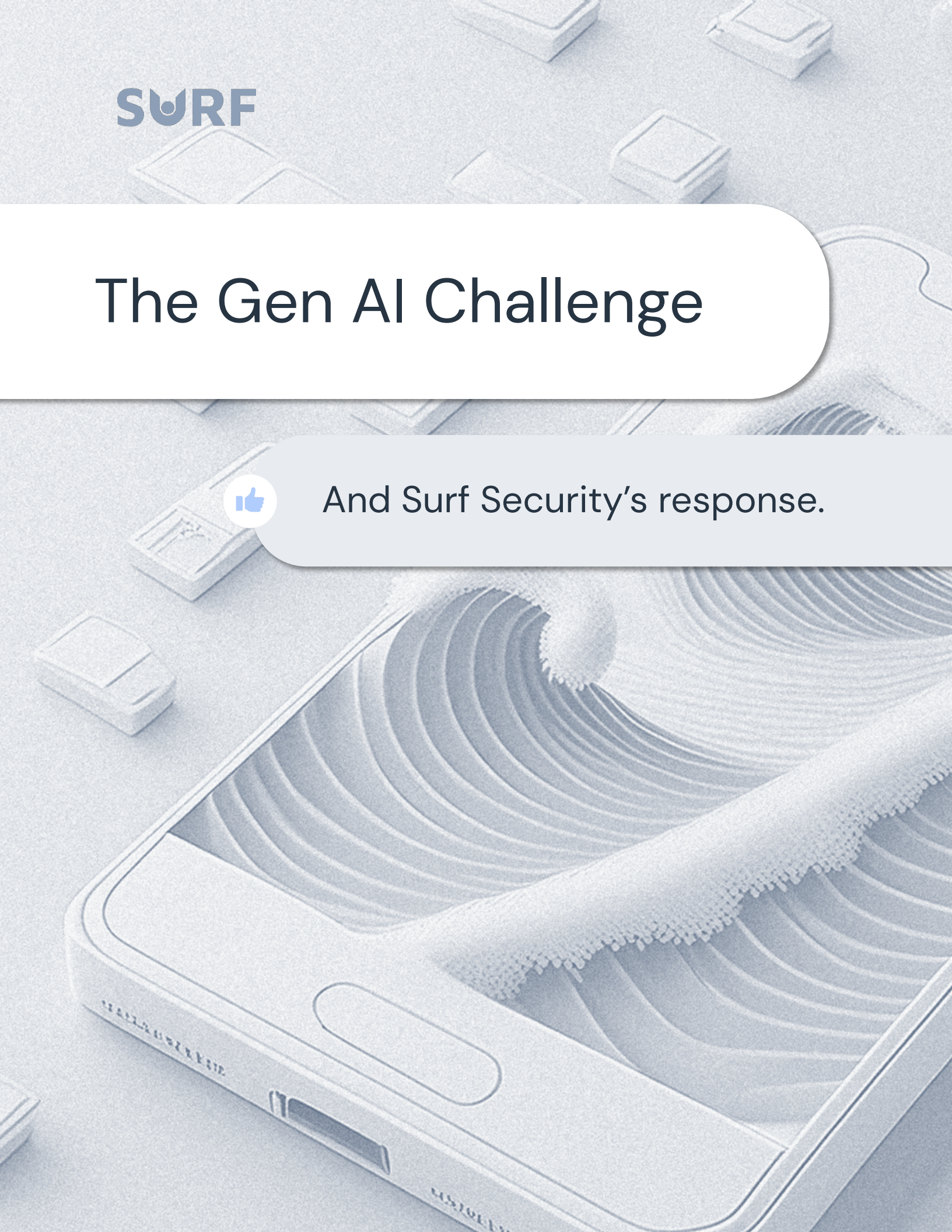
SURF

The Gen AI Challenge

And Surf Security's response.



Tackling GenAI security and privacy risk from inside the browser

IT and security leaders have quite a battle on their hands. By one estimate, there were over 3,200 publicly reported data breaches and leaks last year in the US – a new record, surpassing the previous all-time high by 72 percentage points. Yet while the majority of these incidents were the result of malicious third parties, over a fifth (22%) were down to insider error. The arrival of generative AI (GenAI) tools has amplified these risks.

Although tools like ChatGPT feature some security and privacy guardrails, many organisations are finding out the hard way that stricter policies and security controls are needed to mitigate this emerging insider risk. But few have considered a novel yet effective way of achieving this: powerful zero trust security delivered via an enterprise browser.

The GenAI challenge

Publicly available GenAI tools like ChatGPT are transforming roles as diverse as software development and customer service. Nearly half (46%) of Fortune 100 execs believe they risk falling behind if they don't adopt the technology as quickly as possible. But to optimise the business value of GenAI, IT and security leaders must first manage the new risks they create.

That means restricting who can use these tools, and limiting what information they enter as prompts. OpenAI states in its privacy policy that it might use such inputs to provide, analyse and improve its services, and to develop new programs and services. It might also share the information with third parties without any further notice. That's a huge privacy, security and compliance red flag.

Employees might unwittingly enter:

- Highly regulated customer/employee personally identifiable information (PII).
- Sensitive IP/trade secrets/corporate information.

In a worst-case scenario, such information may be surfaced in the AI model's responses to other users. Samsung found this out the hard way last year, after developers uploaded sensitive code to ChatGPT to help them with debugging. In a separate case, an employee at the tech giant shared meeting notes with the AI to convert them into a presentation.

