SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

新一代远程办公安全方案

让IT更简单，更安全，更有价值

Make IT Simpler, More Secure and Valuable

突如其来的疫情打破了全球宁静

负面影响

· 受疫情影响，春节假期延长、人员流动受限、各地延迟复工，疫情对我国经济的短期冲击不可避免。

· 受此次疫情影响严重的市场主体正面临较大生存压力，尤其是中小型制造业、服务业企业，值得重点关注。

积极因素

· 疫情结束后疫病防控体系的完善和改革以及相关产业的发展，也将成为疫情过后重要的经济增长点。

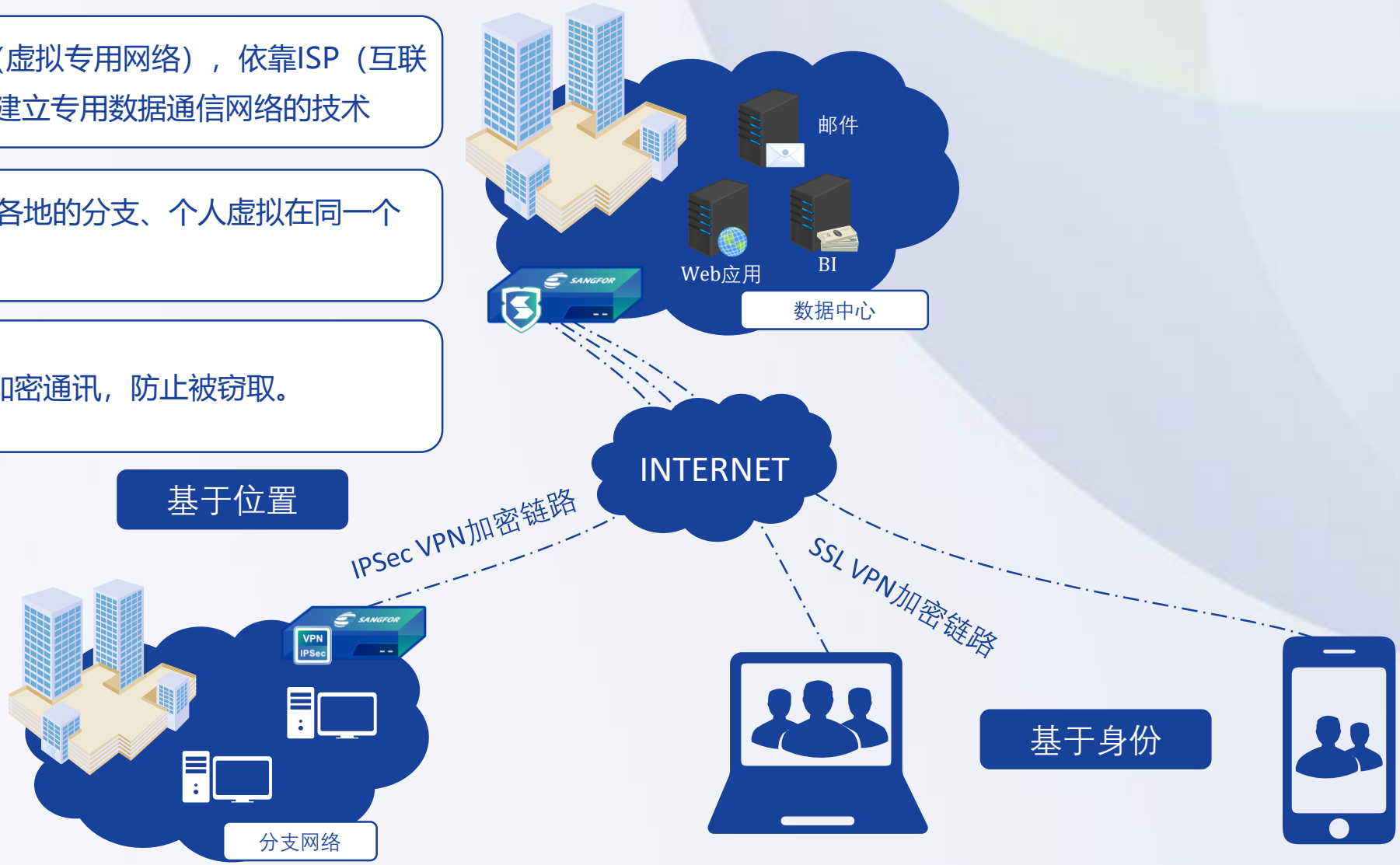
· 在疫情影响下，电子商务、电子政务、居家办公、虚拟会务/商务、线上教学等新业态和新模式将迎来新一轮快速发展。

