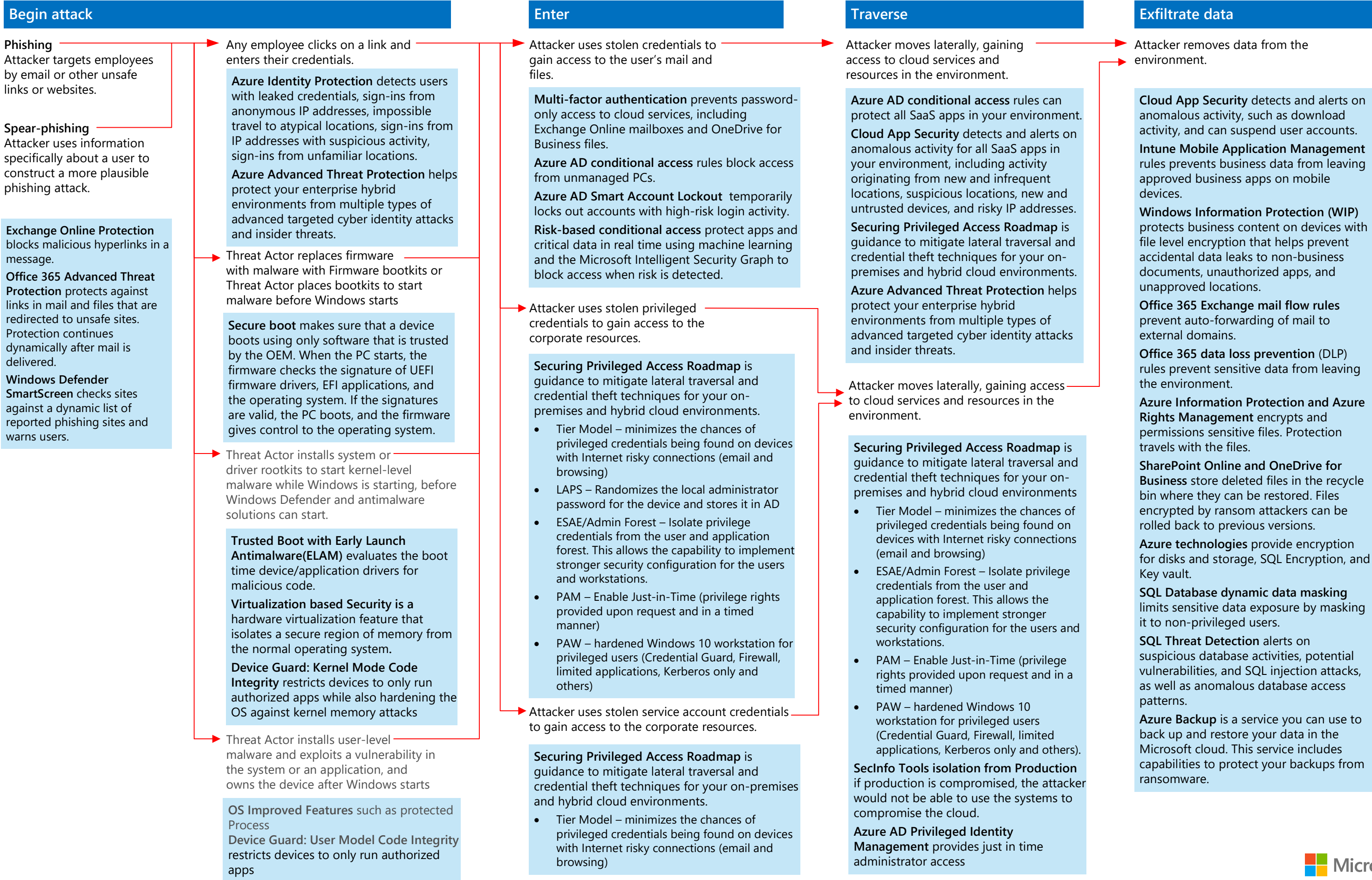
