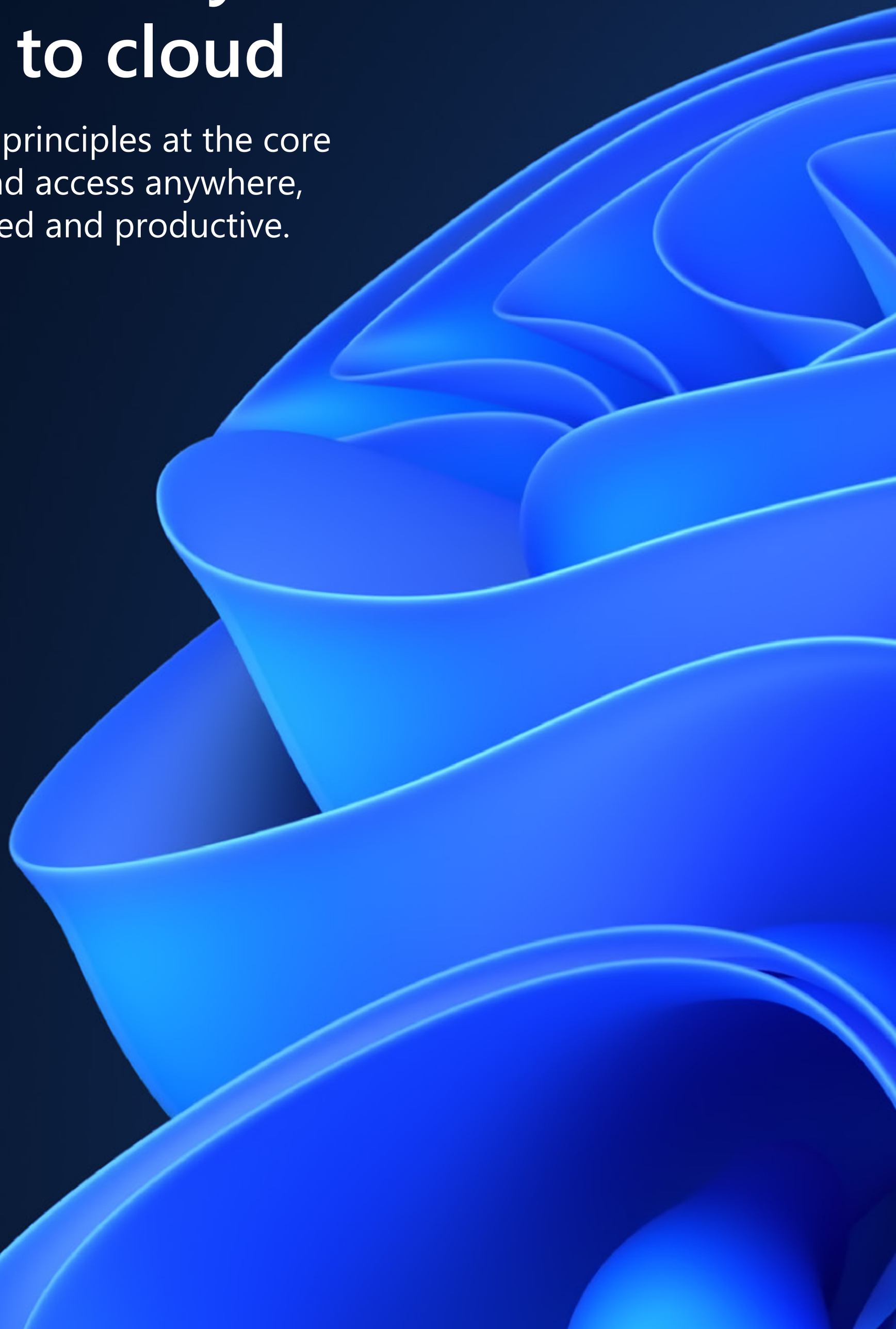
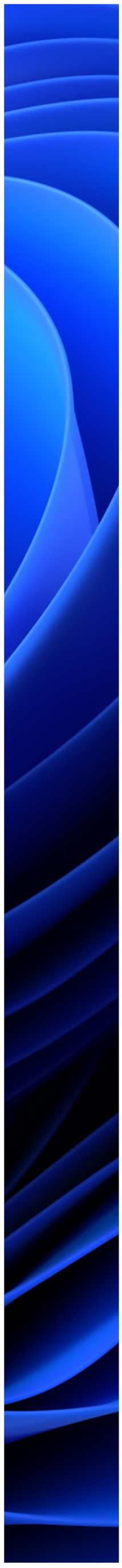
Windows 11 Security Book: Powerful security from chip to cloud

Built with Zero Trust principles at the core to safeguard data and access anywhere, keeping you protected and productive.