传统远程接入解决方案——VPN

VPN： Virtual Private Network（虚拟专用网络），依靠ISP（互联网服务提供商）提供的公网线路，建立专用数据通信网络的技术

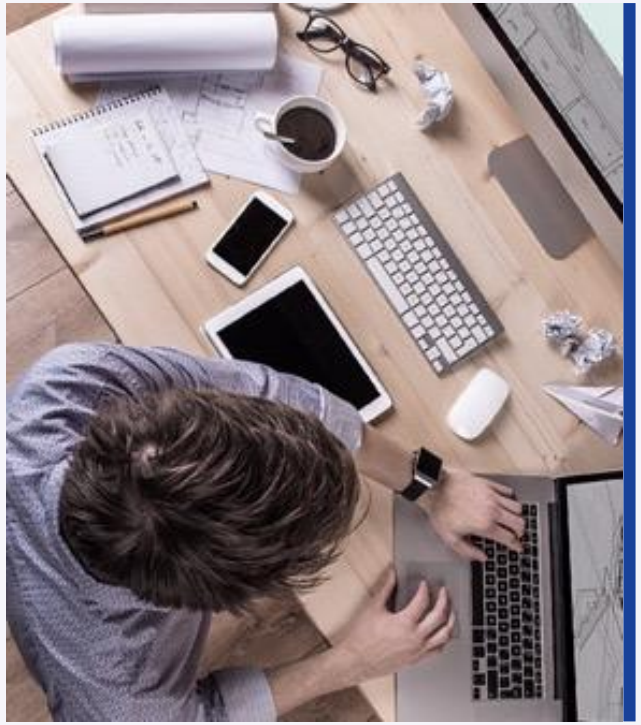
VPN可以通过远程连接，把分散在各地的分支、个人虚拟在同一个局域网环境

在Internet上建立专用网络，进行加密通讯，防止被窃取。



面临的问题——规模化远程办公需求升级

远程办公规模化常态化带来新的挑战



使用角色发生变化

从运维人员、部分高管变成各业务人员、各级主管、职能人员、开发人员、第三方供应商等；

接入终端复杂度增加

业务接入的终端从内网的PC、统采的PC 变成了各类BYOD个人终端，安全隐患大幅增加

使用的环境发生变化

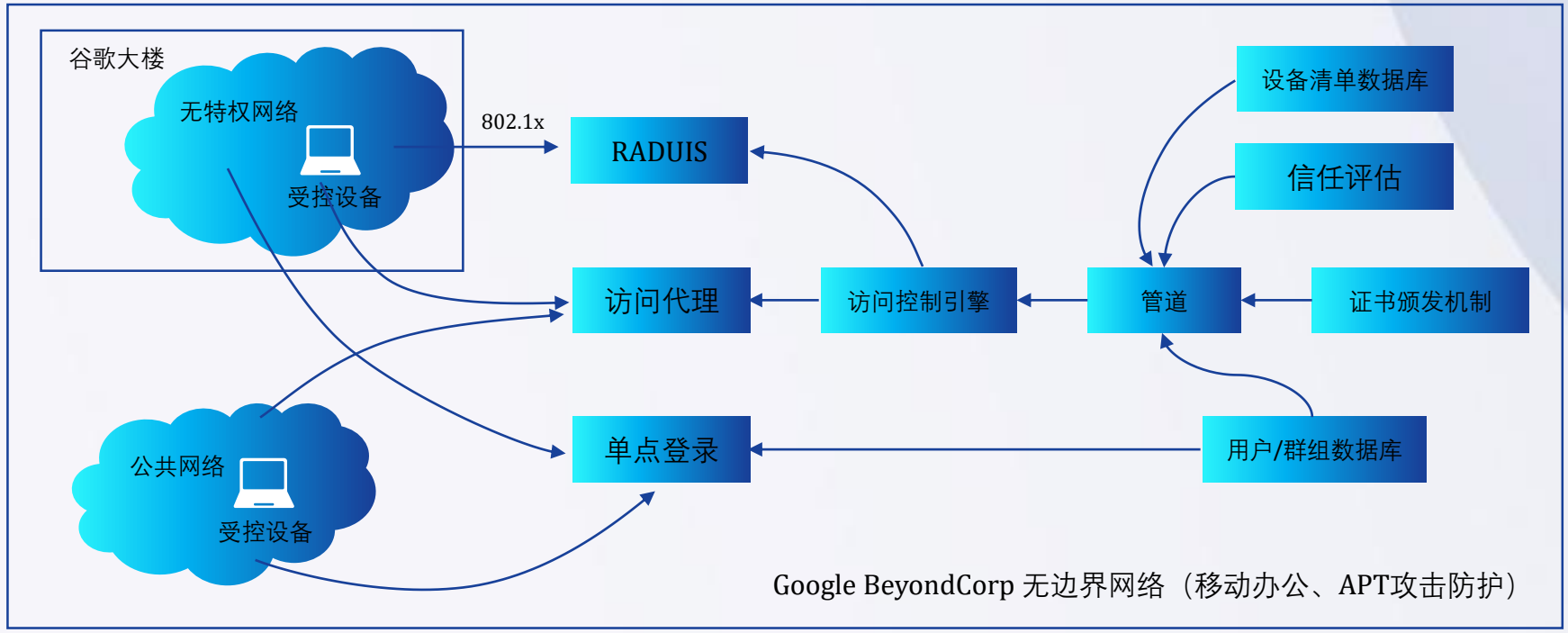
办公大楼、办事处、居家、出差途中、机场咖啡厅等场所，环境复杂，边界模糊。

使用场景发生变化

从远程运维、流程审批拓展到远程办公、远程开发、远程协同、居家坐席等

未来新趋势从零信任VPN开始

零信任安全架构热潮



著名研究机构Gartner预测：

- 到2022年，向合作伙伴开放的80%业务应用程序将通过零信任网络访问（ZTNA）进行访问。
- 到2023年，60%的企业将逐步淘汰大部分远程访问虚拟专用网（VPN），取而代之的是ZTNA。
- 到2023年，40%的企业将会把零信任网络访问（ZTNA）应用到其他场景。

