PROTECTED HARBOR

Secure by Design and its Principles

“Secure by design” means making security a core focus during the entire development of a product—right from its initial concept. Instead of treating security as an addon or patch after launch, it’s embedded into every stage of design and development to identify and fix potential weaknesses early on.

The goal is to ensure consumers can trust that the technology they use is safe and resilient to threats from day one.

Secure by Design vs. Secure by Default

- **Secure by Design:** Products are built and tested from the ground up to reduce security flaws before reaching the market.
- **Secure by Default:** Products are configured to be secure right out of the box. Security settings like multifactor authentication and logging are enabled automatically, without the need for user intervention.

Why Is It Important?

With cyber threats on the rise, technology providers can no longer afford to wait for customers to find vulnerabilities after they’re using a product. Traditionally, customers were left to apply patches, monitor for issues, and pay extra to secure their systems. This reactive approach leaves users exposed to attacks, risking their finances, privacy, and even health.
By building security in from the beginning, manufacturers can avoid these risks, making their products safer from the start and reducing the chances of cyber incidents and data breaches.

- **Secure by Design Architecture**
- **Reduces the need for constant updates and patches.**
- **Protects critical systems, like healthcare and finance, from being compromised.**
- **Builds user trust by delivering secure products that are safe to use immediately.**

By adopting a “secure by design” mindset, technology companies can shift the responsibility from customers to manufacturers, making everyone safer.

3 Key Principles of Secure by Design

PRINCIPLE 1
TAKE OWNERSHIP OF CUSTOMER SECURITY OUTCOMES

Security shouldn’t be the customer’s problem. It’s up to software manufacturers to build security into their products from the start, ensuring they’re safe to use without extra steps.

PRINCIPLE 2
EMBRACE RADICAL TRANSPARENCY AND ACCOUNTABILITY

Manufacturers should openly share insights from product deployments and vulnerabilities. This helps others learn from past mistakes and successes, improving security industrywide.

PRINCIPLE 3
LEAD FROM THE TOP

Security needs to be a top priority, led by executives who integrate it into every stage of product development throughout the organization.

PROTECTED HARBOR

YOUR TRUSTED PARTNER IN CYBERSECURITY

+1 201-957-1616

protectedharbor.com

sales@protectedharbor.com