Windows

Table of contents



Introduction

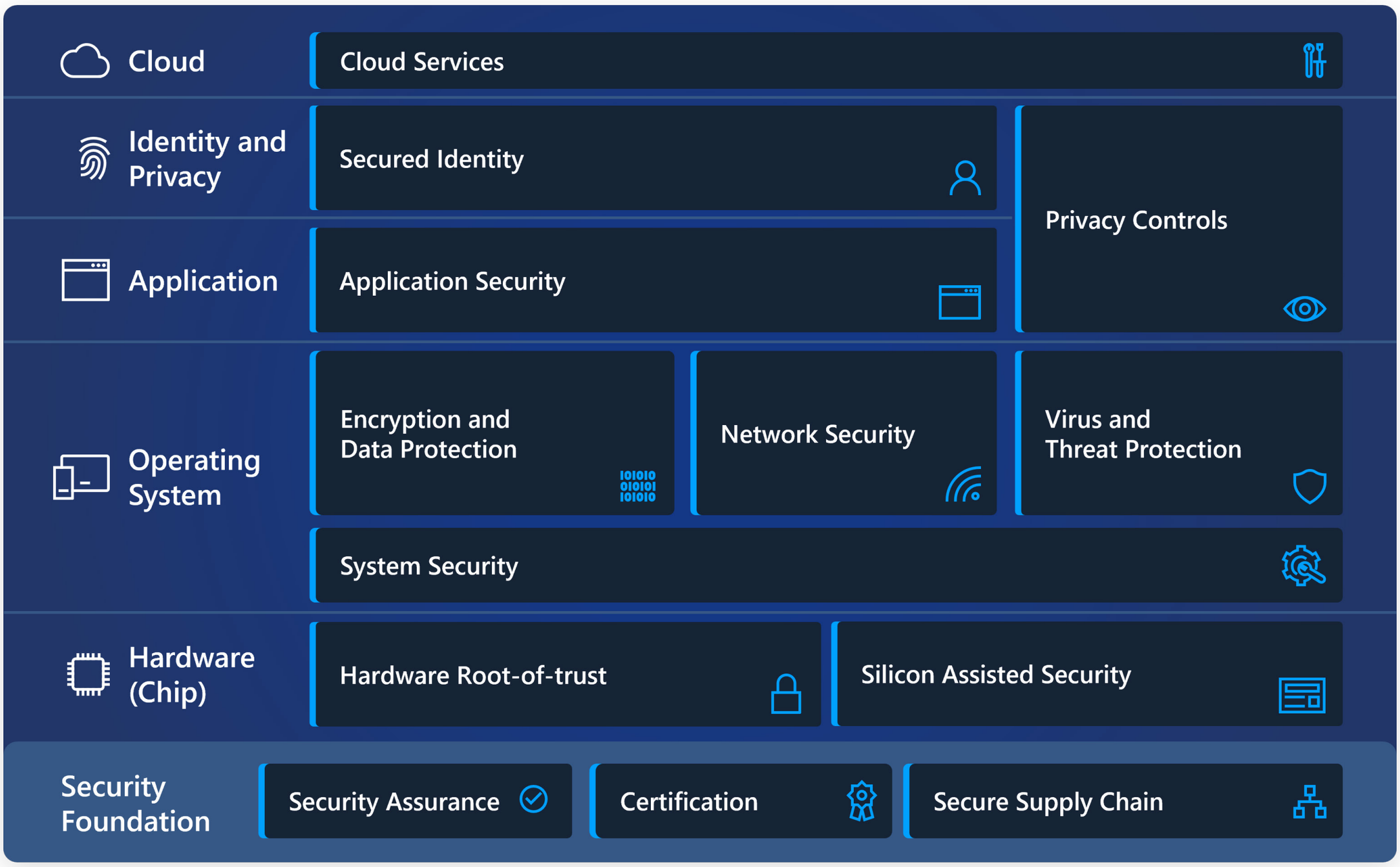
The acceleration of digital transformation and the expansion of both remote and hybrid workplaces brings new opportunities to organizations, communities, and individuals. Our work styles have transformed. And now more than ever, employees need simple, intuitive user experiences to collaborate and stay productive, wherever work happens. But the expansion of access and ability to work anywhere has also introduced new threats and risks. According to the new data from the Microsoft commissioned Security Signals report, 75% of security decision-makers at the vice-president level and above feel that the move to hybrid work leaves their organization more vulnerable to security threats.