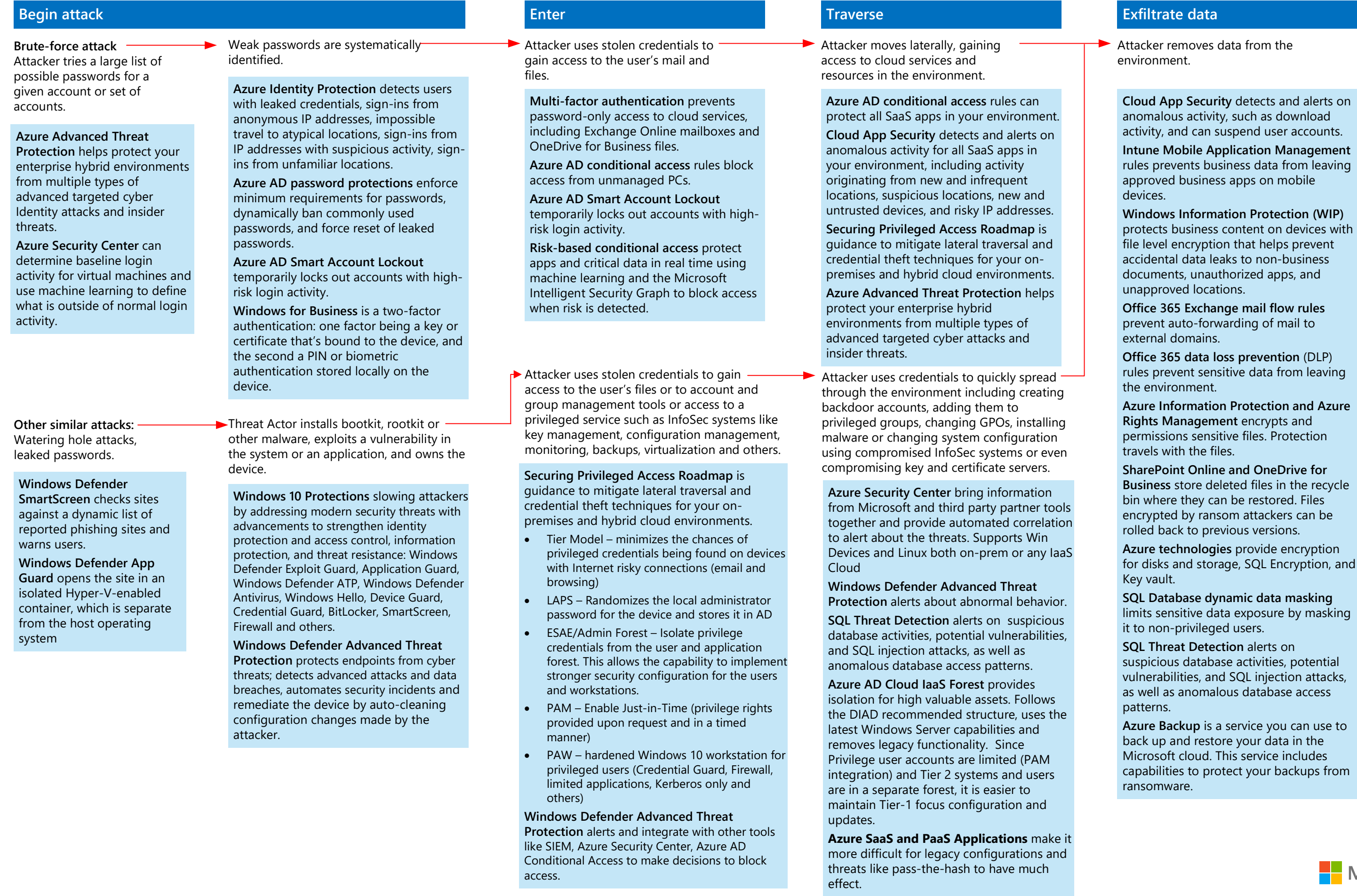