Data leaks like this can cause financial and reputational damage. It could mean a regulatory fine (eg GDPR, CCPA) if PII is accidentally exposed. Or loss of competitive advantage, if sensitive internal information or IP is shared. That's why a growing number of organisations including Amazon, Verizon and JPMorgan are banning or restricting use of GenAI.

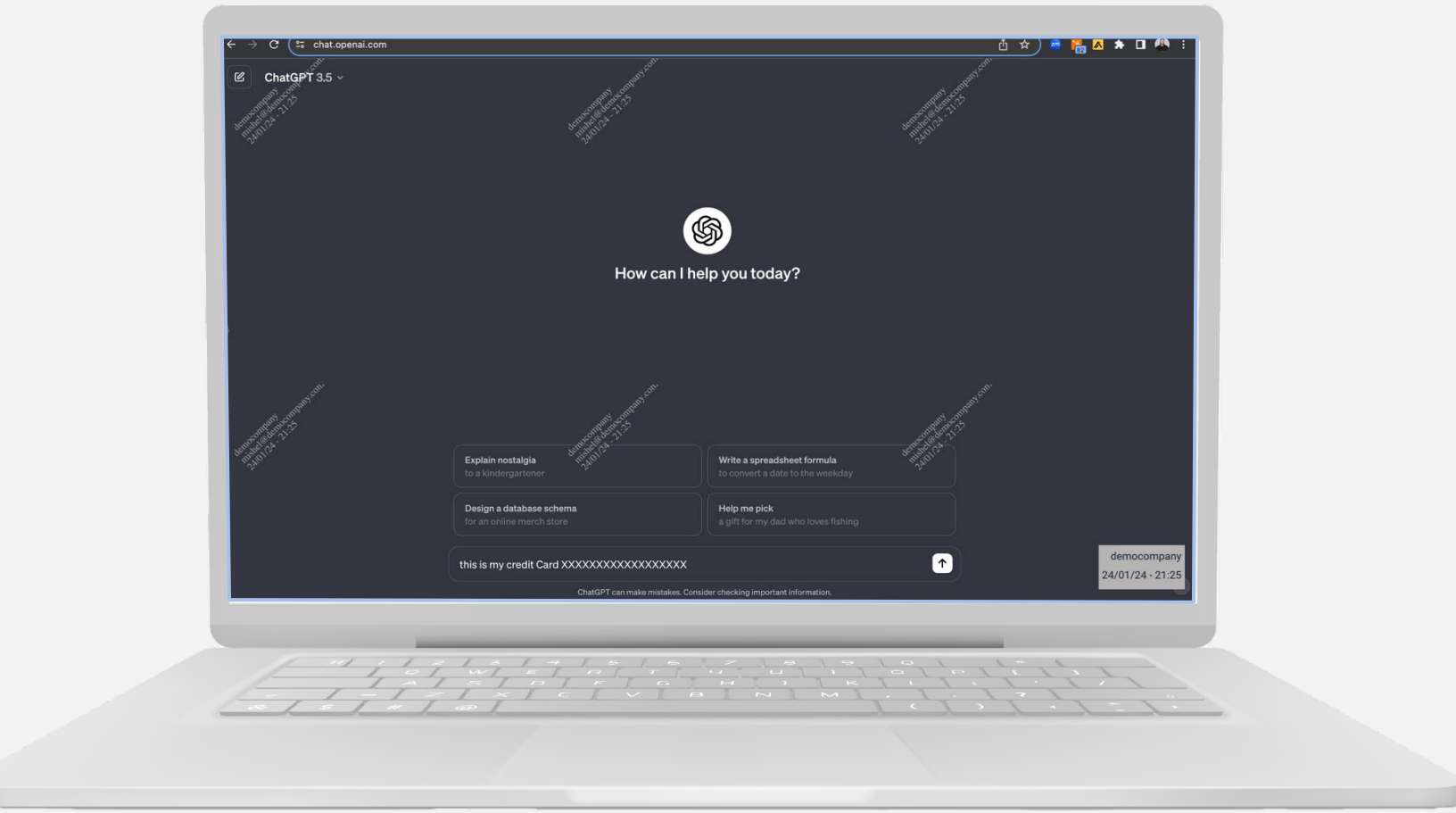
Browser-centric security

Enterprises wanting to follow suit might view the browser as an epicentre of privacy and security risk. In fact, rather than being part of the problem, it could be the solution. Imagine a zero trust browser that supports user authentication and device posture checks, and delivers a secure, isolated browsing experience with centralised policy management. That's the power of SURF's Enterprise Browser.

Alongside many other features,

it can help mitigate GenAI data leak risks by:

- Supporting identity and access management (IAM) policies, to limit who has access to GenAI tools.
- Masking sensitive PII and other information so it cannot be mistakenly entered into the GenAI.
- Supporting DLP policies to prevent cut-and-paste of sensitive enterprise information into the GenAI tool.
- Offering audit logs, session records and robust reporting to enhance insight for auditing and forensic analysis.



All of this is delivered from within the browser, so there's zero cloud infrastructure cost and zero performance impact.

Gartner predicts that by 2026, 25% of organisations will be using enterprise browsers – up from less than 10% today. ***Isn't it time for you to join them?***

Contact us

To find out how SURF can simplify security for your organization, please visit www.surf.security or email us on info@surf.security