



# 2022 建筑行业预测 系列之一

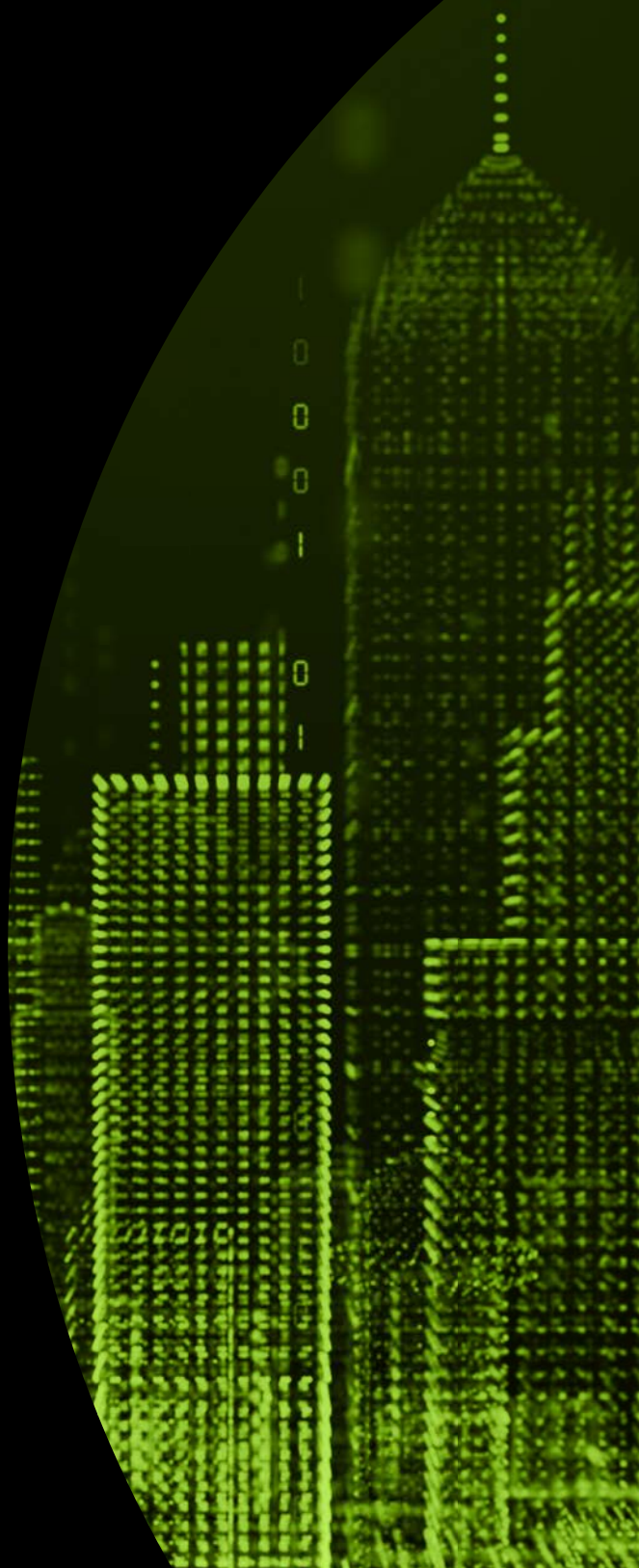
2022年3月

因我不同  
成就不凡

始于1845

# 构建建筑业网络安全

为何建筑和基础设施  
公司应在勒索软件战争  
时代塑造弹性战略？



## 简介

建筑4.0正在以一种不可预测的方式改变行业格局。人工智能 (Artificial Intelligence) 和高级分析 (Advanced Analytics) 正在实现新效率并创造风险管理新途径。

信息物理系统应加强绿地和棕地项目互联建筑设施的交付与管理。数字安全是避免混乱和增强复原力的关键所在。

多数分析员表示,建筑和基础设施 (Construction & Infrastructure) 行业将在2022年实现增长<sup>1</sup>。建筑和基础设施将支持国家的增长计划,加大医疗、公共安全和其他公共基础设施的投资。由于疫情已经将该行业从传统遗留限制性IT转向数字加速计划,网络安全的立足点需要从基于外围演变为面向数据。

在勒索软件战争时代,完整性和可用性作为高级分析和人工智能的本质属性应该予以留存。一流的运营商如果想要保持对竞争对手的创新投资优势,就必须保护其流程技术。由此而论,数据治理应该优先考虑分类和安全性。

## 数字身份

据Gartner称,“对关键基础设施领域组织的网络攻击急剧增加,从2013年的不到10次增加到2020年的近400次,增长达3,900%”。<sup>2</sup>

建筑和基础设施正面临诸多挑战:疫情危机、绿色革命和供应短缺,不一而足。为应对数不胜数的严峻挑战,建筑和基础设施应该转变其整体价值链。垂直整合需打破产业链层层障碍。应当部署数字身份和特权访问管理,以确保访问控制的同时整合供应商和承包商。

## 安全备份

采用建筑信息模型 (Building Information Modeling) 和数字孪生需要特别注意,确保数据的完整性和可用性。应当部署网络分段和日志监控,以最大限度减少网络攻击造成的业务影响。安全的备份环境,包括现场或基于云的备份,保障在必要时恢复数据,使生产和上市时间持续连贯。

