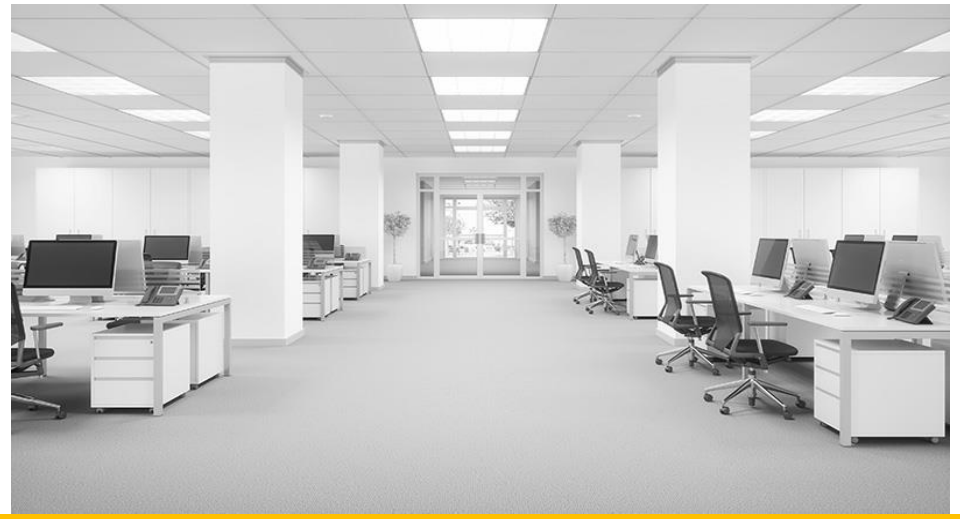
TWINTECH SOLUTIONS

Your Trusted Cyber Partner

IT Firm Global Infrastructure CASE STUDY

IT Firm Global Infrastructure – CASE STUDY



IT Firm's Business Situation

The IT company, in this scenario, offers application products based on .Net and Java to a diverse global customer base. The products are deployed over the internet, and the company maintains multiple server locations to facilitate swift and convenient software deployment for its clients.

"For example, the USA customers connect to servers in N. Virginia, while those in India connect to Mumbai servers."

