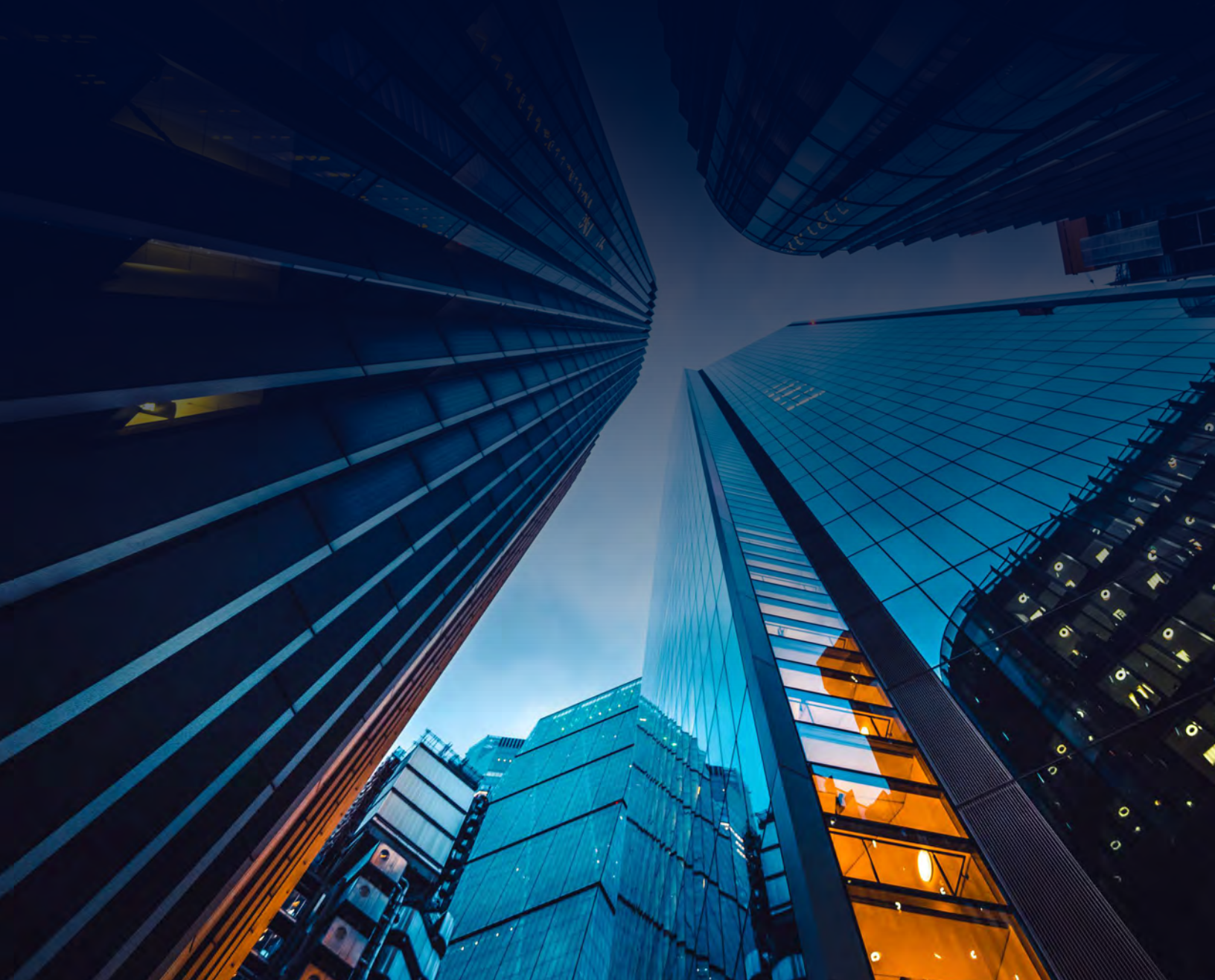
LTIMindtree

CASE STUDY

Black-Box Infrastructure Penetration Testing for a Large Investment Company



Client profile

A large investment company based in Canada has expressed interest in performing a black-box approach penetration testing to identify potential vulnerabilities across its infrastructure. The company has over 300 external and 2000 internal assets.

