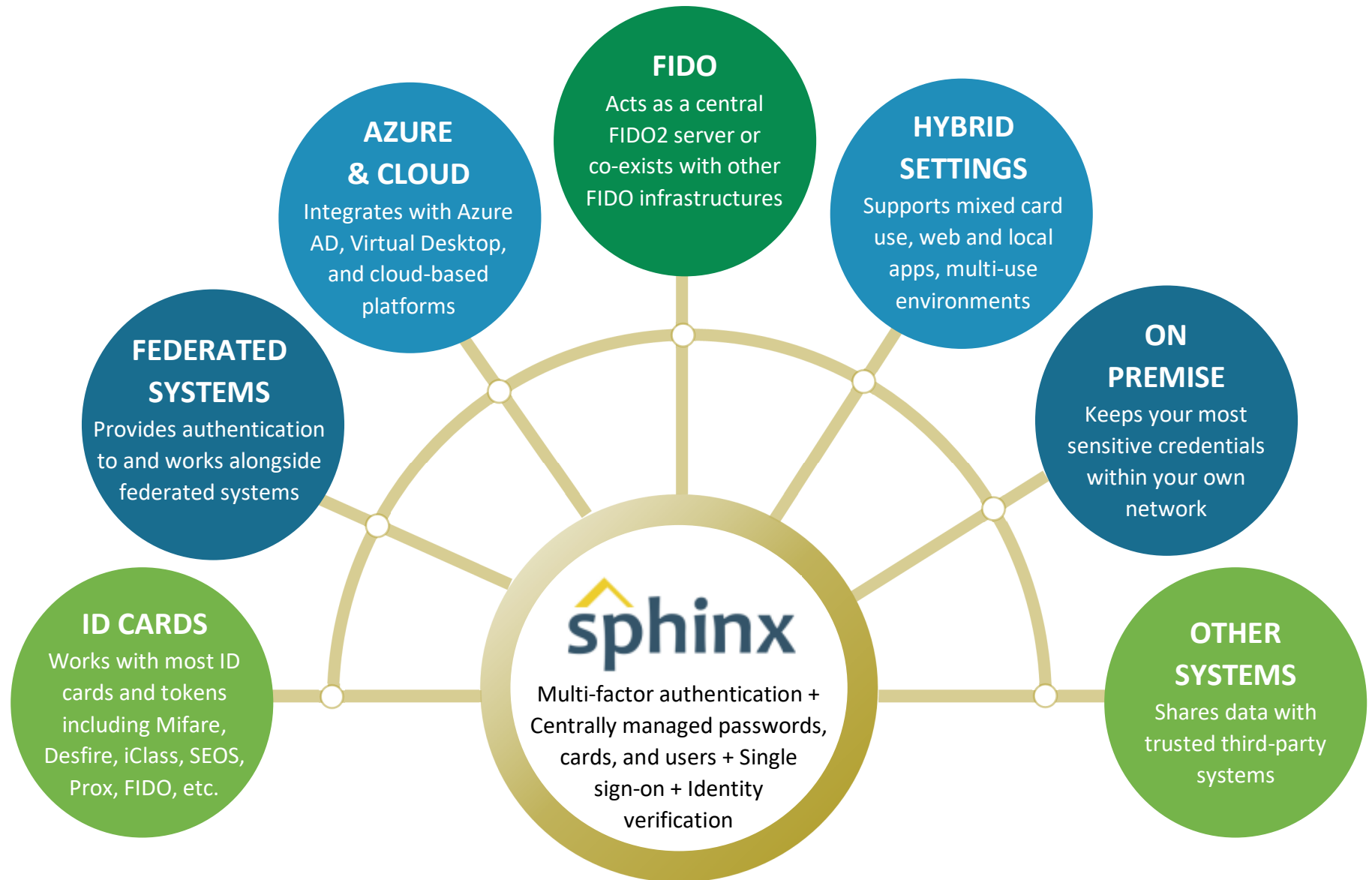


SPHINX LOGON

A CENTRAL HUB THAT WORKS WITH ALL YOUR AUTHENTICATION NEEDS



SPHINX LOGON

A CENTRAL HUB THAT WORKS WITH ALL YOUR AUTHENTICATION NEEDS

ID CARDS

You can start with Prox cards, move some users to Desfire cards down the road, then decide to add FIDO tokens for certain logons. Sphinx seamlessly handles all of the card technologies at once, and users can even have multiple tokens if desired.

FEDERATED SYSTEMS

Once a user is authenticated, a federated system can provide access to any number of shared access points and information without the need for further authentication. This provides great convenience for users, but also requires that users' identities are securely authenticated at the primary point of access. The Sphinx server can be used to provide this verification.

AZURE & CLOUD

Many organizations use Azure/Office 365, cloud applications, and Virtual Desktop to get access to data from any location. Also here, the primary authentication point is critical, since one logon can often provide access to a plethora of privileged information.

FIDO

FIDO is a big authentication buzzword at the moment. But it's important to note that FIDO was conceived as a user-managed credential. For enterprise to optimally incorporate FIDO cards and tokens IT admins need a place to centrally manage them. Sphinx features an integrated FIDO server option, which enables admins to manage access to web applications protected by the FIDO token. With Sphinx, the same FIDO token can be used to auto-logon also to apps that are not FIDO enabled or part of a federated security system.

HYBRID SETTINGS

Sphinx is more valuable than ever in the hybrid environments of today, because it securely protects the "front door". One organization may use a mix of password logon, logon to federated systems, and logon to Office 365. The Sphinx IT admin can oversee and protect access to all of these various locations and portals from the Sphinx hub.

ON PREMISE

With so much data being stored in the cloud, many organizations still prioritize storing their most valuable "keys" on premise. This keeps your most sensitive data, such as passwords, within your own network, under your own control. Although Sphinx' secure server can be used both on premise and in the cloud, the great majority of Sphinx customers choose on premise storage.

OTHER SYSTEMS

Sphinx was built using open standards so it's easy to share data with other trusted applications through its server and client APIs. For example, Sphinx can deliver security events to SIEM (Secure Information Event Management) systems for real-time alert handling. User data can also easily be shared with other ID management systems, such as facility access systems, etc.