At Microsoft, we work hard to **empower every person and every organization on the planet to achieve more**. We're committed to helping customers get secure—and stay secure. With over $1 billion invested in security each year, more than 3,500 dedicated security professionals, and some 1.3 billion Windows 10 devices used around the world, we have deep insight into the threats our customers face.

Our customers need modern security solutions that deliver end-to-end protection anywhere. Windows 11 is a build with Zero Trust principles for the new era of hybrid work. Zero Trust is a security model based on the premise that no user or device anywhere can have access until safety and integrity is proven. **Windows 11 raises the security baselines with new requirements built into both hardware and software for advanced protection from chip to cloud**. With Windows 11, our customers can enable hybrid productivity and new experiences without compromising security.

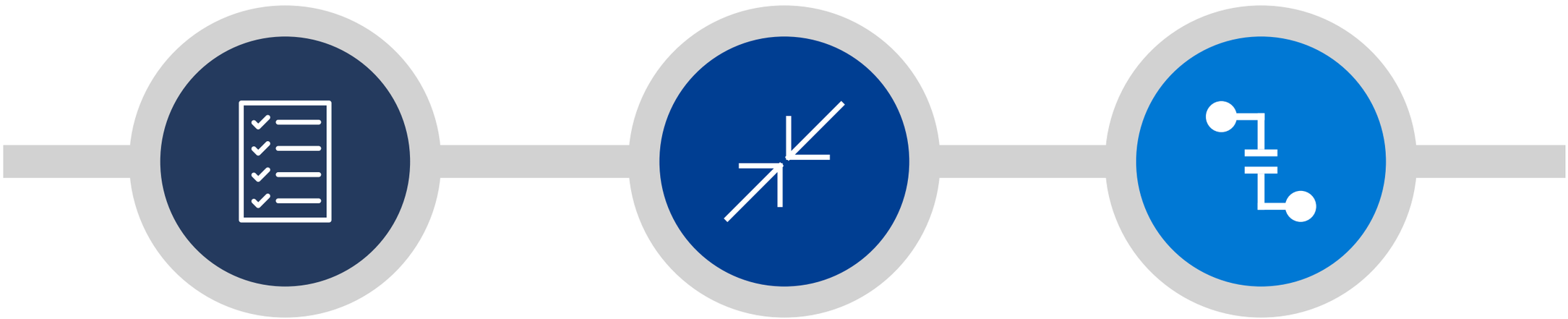
Approximately 80% of security decision makers say that software alone is not enough protection from emerging threats.[1]

In Windows 11, hardware and software work together for protection from the CPU all the way to the cloud. See the layers of protection in this simple diagram and get a brief overview of our security priorities below.



How Windows 11 enables Zero Trust protection

The Zero Trust principles are threefold. First, verify explicitly. That means always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies. The second uses least-privileged access, which limits user access with just-in-time and just-enough-access, risk-based adaptive polices, and data protection to help secure both data and productivity. And lastly, assume breach. Assume breach operates in a manner that minimizes blast radius and segments access. Verify end-to-end encryption and use analytics to gain visibility to improve threat detection and defenses.



Verify explicitly

Use least privileged access

Assume breach

For Windows 11, the Zero Trust principle of verify explicitly applies to the risks introduced by both devices and users. Windows 11 provides chip-to-cloud security, giving IT administrators the attestation and measurements to determine whether a device meets requirements and can be trusted. And Windows 11 works out of the box with Microsoft Intune and Azure Active Directory, so access decisions and enforcement are seamless. Plus, IT Administrators can easily customize Windows 11 to meet specific user and policy requirements for access, privacy, compliance, and more.

Individual users also benefit from powerful safeguards including new standards for hardware-based security and passwordless protection. Now, all users can replace potentially risky passwords by providing secure proof of identity with the Microsoft Authenticator app, signing in with face or fingerprint,[2] a security key, or a verification code sent to a phone or email.