- 
1. “What the 2021 construction demand means for 2022”, published 13 December 2021 <https://www.tomorrowstoday.com/2021/12/13/what-the-2021-construction-demand-means-for-2022/> Accessed 20 December 2021.  
Australian Industry and Skills Committee, “Construction, overview” last updated 18 January 2022 <https://nationalindustryinsights.aisc.net.au/industries/construction> Accessed 18 January 2022.  
James Leggate “Economist Projects 'Very Busy' 2022 for Construction Industry”, published 9 December 2021 <https://www.enr.com/articles/53205-economist-projects-very-busy-2022-for-construction-industry> Accessed 20 December 2021.
  2. Analyst(s): Katell Thielemann, Wam Voster, Barika Pace, Ruggero Contu, Richard Hunter, Critical Infrastructure in Focus, published 17 November 2021 <https://www.gartner.com/en> Accessed 20 December 2021.
  3. Dennis Scimeca “Prepare For More Cyberattacks in 2022” published 15 December 2021 <https://www.industryweek.com/technology-and-iiot/cybersecurity/article/21184175/prepare-for-more-cyberattacks-in-2022> Accessed 21 December 2021.  
Steve Morgan “Cybersecurity Jobs Report: 3.5 Million Openings In 2025”, published 9 November 2021 <https://cybersecurityventures.com/jobs/> Accessed 21 December 2021 accessed 28 July 2020.

### 信息物理系统 (Cyber-Physical Systems) 安全

那些以大量投资扩展其业务组合，提供特许经营、水和废弃物管理、能源系统和工厂、维护和资产管理解决方案的公司，正在尽其所能嵌入信息物理系统。

这一发展将扩大网络威胁的暴露面。尽管“传统”的IT安全如今已很难维持，信息物理系统安全更是难以实现。针对运营技术 (Operational Technology) 环境中信息物理系统的网络攻击已经从干扰流程 (如关闭水厂) 演变为破坏工业环境的完整性。此等威胁场景可能会被更快的5G连接所放大。为了应对新的信息物理系统威胁情形，企业应以全局视野制定信息物理系统安全战略，将运营技术、物联网 (IoT)、工业物联网 (IIoT) 和IT安全作为统筹协调工作的一环来管理。

预计在未来五年内，网络攻击将不断增长，网络安全人才的短缺亦将加剧。<sup>3</sup>

### 网络安全管理即服务

建筑和基础设施等众多行业将因此获得保护其运营的能力。网络安全治理需要多学科资源才能生效。网络安全的自给自足方法不再是一种选择，建筑和基础设施企业应采取多种投资模式，以确保达到适当的网络安全成熟度。

### 信息安全的四个领域将推动2022年网络议程：

风险评估和业务影响分析、漏洞评估工具和红队、安全意识和培训以及安全事故及事件管理。

建筑和基础设施行业应将网络安全融入其良好企业治理战略，以便支持在利益相关者和投资者之间建立信任。



## 作者介绍

### **Gianluca D'Antonio**

风险咨询合伙人  
德勤西班牙  
gdantonio@deloitte.es

## 德勤中国联系人

### **董伟龙**

工业产品及建筑行业领导合伙人  
德勤中国  
rictung@deloitte.com.cn

### **殷莉莉**

建筑行业领导合伙人  
德勤中国  
lilyin@deloitte.com.cn



#### 关于德勤

Deloitte (“德勤”)泛指一家或多家德勤有限公司,以及其全球成员所网络和它们的关联机构(统称为“德勤组织”)。德勤有限公司(又称“德勤全球”)及其每一家成员所和它们的关联机构均为具有独立法律地位的法律实体,相互之间不因第三方而承担任何责任或约束对方。德勤有限公司及其每一家成员所和它们的关联机构仅对自身行为及遗漏承担责任,而对相互的行为及遗漏不承担任何法律责任。德勤有限公司并不向客户提供服务。请参阅 [www.deloitte.com/cn/about](http://www.deloitte.com/cn/about) 了解更多信息。

德勤是全球领先的专业服务机构,为客户提供审计及鉴证、管理咨询、财务咨询、风险咨询、税务及相关服务。德勤透过遍及全球逾150个国家与地区的成员所网络及关联机构(统称为“德勤组织”)为财富全球500强企业约80%的企业提供专业服务。敬请访问[www.deloitte.com/cn/about](http://www.deloitte.com/cn/about),了解德勤全球约345,000名专业人员致力成就不凡的更多信息。

德勤亚太有限公司(即一家担保有限公司)是德勤有限公司的成员所。德勤亚太有限公司的每一家成员及其关联机构均为具有独立法律地位的法律实体,在亚太地区超过100座城市提供专业服务,包括奥克兰、曼谷、北京、河内、香港、雅加达、吉隆坡、马尼拉、墨尔本、大阪、首尔、上海、新加坡、悉尼、台北和东京。

德勤于1917年在上海设立办事处,德勤品牌由此进入中国。如今,德勤中国为中国本地和在华的跨国及高增长企业客户提供全面的审计及鉴证、管理咨询、财务咨询、风险咨询和税务服务。德勤中国持续致力为中国会计准则、税务制度及专业人才培养作出重要贡献。德勤中国是一家中国本土成立的专业服务机构,由德勤中国的合伙人所拥有。敬请访问 [www2.deloitte.com/cn/zh/social-media](http://www2.deloitte.com/cn/zh/social-media),通过我们的社交媒体平台,了解德勤在中国市场成就不凡的更多信息。

本通讯中所含内容乃一般性信息,任何德勤有限公司、其全球成员所网络或它们的关联机构(统称为“德勤组织”)并不因此构成提供任何专业建议或服务。在作出任何可能影响您的财务或业务的决策或采取任何相关行动前,您应咨询合资格的专业顾问。

我们并未对本通讯所含信息的准确性或完整性作出任何(明示或暗示)陈述、保证或承诺。任何德勤有限公司、其成员所、关联机构、员工或代理方均不对任何方因使用本通讯而直接或间接导致的任何损失或损害承担责任。德勤有限公司及其每一家成员所和它们的关联机构均为具有独立法律地位的法律实体。