全面身份化　多源信任评估　威胁阻断

可信访问

零信任发展史

零信任安全架构在2010年被提出（著名研究机构Forrester首席分析师 约翰.金德维），在2011年Google开始启动BeyondCorp零信任项目，在2014年Google发表了5篇BeyondCorp零信任安全架构相关的论文，在2017年Google BeyondCorp零信任项目完整实施落地，同年各大厂商（思科、微软、亚马逊）开始投入零信任安全架构产品的研发。

零信任概念

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

零信任是什么？

- 一个全新的安全架构理念
- 一种全新的安全建设方法论
- 一套全新的安全建设指导思路

SDP、IAM、微分段/微隔离

是零信任的三种技术实现方案（其中SDP和IAM用于保护『用户到业务』的访问安全，微分段/微隔离用于保护『业务到业务』的访问安全）

ZERO TRUST

零信任能解决哪些问题？

- 以网络位置设定默认信任带来的安全问题

（传统安全架构 - 假设内网是可信的）

- 以默认或静态信任为基础的访问控制带来的安全问题

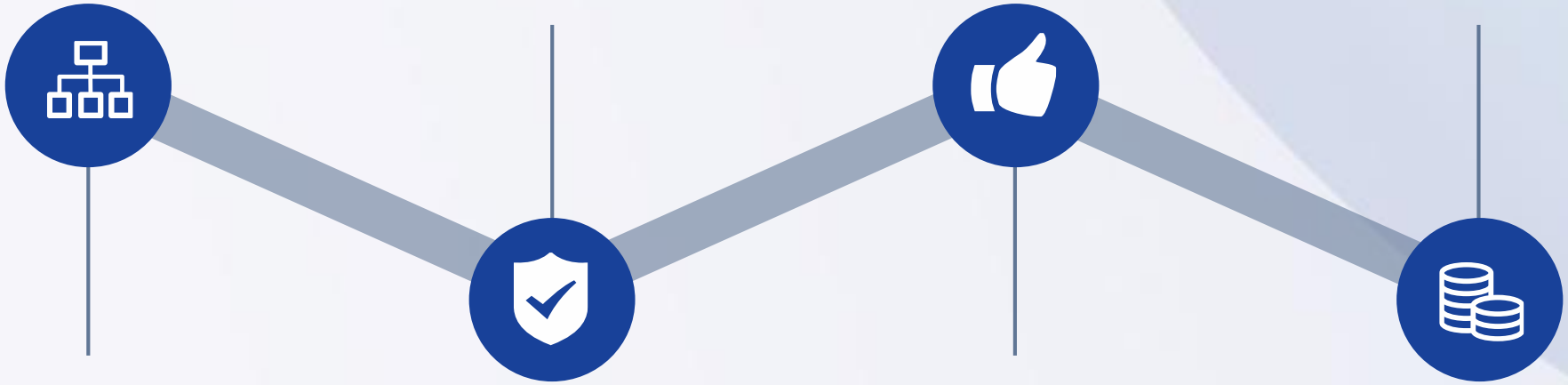
（传统安全架构 - 通过认证后用户是可信的）

（传统安全架构 - 通过静态授权后访问是可信的）

基于SSL安全接入技术进行创新改进

从“静态双因素认证”升级为“动态自适应身份认证”

