WHITE PAPER

Secure by Design: Building cybersecurity into the foundation

Why this philosophy matters and how it reduces your attack surface from the inside

SOPHOS

Executive summary

Secure by Design is a software development philosophy that treats security as a foundational requirement rather than an afterthought.

Instead of building a product first and bolting on security fixes later, Secure by Design demands that security considerations are embedded into every stage of the development lifecycle — from architecture and design through coding, testing, deployment, and maintenance.

The core idea is straightforward: If you build something securely from the ground up, your users are protected by default rather than only when they know how to configure the right settings or when security gaps are fixed after the fact.

In practical terms, this means adopting principles like least privilege (giving users and processes only the minimum access they need), secure defaults (shipping products with the safest configuration out of the box), defense in depth (layering multiple security controls so that no single failure is catastrophic), and eliminating entire classes of vulnerabilities through safer languages, frameworks, and design patterns.

The core idea is straightforward:

If you build something securely from the ground up, your users are protected by default rather than only when they know how to flip the right settings or when security gaps are fixed after the fact.

Why was the Secure by Design approach introduced?

For decades, many players in the technology industry operated under a “ship fast, patch later” model. One consequence of that legacy is that cybersecurity can be seen as just a cost center — something that slows releases and frustrates developers. The impacts are playing out in real time: constant vulnerability disclosures, rushed emergency patches, and breaches that drain billions from organizations while exposing the personal data of hundreds of millions of people.

The Ivanti Connect Secure vulnerabilities, the Log4Shell exploit in a ubiquitous open-source library, and the MOVEit Transfer vulnerabilities all demonstrated that reactive security simply cannot keep pace with determined adversaries.

Recognizing this imbalance, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), together with international partners, published formal Secure by Design guidance in 2023, urging technology manufacturers to take ownership of their customers' security outcomes.

Secure by Design principles state that the burden of security should rest on the vendors who build the products, not on the end users who deploy them. This changed the way vendors talked about the security of technology products, moving the conversation from individual responsibility ("users should patch promptly") to manufacturer accountability ("vendors should ship products that are secure from day one").

Why Secure by Design matters most for cybersecurity solutions

It's a striking reminder that even security tools can sometimes become the entry point for an attack. Yet it happens with alarming regularity.

This highlights a critical weakness for many organizations: Once a perimeter device is exposed, attackers will keep coming back to it repeatedly until it is fully secured. Firewalls and other edge systems can remain vulnerable even after a fix is available. Across all confirmed exploited vulnerabilities in recent analysis of incidents Sophos remediated, the median time between a vendor publishing an advisory or patch and an attacker exploiting that flaw was 322 days — almost a full year of opportunity for adversaries. Cybersecurity vendors can't assume users are going to patch immediately.

The privileged position problem

Cybersecurity tools occupy the most sensitive corners of an organization's infrastructure. Endpoint detection agents run with kernel-level access. SIEM platforms ingest logs from every system. Identity providers hold the keys to every account. Firewalls sit at the boundary between trusted and untrusted networks.

When security products sit at the heart of an organization's defenses, they carry a heightened responsibility to follow Secure by Design principles. Vendors in our industry play a critical role in protecting customers, and that trust comes with expectations around how products are engineered.

This privileged position means that a vulnerability in a security product doesn't just expose itself, it exposes everything it was designed to protect. An attacker who compromises an endpoint detection and response (EDR) agent doesn't just own one tool — they own the endpoint with the highest privileges. A flaw in a VPN appliance doesn't just break remote access, it hands an adversary a direct tunnel past every perimeter control.

What happens when Secure by Design is ignored?

The consequences of neglecting Secure by Design principles are well-documented and, if not followed properly, leave businesses, users, and the internet as a whole, less safe.

- **Escalating breach costs.** When vulnerabilities are discovered post-release, fixing them is exponentially more expensive than addressing them during development.

- **Erosion of trust.** Customers, regulators, and partners lose confidence in organizations that suffer repeated security incidents. Reputation damage can outlast the technical remediation by years.

- **Regulatory and legal exposure.** Governments worldwide are tightening cybersecurity regulations. The European Union's Cyber Resilience Act, for example, will impose mandatory security requirements on products with digital elements sold in Europe. Organizations that ignore Secure by Design principles risk non-compliance, fines, and market exclusion.

- **National security risks.** Critical infrastructure, such as power grids, water treatment plants, and healthcare systems, increasingly relies on internet-connected devices and systems. Insecure-by-default products in these environments create openings for state-sponsored adversaries and ransomware operators, with potential consequences that could upend a someone's everyday life.

- **Perpetual patch fatigue.** Without secure foundations, organizations are trapped in a reactive loop: scanning for vulnerabilities, prioritizing patches, testing updates, and deploying fixes — repeatedly. This drains resources that could be spent on deeper cybersecurity investigations.

How to choose a Secure by Design firewall

When evaluating your next firewall, ensuring it is truly Secure by Design should be a top priority. However, it can be difficult to cut through vendor marketing to understand what capabilities a solution actually delivers. The following criteria will help you identify the key characteristics to look for when selecting a firewall built on genuine Secure by Design principles:

1. Hardened architecture

As we've seen, it's critically important that the architecture of the firewall is designed from the code to the core to be Secure by Design. But of course, it's very difficult to know what a specific firewall vendor has done to harden their product. Most vendors will claim their products are secure, but ultimately, their recent track record will reveal the actual truth.

