防勒索?防钓鱼?如何应对企业远程办公安全新挑战

方案背景：

2020 年，一场疫情席卷全球，远程办公成为了工作的常态，在这样的场景下，如何在确保员工身份、设备及数据信息安全的前提下实现员工间的远程协作，成为企业的重中之重。

尤其，对于在中国的诸多外企而言，由于中国网络安全监管的特殊性，很多外企选择在中国采用独立 IT 基础架构及应用部署，在这样的复杂网络环境下，如何实现全球化办公的安全监管更是难上加难。

为此，针对当前复杂的全球化办公困境，诺未结合多年来服务外资企业的丰富经验，提出了集核心架构、桌面应用及安全策略三位于一体的综合解决方案。

针对当前全球移动化办公的现状，诺未高度关注企业的协作安全。任何的安全漏洞，都将对企业造成无法衡量的损失，因此诺未的解决方案以“安全”作为贯穿始终的核心价值，从底层架构到桌面应用的每一个环节都匹配有对应的安全策略，确保员工在世界的每一个角落都能进行安全的生产与协作。

客户案例：

以诺未服务的一家飞机配件设备制造公司为例，公司总部位于美国，在中国拥有多个分公司。由于公司战略及国家法律要求，客户决定从总部环境中拆分，在中国独立建立一整套 IT 基础架构及应用系统，并提出了他们的需求：

- 基于公网的用户验证和安全策略
- 统一的身份验证（Windows/ERP/O365 等）

- 基于公网的集中管理、有效管理电脑及办公移动设备
- 对企业重要文档加密和限制，防止核心数据泄露
- 信息安全（防钓鱼，防勒索等）
- 应用和数据的安全性

解决方案：

客户高度重视企业的协作与信息安全，正好与诺未的核心价值不谋而合， 经过对客户公司业务、组织架构、现有环境等多维度的评估，诺未最终为其匹配了适合该公司的集核心架构、桌面应用及安全策略三位于一体的综合解决方案。

核心架构

在架构层面，综合考虑客户的业务需求，我们通过员工身份验证，实现跨组织边界的系统和应用程序的单一登录访问。这样使员工的所有操作都基于身份安全的大前提下进行。

AD+ADFS	ERP	Security
• AD*2 • ADFS Proxy*2 • ADFS*2 • AD Connect*1	• IIS Web*1 • Application*1 • SQL PaaS*1	• PALO ALTO*2 • Jump server*1 • Azure Backup • Subnet, NSG

桌面应用

在桌面应用设计环节，除了匹配 Microsoft 365 软件进行协作以外，诺未还为客户增加了 EMS 套件，实现统一的身份与访问管理、移动设备管理、信息保护及威胁防护。

安全策略

在安全策略层面，诺未从账户安全、Microsoft 365 安全、云安全、数据安全、防勒索等多个维度部署安全基线，对客户信息进行的全方位防护。

账户与访问安全基线

账户与访问安全基线
• **所有用户登录所有应用都启用MFA** • 定期检查及审计管理员组 • 删除不需要的用户凭证（密码和访问密钥） • 启用按条件访问（例如只允许在公司内网访问） • 最小范围授权

- 启用 MFA(Multi-factor Authentication) 多重要素验证后，企业内所有员工要通过两种以上的认证机制之后，才能得到授权，使用电脑资源，进而确保员工的账户与访问安全

Microsoft 365 安全基线

Microsoft 365安全基线
• 使用本地AD账户同步及策略 • **使用ATP** • 使用强密码及过期策略 • 所有用户开启MFA二次身份验证 • 使用安全中心报告 • **Sharepoint/Onedrive文件存储及备份**

- 开启 ATP(Advanced Threat Protection)后，系统可以在员工协作办公的同时，自动检测并阻止未知威胁
- 打开 Sharepoint/ Onedrive 文件存储及备份，可以有效防止员工数据丢失，双重确保信息安全

云安全基线

云安全基线
• 采用云备份及状态邮件通知 • 定期测试备份的完整性以及是否可以恢复备份 • 通过内网或IP白名单控制访问Azure及资源 • 合理规划NSG/Vnet/网段 • 关闭服务器RDP/SSH外网登录 • **部署下一代防火墙** • **部署堡垒机** • **WAF** • 补丁管理 • 防毒软件 • 监控管理

- 通过部署下一代防火墙，从用户、应用、内容三个层面确保身份及信息安全
- 通过部署堡垒机，进行运维操作故障的追溯及回放，并满足企业的审计合规要求
- 通过开启 WAF(Web Application Firewall)网页应用防火墙严格数据泄密

数据安全基线

数据安全基线
• WEB SSL加密 • **服务器之间及数据库传输加密，SSL/TLS/VPN** • 磁盘加密（Bitlocker） • **数据备份（本地或异地）**

- 使用基于 SSL/TLS 的 HTTP 加密通信，确保服务器之间及数据库之间的数据安全

防勒索

防勒索	
• **防钓鱼培训** • **ATP** • **关闭RDP/SSH公网登录** • **补丁管理** • **异地备份**	▪ 采用机器学习进行 URL 分析，有效防止钓鱼攻击 ▪ 通过关闭 RDP(Remote Desktop Protocol) 远程桌面协议及 SSH(Secure Shell)安全外壳协议有效防止线上勒索

客户现状:

不仅如此，诺未的整套方案已在多家客户中落地使用，行业遍布零售、金融、教育等各行各业，帮助企业大大提升了在应对未知变化与挑战时的抵御能力，助力企业在动荡赢得先机，加快发展步伐。

目标客户:

诺未的这套综合解决方案同样适用于绝大多数具有高度安全协作需求的外资企业，不仅能满足企业员工在全球化移动办公时的安全，而且保障了员工与客户交互时的信息及数据安全。

关于诺未:

上海诺未网络科技有限公司（Nova Tech）成立于 2011 年，为客户提供基于微软云的解决方案与服务，是微软多年的金牌合作伙伴。

诺未始终坚持提供最优质的服务助力客户发展与变革。

我们愿意深入了解您的业务模式和工作流程来帮助您挑选和实施最佳的解决方案来应对商业挑战。

诺未以“解决客户的问题，为他们带来价值”为使命，为客户提供更优质的服务。目前服务于全球 500+企业，60000+客户。

NOVATECH