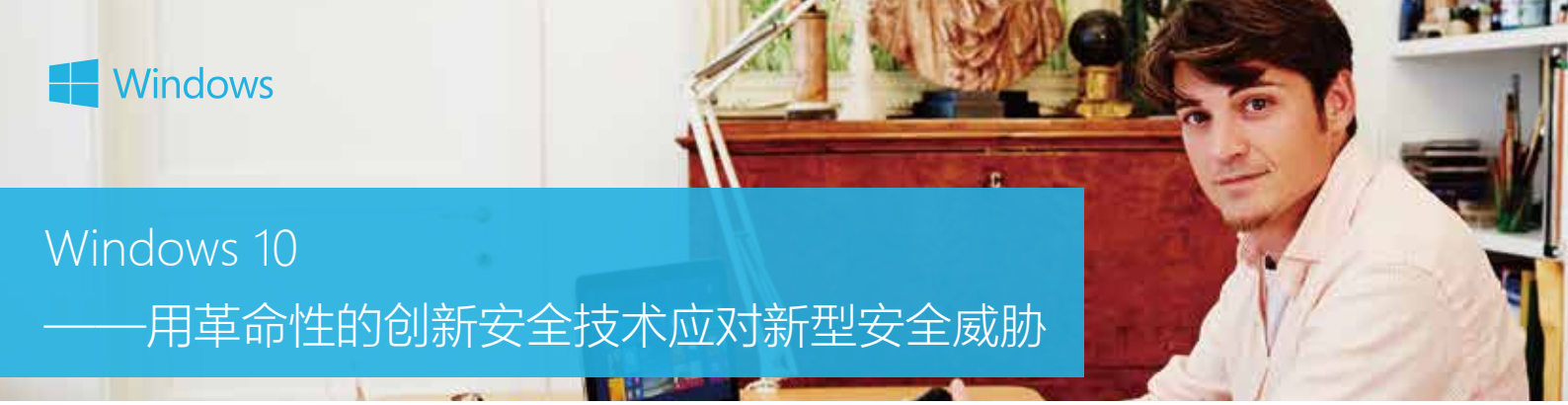

Windows

Windows 10
——用革命性的创新安全技术应对新型安全威胁

在这个云为先、移动为先的快速发展时代，安全成为新的热点。无论是个人还是企业用户，都面临网络安全的严峻挑战，迫切需要创新性的安全技术手段，保护用户避免蒙受损失或面对不可预估的风险。

微软悉心打造的最新一代Windows 10服务平台，为用户提供了性能优异，深度整合，高性价比，便于实施的安全保护体系，帮助用户应对新型的安全威胁。用户可以获得全方位的安全保障，包括便捷安全的新一代身份验证，从系统底层核心构建起来的可靠恶意软件抵御机制，个人隐私数据和企业敏感数据的分割保护模式等，为用户打造安全的系统生态平台。

	新时代的安全威胁	Windows 10的安全创新
Windows 10革新性的身份验证		
身份验证	• 基于传统的密码身份验证方式已经过时，一旦密码失窃，用户将面临身份被盗用，个人隐私被泄露等风险，而企业直接面临敏感数据外泄，IT环境受损和被恶意攻击的威胁。	**新一代身份验证（密码被盗也不用担心）**—— 革新的多因素身份验证，可使用生物识别验证(如指纹、虹膜、面部识别)，成本低且易于实施，极大提升验证安全性，防止身份信息被盗用。 **真正的单点登陆** —— 借助多因素身份验证，一次验证可以登陆多个业务系统或互联网应用，既安全又便捷。
Windows 10安全易用的数据保护		
数据保护	• 设备，磁盘丢失或者被盗，用户隐私数据或者企业商业数据将面临泄露风险。 • 个人自带设备在企业内网中混用，导致企业数据泄露的可能。 • 移动设备接入管理，敏感数据面临泄露的风险。	**数据加密** —— 更易于实现的磁盘加密技术，即使设备丢失或被盗也不会导致数据外泄。 **便捷的个人自带设备管理** —— 数据的分离与控制，能够随时远程管理个人自带设备上的企业数据，个人数据不受影响。降低企业敏感数据泄露风险。 **受信任访问** —— 移动设备或应用访问受策略限制，阻止未经授权的设备或应用访问业务数据。
Windows 10全方位抵御恶意软件		
威胁抵御	新的挑战 • 恶意软件——越来越复杂的网络攻击。	**安全可信启动** —— 结合UEFI和TPM，Windows 10启动建立在完整的可信链条上，保障系统引导的每一步都是安全的。 **虚拟安全模式** —— 将系统核心进程放入使用虚拟化技术保护的沙箱中运行，即便遭到攻击，系统依然稳若泰山。 **设备卫士** —— 只安装和运行经过认证和准许的应用程序，根本上杜绝了恶意软件被执行的风险，先验证再安装执行，最大限度的保障系统安全。 **应用防护** —— 基于云的开箱即用的恶意软件防护工具Windows Defender可以应对最新的安全威胁。 **自动安全更新** —— 全新的Windows update，自动推送安装更新，简便快捷。

基于TPM安全技术基础

激活TPM支持 的Windows 10设备= 安全 + 可控 + 可靠

安全： Windows 10给万物互联时代的用户带来了众多革命性新型安全特性，TPM（Trusted Platform Module可信平台模块）作为可信计算业界事实上的标准，为Windows 10安全性提供强有力的底层平台支撑，保证系统安全启动并运行，并向云端提供根信任。

可控： 在TPM标准中允许对其核心算法进行替换，满足各国商用密码必须国内自主研发的信息安全要求。

可靠： 微软公司长期致力于与中国政府和本土厂商在信息安全领域的密切交流和合作，并与国内主流的安全技术与设备供应商携手建立全球防御者联盟，面对全球网络安全的严峻挑战，共同保护最终客户。例如，由中国本土厂商国民技术股份有限公司自主设计并制造的商业化TPM安全芯片，已经获得国家商用密码管理办公室颁发的商用密码产品型号证书（编号为SXH2014022），这为国内客户提供了更多的选择。另外，银监会最新颁布的针对金融行业安全可控技术实施指导要求，也把TPM技术的应用列入准许范围。

Windows 10 身份管理的游戏规则改变者 | 最好的开箱即用的数据保护 | 最大程度保护关键设备，免受恶意软件攻击

安全可控，易于部署，易于实现，
*是时候换一个**现代操作系统**了*