Business challenges

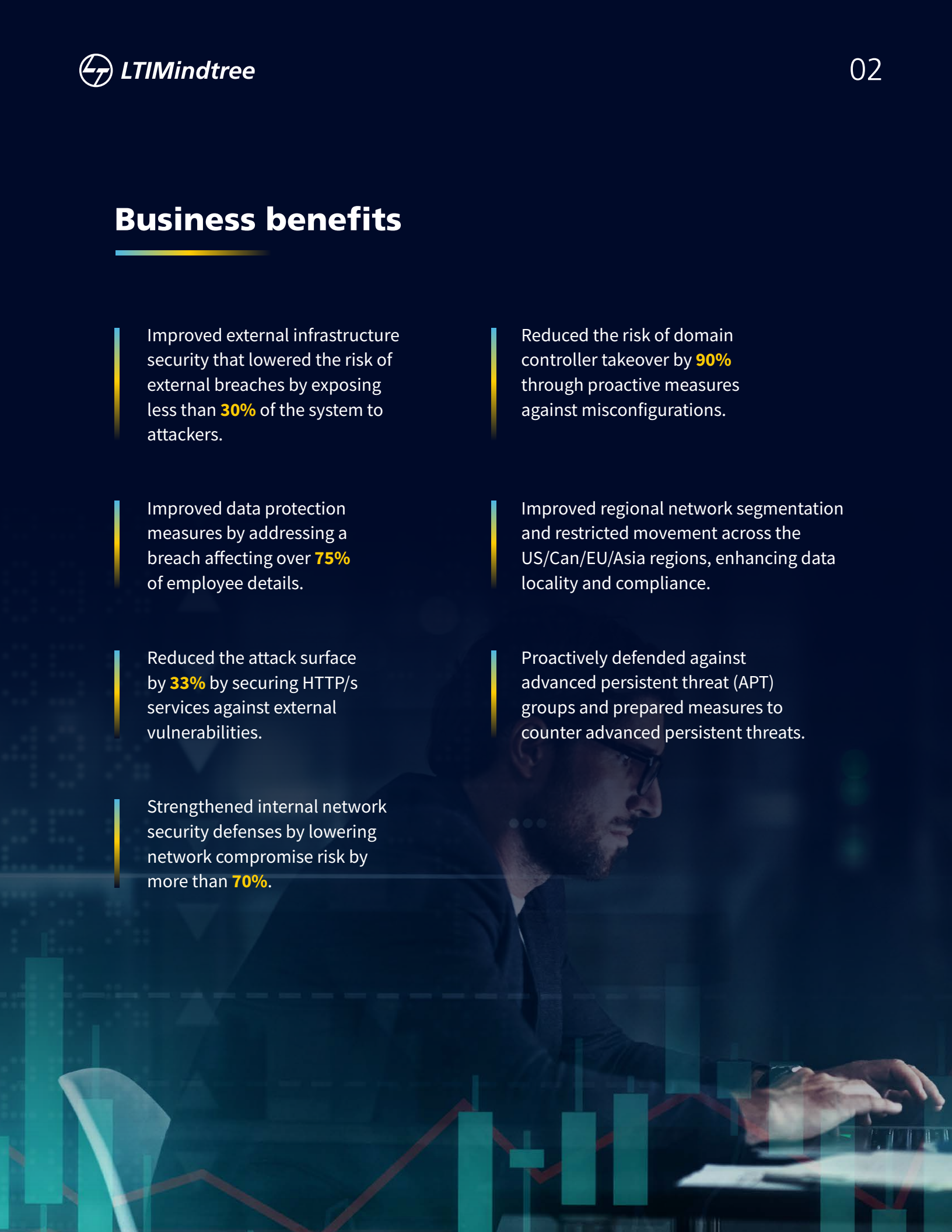
- Lack of a 24/7 vulnerability management solution to identify critical vulnerabilities
- The internal network was flat and could be reachable from any critical server or endpoint
- The Active Directory was not properly configured
- Critical vulnerabilities on internal IPs and domain controllers posed a risk to the overall network compromise
- Insufficient network segmentation allowed attackers to move freely across regions and escalate privileges
- Business continuity and disaster recovery plans were either outdated or incomplete, leaving the organization ill-prepared for major disruptions or cyberattacks
- Configuration management for critical infrastructure components lacked proper enforcement, exposing them to misconfiguration-based attacks

LTIMindtree solution

- Performed grey-box pen-testing on internal infrastructure stretched across the USA, Canada, Europe, and Asia.
- Recognized external assets' IP addresses via passive reconnaissance and identified internal IPs from the US/Can/EU/Asia regions.
- Collected employee details from previous data breaches via open-source intelligence (OSINT).
- Enumerated running external services to find and exploit possible vulnerabilities in a controlled manner.
- Enumerated running internal services to find vulnerabilities on workstations and networking devices.
- Identified Active Directory attack path and reported all the findings with possible patches, solutions, or workarounds.

Business benefits

- Improved external infrastructure security that lowered the risk of external breaches by exposing less than **30%** of the system to attackers.
- Reduced the risk of domain controller takeover by **90%** through proactive measures against misconfigurations.
- Improved data protection measures by addressing a breach affecting over **75%** of employee details.
- Improved regional network segmentation and restricted movement across the US/Can/EU/Asia regions, enhancing data locality and compliance.
- Reduced the attack surface by **33%** by securing HTTP/s services against external vulnerabilities.
- Proactively defended against advanced persistent threat (APT) groups and prepared measures to counter advanced persistent threats.
- Strengthened internal network security defenses by lowering network compromise risk by more than **70%**.



LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by 82,000+ talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — combines the industry-acclaimed strengths of erstwhile Larsen and Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale. For more information, please visit https://www.ltimindtree.com/.