Common attacks and Microsoft capabilities that protect your organization



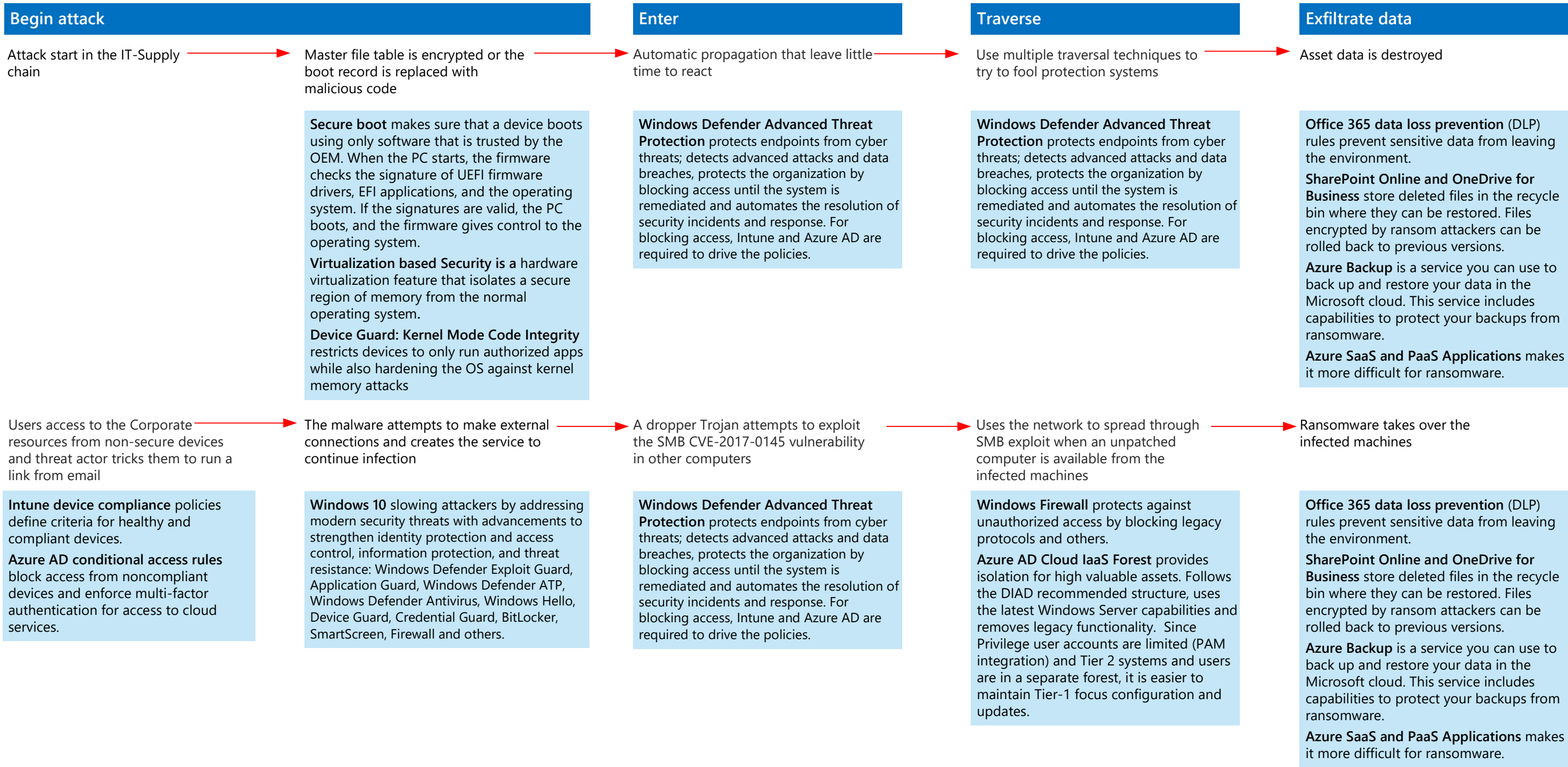
Common attacks and Microsoft capabilities that protect your organization



Common attacks and Microsoft capabilities that protect your organization



Common attacks and Microsoft capabilities that protect your organization



Begin attack

User uses an USB Device to copy data
or
User uses a cloud service to exfiltrate information
or
User uses wrong application to open or save documents at (IE: Partner app instead of Organization's)
or
Personal Device was enrolled into the organization's environment. After saving lots of data in the device, the user leaves the organization

Azure AD single identity for all cloud applications can help report and audit all user access.
Intune manages the device and apply Mobile Application Management (MAM) policies

Enter

Control of Data location is lost

Azure AD conditional access rules can protect all SaaS apps in your environment.
Cloud App Security detects and alerts on anomalous activity for all SaaS apps in your environment, including activity originating from new and infrequent locations, suspicious locations, new and untrusted devices, and risky IP addresses.

Exfiltrate data

Data gets published in the internet or sold to competitors

Windows Information Protection (WIP) protects business content on devices with file level encryption that helps prevent accidental data leaks to non-business documents, unauthorized apps, and unapproved locations.
Azure Information Protection and Azure Rights Management encrypts and permissions sensitive files. Protection travels with the files.