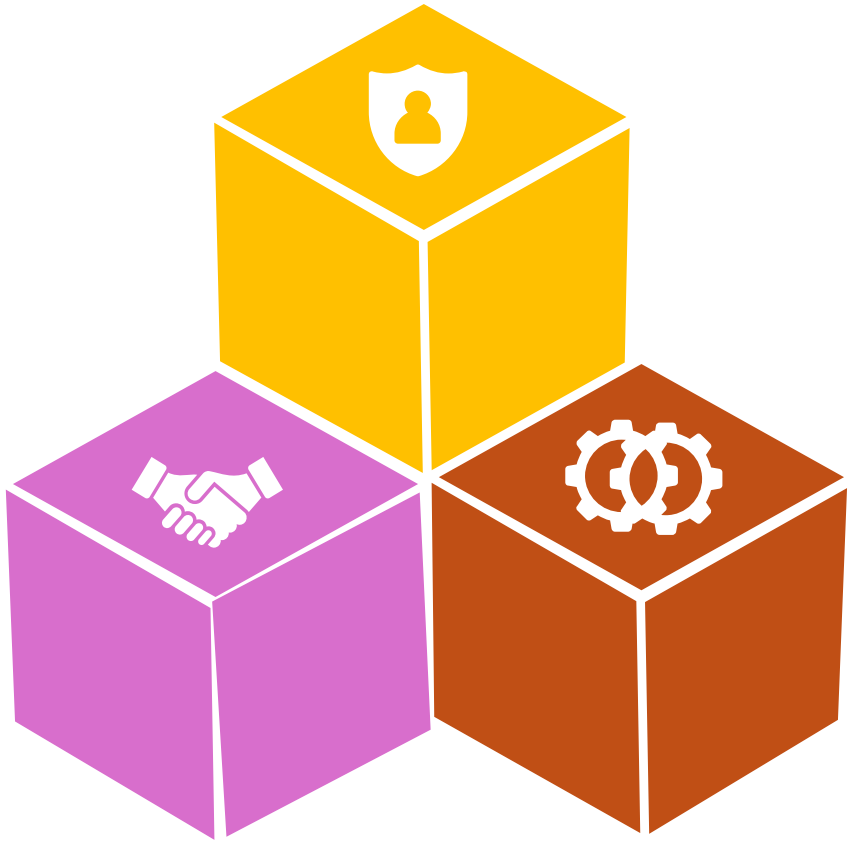
Network Security

IT Firm Global Infrastructure – CASE STUDY

scope

1. The IT company aimed to conduct an extensive network penetration test on their infrastructure in the USA and India.

Network Security



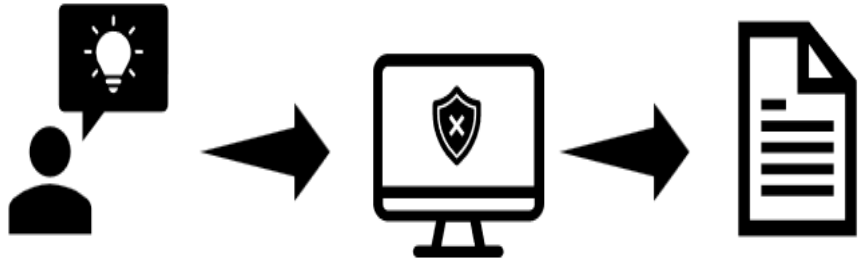
2. The primary focus was to guarantee the prevention of data leaks when the USA and India offices communicated for daily work. Additionally, they sought to verify the resilience of the product deployment infrastructure against potential Denial-Of-Service attacks.

3. TwinTech was engaged to conduct the PenTests and offer Information Security consulting to enhance cybersecurity practices.

IT Firm Global Infrastructure – CASE STUDY

An internal testing of network infrastructure, proxy servers, internet connectivity, and server access was suggested. An external testing in a black box mode was suggested for deployment infrastructure.

TwinTech had a Kick-Off meeting with firm's CEO and IT Manager to define PenTesting scope



Network Security

IT Firm Global Infrastructure – CASE STUDY

TWINTECH SOLUTIONS

We simulated as a malicious hacker, After performing reconnaissance, a series of internal network pentest attacks were performed.

An elaborate PenTesting exercise was performed to ensure perimeter defense is adequate, and only the online services required for deployment functionality purpose is available and secure.

This was followed by a series of password attacks such as, trying to crack windows passwords, download spyware, download files from internet which were supposed to be blocked by network policies, disable anti-virus etc.

Separate DDOS/Stress testing was performed on the deployment infrastructure.

Firewall Audit was conducted to ensure that firewalls at USA and India ends were configured properly.

Network Security

IT Firm Global Infrastructure – CASE STUDY

TWINTECH SOLUTIONS

A report with all severity Critical, High, Medium, Low & Info vulnerabilities and the corresponding remediations to fix it, was created.

The tasks performed were patch management architecture review, endpoint security deployment, deploying infrastructure security revamp etc.

IT firm's tech management was informed about maintaining the confidentiality of the report

After concluding the test and signing the reports, TwinTech Solutions acted as security consultants to the IT firm for upcoming months.

Based on the vulnerabilities found, a cyber security architecture change was suggested.

Network Security

IT Firm Global Infrastructure – CASE STUDY

TWINTECH SOLUTIONS

About Client & Client Team

- Software Development Company focusing on Lending Solutions Based out of California.
- Director IT Infra Structure , California