从“访问行为审计”升级为“动态访问控制和灰度处置”



从终端的“基础准入“升级为”持续动态环境检测与业务准入”

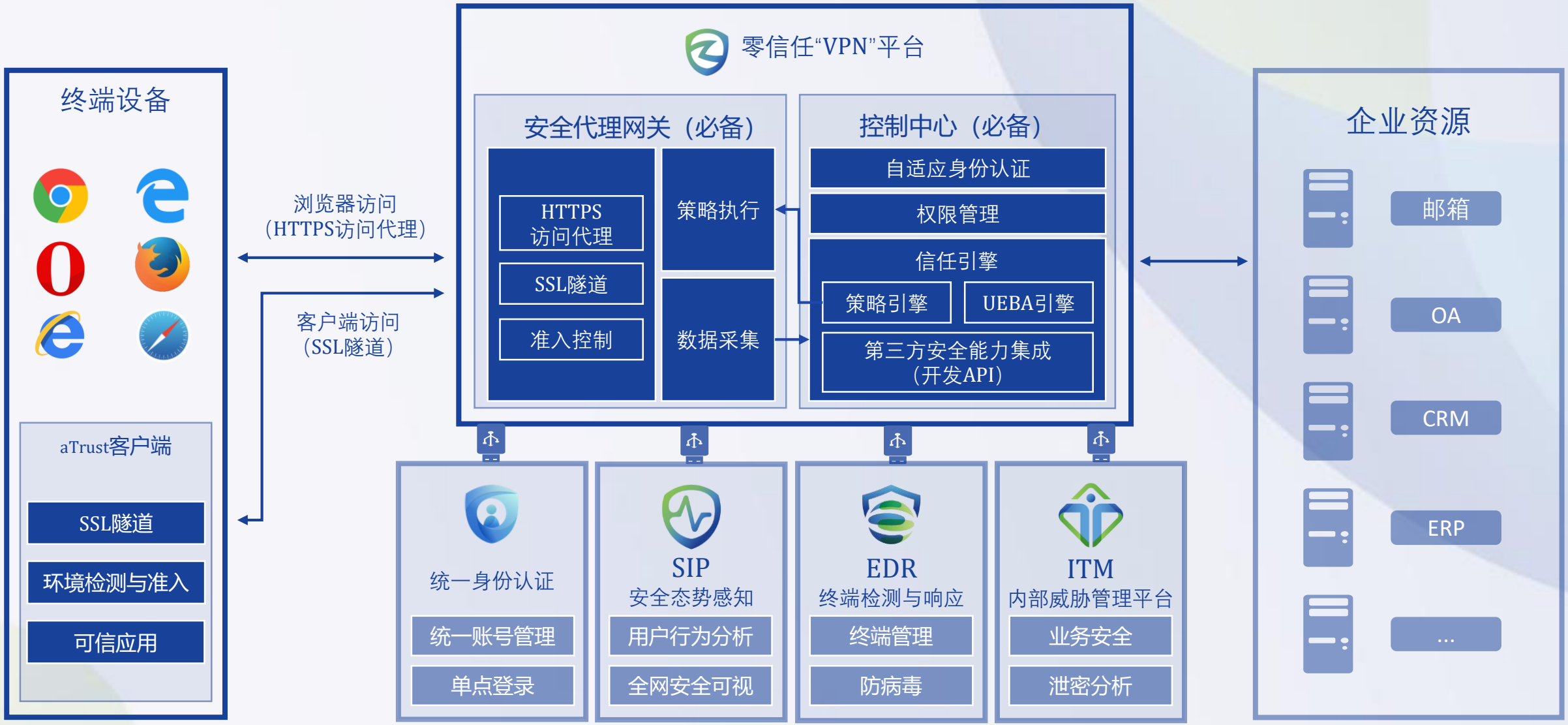
从“静态权限”升级为“动态权限”