Here are some obvious items to check for:

- Multi-factor authentication (MFA) support across all areas of the firewall (admin, VPN, portals).
- Integrated support for Zero-Trust Network Access (ZTNA) so you can eliminate the need for remote access VPN.
- Secure remote management that does NOT require SSH or remote login to the device from the Internet.
- Hardened and containerized user portals if they're exposed to the internet.
- Recent updates in their release notes that indicate they are addressing Secure by Design principles.

2. Automatic vulnerability patching with no downtime

One of the biggest attack vectors against network infrastructure is unpatched vulnerabilities. Once a vulnerability is discovered, it can be weeks before it's actually patched. Many users suffer from patch fatigue as you're constantly forced to apply new patches and accept the associated downtime on a regular basis.

Make your life easier and ensure your system is patched quickly by working with a vendor that offers automatic over-the-air updates that don't require downtime. Don't fall for marketing of so-called "automatic updates" — verify what they mean by that. If an update still requires a reboot and downtime, that's not "automatic."

3. Automatic auditing of configuration risk

Another common contributor to a security incident is firewall misconfiguration. Unfortunately, most firewalls won't tell you they are misconfigured, leaving a potential opening that could be exploited. Demand that your next firewall automatically and continuously audits important configurations and highlights high-risk settings so you can address them easily.

4. Proactive monitoring by the vendor

When most firewalls come under attack, you'll likely never know until it's too late. Fortunately, that's not the case with every firewall. Select a firewall vendor that monitors its own products remotely, gathering telemetry to detect signs of compromise early in an attack. Vendors should be willing and able to act quickly if abnormal activity is detected by quickly contacting you or your cybersecurity partner to help identify and remediate the attack.

5. A vendor committed to Secure by Design

This should go without saying, but if you've got this far, you've probably already got a vendor in mind that is clearly committed to Secure by Design principles. But don't just take their word for it. Dig into their recent history, progress reports, and their release notes to understand exactly how committed they are to your security.

Sophos' commitment to Secure by Design

On May 8, 2024, Sophos became one of the first organizations to commit to U.S. Cybersecurity and Infrastructure Security Agency (CISA) Secure by Design initiative, which focuses on seven core pillars of technology and product security:

1. Multi-factor authentication.
2. Default passwords.
3. Reducing entire classes of vulnerability.
4. Security patches.
5. Vulnerability disclosure policy.
6. CVEs.
7. Evidence of intrusions.

Aligned with our core organizational values around transparency, Secure by Design has been a guiding force as we continually evaluate and improve our security practices.

We published our pledges for improvement and publicly share the progress we are making against the seven core pillars of the Secure by Design framework. Of course, cybersecurity is constantly evolving and the job is never "done." Continuing to refine and enhance the application of Secure by Design principles across our portfolio is an ongoing, and central, part of our ethos.

Sophos is unique in offering several important Secure by Design features that significantly improve Sophos Firewall's security posture, while also making your life much easier. Sophos Firewall is the only firewall on the market that offers truly automatic, over-the-air security patches that require zero downtime. We are also the only vendor that is actively monitoring our entire install base of customer firewalls for any signs of an attack to enable us to respond quickly to help you and your cybersecurity partner remediate it — and immediately ensure all other customers are protected from similar attacks.

Takeaways

Aligned with our core organizational values around transparency, Secure by Design has been a guiding force as we continually evaluate and improve our security practices.

The latest version (v22) of Sophos Firewall further extends its Secure by Design capabilities, significantly bolstering the firewall's security posture.
These capabilities include:

- A new Heath Check feature to reduce the risk of a misconfiguration leading to a potential attack.
- An all-new control plane re-architected for maximum security and scalability that eliminates a whole class of vulnerabilities.
- The addition of a Sophos XDR Linux Sensor that enhances the real-time monitoring of our entire customer base's system integrity by our own security teams, enabling them to identify and respond to attacks more quickly.
- Firmware updates that are now encrypted and certificate pinned for authenticity.
- An upgrade to the latest Sophos anti-malware engine with enhanced zero-day, real-time detection of emerging threats.

Our work in the Pacific Rim campaign gave us a front-row view into how determined, well-resourced threat actors operate — and what it really takes to defend against them. The campaign reinforced that adversaries aren't waiting for weaknesses to appear; they're actively hunting for design shortcuts, configuration gaps, and unpatched systems across global infrastructure.
That experience directly shaped our Secure by Design approach.

It underlined that modern defenses must start with reducing the attack surface at the product level, building in strong defaults, tightening authentication paths, and eliminating opportunities for misuse long before a vulnerability ever makes it into the wild.

The path forward

Secure by Design does not eliminate all vulnerabilities, nor does it absolve organizations from ongoing vigilance. But it has become a fundamental foundation to cybersecurity for reducing the attack surface. The question is no longer whether Secure by Design is a good idea. It is how quickly it is adopted.

SOPHOS

Ready to assess your cybersecurity program?

Speak to a Sophos expert today.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com