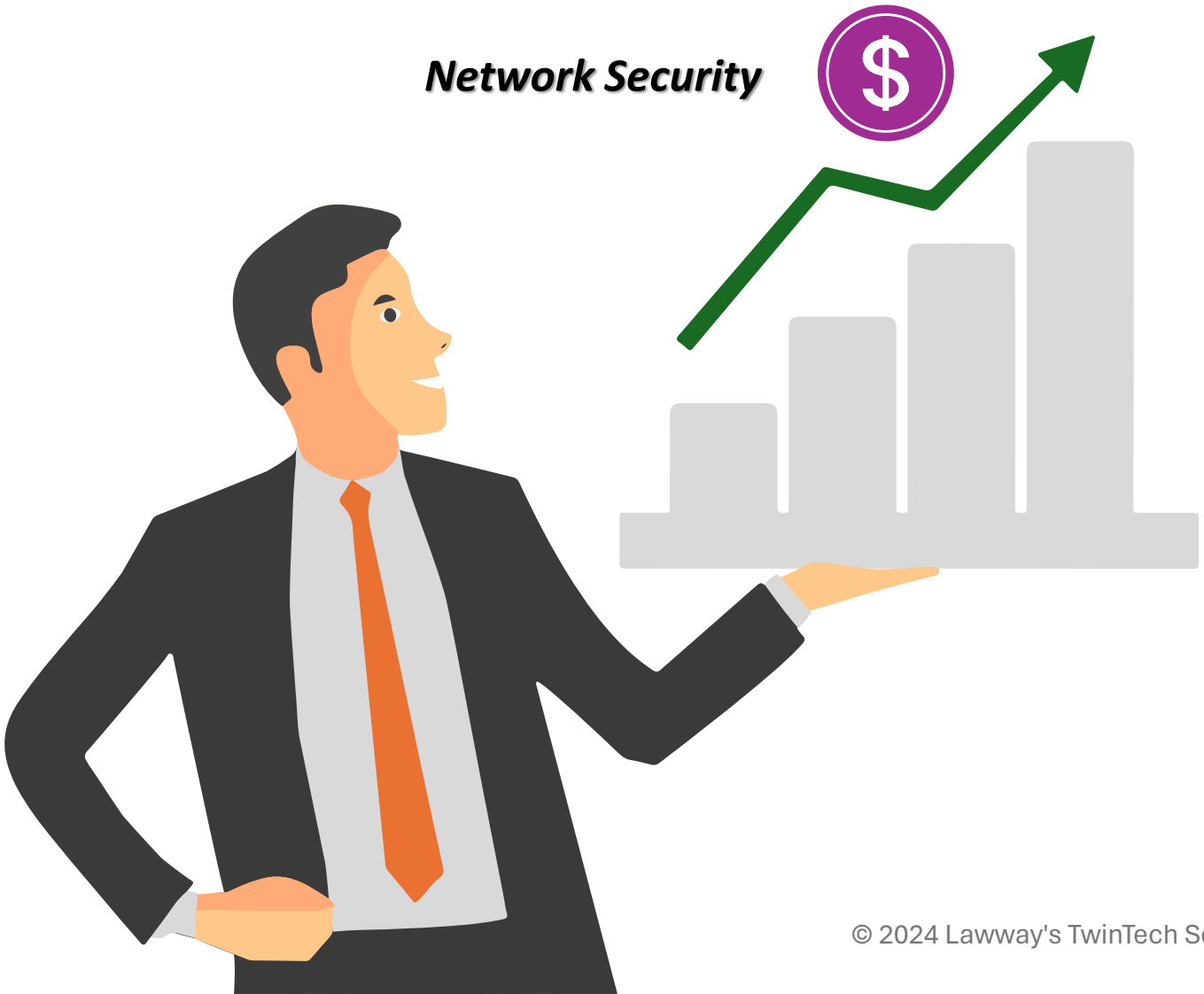
Client Needs

- Secure global communication channels
- Resilient product deployment
- Comprehensive network penetration test
- Cybersecurity enhancement

Key Strategies Implemented

- Comprehensive Testing Approach
- Thorough Vulnerability Identification
- Holistic Security Enhancement
- Business Confidence and International Recognition

IT Firm Global Infrastructure – CASE STUDY



BENEFITS

- IT firm's management could roll out more product securely, using revamped deployment infrastructure, which helped them gain confidence for future such plans.
- IT firm could secure business contracts with firms in Europe due to the fact that the infrastructure was **CREST certified** for cyber security and met international standards
- As an outcome of penetration test, vulnerabilities resulting into data leak were found, and fixed by deploying appropriate IT policies and software checks. This helped IT firm achieve a better internal security.