深信服零信任“VPN”解决方案

深信服零信任“VPN”--融合零信任思想及VPN领域多年积累与创新

以身份为中心，构建可信访问、极简运维、智能权限的零信任安全架构

深信服零信任“VPN”整体架构



以身份为中心，构建可信访问、极简运维、智能权限的零信任安全架构

深信服零信任“VPN“核心优势及价值

核心价值：
全面身份化，并平衡安全与体验
核心优势：
动态自适应身份认证
认证增强
认证体验优化

核心价值：
业务最小暴露面、解决终端接入及访问业务安全保障难题
核心优势：
网络隐身，SPA单包授权机制（规划中）
动态全周期环境检测
可信应用
与全局业务准入

核心价值：
规模化远程办公
提升用户使用、运维体验
核心优势：
B/S业务免客户端
优化的传输技术
内外网一致体验
权限自梳理工具

核心价值：
动态调整权限，最小化权限，保护核心业务
核心优势：
安全基线（动态权限）
智能权限基线工具
灰度处置

价值演示：重构身份安全可信

简介：员工可以基于零信任架构随时随地开启办公。在不同的环境下，身份确认的强度也不一样。一旦识别到当前身份可能存在盗用/其他风险时，零信任将增加身份认证强度来保障身份可信度。

适用场景：全场景。

1. 账号风险：安全优先，身份二次校验

弱密码被盗风险：LDAP服务器存在大量弱密码，使用弱密码登陆时？

异地登录账号盗用风险：上次上海登录，这次长沙登录，是本人吗？

异常时间段登录异常风险：凌晨登录访问，是本人还是黑客？

SANGFOR 深信服科技

深信服智安全 SANGFOR SECURITY

深信服远程办公的积累与实践



深信服VPN领域近20年的技术和实践积累

深信服SSL VPN连续12年国内市场第一（IDC）
国内唯一入围Gartner魔力象限

深信服大量的客户积累

90%	80%	80%	85%	90%	95%
政府部委	全球500强 中资企业	银行/证券/保险	985/211高校	医疗百强	三大运营商

深信服VPN领域近20年的技术和实践积累

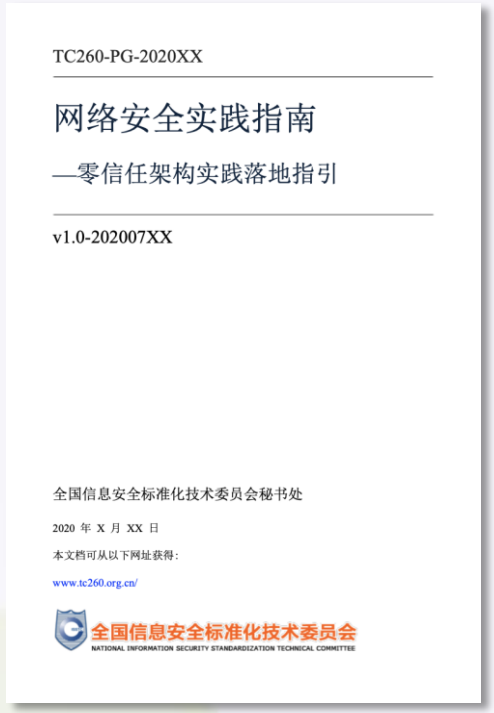
VPN技术领域近20年积累与创新

- ✓ **国家SSL/IPSEC VPN技术标准核心制定者**
- ✓ **2005年全球率先推出SSL、IPSEC一体化的VPN 安全网关**
- ✓ **VPN领域的专利技术积累：**

一种基于WEB的线路自动选择方法、
利用网页进行动态寻址的方法和系统专利、
多路复用VPN隧道的连接方法等专利积累等

零信任相关标准及生态实践

参与行业标准与指南制定


TC260-PG-2020XX

网络安全实践指南

—零信任架构实践落地指引

v1.0-202007XX

全国信息安全标准化技术委员会秘书处

2020 年 X 月 XX 日

本文档可从以下网址获得：

www.tc260.org.cn/

全国信息安全标准化技术委员会

NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

《网络安全实践指南-零信任架构实践落地指引》（即将发布）——信安标委（TC260）实践指南，TC260牵头，核心参与单位

CSA SDP工作组首批参与单位

为提高SDP在中国企业的应用，在中国云安全联盟的支持下，CSA GCR成立SDP工作组。工作组于2019年3月成立，深信服成为首批参与单位之一。


THANK YOU
2020深信服科技