中国北方工业有限公司是我国兵器行业国际化经营主力军，是国家实施“一带一路”战略的重要团队。北方公司始终以服务国家国防安全、服务国民经济社会发展为使命，综合利用国际国内两个市场、两种资源，构建了遍布全球的海外经营网络，开创了防务产品、石油、矿产、国际工程和专业化民品、投资与资产经营协同发展的国际化经营格局，实现了从进出口贸易公司向贸易、产业和现代金融一体化运作大型跨国企业的转型。

案例名称:中国北方工业有限公司“零信任”网络安全架构体系建设项目

提供单位:中国北方工业有限公司

案例介绍:

为提升网络安全防护技术能力，有效应对网络安全风险，构建安全、稳定、快速的网络环境，北方公司结合自身实际情况，实施构建了“零信任”网络安全防护架构体系（以下简称零信任网络安全项目）。

项目基于零信任理念，实现先认证、后连接、再访问的核心原则，保证终端可信、流量可信、身份可信、应用隐藏，确保业务应用的安全访问，零信任网关通过拦截应用请求，并与数字身份管理平台进行身份核验、多因素认证，实现应用系统的认证接入和单点登录，同时，数字身份管理平台作为零信任网络安全防护架构的基础底座，为零信任安全网关、安全设备及业务应用提供系统账号的全生命周期管理和整个访问过程的认证鉴权和访问控制。

系统从身份能力构建入手，逐步构建北方公司零信任架构所需要的功能，主要包括：

1.实现对应用的有效防护。通过SPA单包授权技术、双向加密通信机制、反向代理技术，接入北方公司网络即可访问应用主机的现状，根据需要定义网络隔离策略，杜绝木马和各类攻击行为对应用主机造成的影响。

2.构建身份校验与认证机制。通过SDP控制器可编排的能力，实现北方公司用户、设备的接入安全，对其进行身份验证和授权，解决传统网络隔离模式下网络身份认证与应用身份认证分离的问题，拒绝非受保护应用流量可自由进入北方公司数据中心网络。

3.建立持续安全防护机制：通过联动风险引擎，监测、预测各类安全活动事件，对用户行为开展风险检测与评估，构建访问身份的持续认证、动态授权机制，建立设备信任、用户信任、流量信任、应用信任的信任链机制。

4.建立统一的用户身份管理体系，实现用户的全生命周期自动化管理：构建集中的包含内外部用户的平台，通过该平台实现全公司的机构、人员管理，同时实现以主数据、人力资源数据为新统一身份认证的数据来源，将会对用户名下的应用系统账号信息进行相应的联动，实现用户、组织机构、账号的全生命周期管理。同时提供平台分级管理服务，实现北方公司身份管理体系用户、组织机构、账号数据分级分权的管理模式。提供数据同步服务，获取数据源头数据，按照各应用系统规则与同步策略，提供数据和属性到各业务系统。

5.提供统一用户访问门户，根据用户权限展示用户有权限的应用系统列表，实现用户方便快捷的访问应用。提供员工自助自服务能力，实现修改密码、重置密码等自助服务。

6.建立统一的应用访问入口，：依托数字身份管理平台，对公司关键业务或用户使用范围较广的应用进行应用系统集成，实现用户方便快捷的应用访问，提供统一的应用访问入口，支持不同强度、不同因素的认证方式，实现用户登录验证过程中身份认证管理系统校验，做到一次认证，单点安全登录到有权访问的各类应用系统。

7.建立多安全级别的融合认证平台，实现用户访问应用的安全保障：实现统一认证与访问控制模块，实现扫码认证、短信认证、密码认证等多种认证相结合的认证方式，并实现各类不同认证方式的单点登录服务，为各类业务应用提供统一认证界面与服务，在提高认证安全性的同时，提升最终用户登录系统的便利性。

8.建立完善的审计体系，实现以用户为基点的应用访问审计：提供对用户的应用访问权限进行集中管理，并对用户的认证及用户应用访问进行记录和审计，通过集中收集、存储和管理用户在业务系统中活动的审计信息，对身份、权限、资源的集中审计和分析，并形成审计报表、视图，实现系统资源访问安全预测和预警能力，并结合身份、权限管理规范，实现实时合规性分析。

北方工业
NORINCO