TATA COMMUNICATIONS

TATA

FACING THE FUTURE OF SECURITY

How the banking, financial services and insurance (BFSI) sector can prepare for the digital age

AT A GLANCE

The digital transformation dilemma
Opportunities for enterprises – and cyber criminals

A global story
How cyber security has changed forever

The challenge now
Why traditional security solutions can't keep up

The need for a holistic approach
People, Process, Technology

Tata Communications' Managed Security Services
Leading the way to a secure, connected state

THE BANKING AND FINANCIAL SERVICES SECTOR IS FACING A DIGITAL DILEMMA

From managing paper records to offering online purchases and one-click premium payments, banks and insurance entities have invested heavily to elevate the customer experience – and differentiate their offering. The COVID-19 pandemic has only served to accelerate this move online, but while digital transformation is a way to improve the bottom line and future-proof businesses, it comes with increasing security concerns too.

Given the critical importance of customer security in online and mobile banking, the growing threat of cybercrime is of particular concern to the BFSI sector. With attacks on digital banking systems, core transactional and back-office systems, and even ATMs, enterprises must act to protect their customers, their reputation – and the complex IT systems that make their business possible.

Data breaches are on the rise

As financial institutions forge ahead with digital transformation efforts, the pace of change has created more opportunities for attacks against networks and critical infrastructure. One of the most significant threats comes in the form of ransomware and extortion – with one organised gang claiming profits of over USD $100 million in a single year.[1] And just one attack on New Year's Eve last year cost currency exchange firm Travelex a staggering USD $2.3 million to regain access to its data.[2]

Meanwhile, traditional phishing attacks that aim to steal login credentials and Distributed Denial of Service (DDoS) attacks that attempt to sabotage digital transactions, are causing considerable damage to the BFSI sector. There has been a marked increase in DDoS attacks on the critical servers of banks and financial services institutions, with the financial and personal data held by the sector making it a prime target for Advanced Persistent Threat groups, including terrorist organisations. These attacks are designed to disrupt operations by targeting critical workloads.

422 million

Number of customers whose data was exposed in a 2019 breach of one of India's largest banks[3]

143

Of cash machines are vulnerable to attack[7]

542%

Spike in DDoS attacks (from Q4 2019 to Q1 2020)[4]

$3.92 million

Average cost of a data breach[8]

80%

Global rise in DDoS attacks (Q1 2020 versus Q1 2019)[5]

$6 trillion

Expected global spend on cybersecurity by 2021[9]

143

Cash machines shut down by Belgian bank Argenta following a 'jackpotting' cyberattack in 2020[6]

Source:

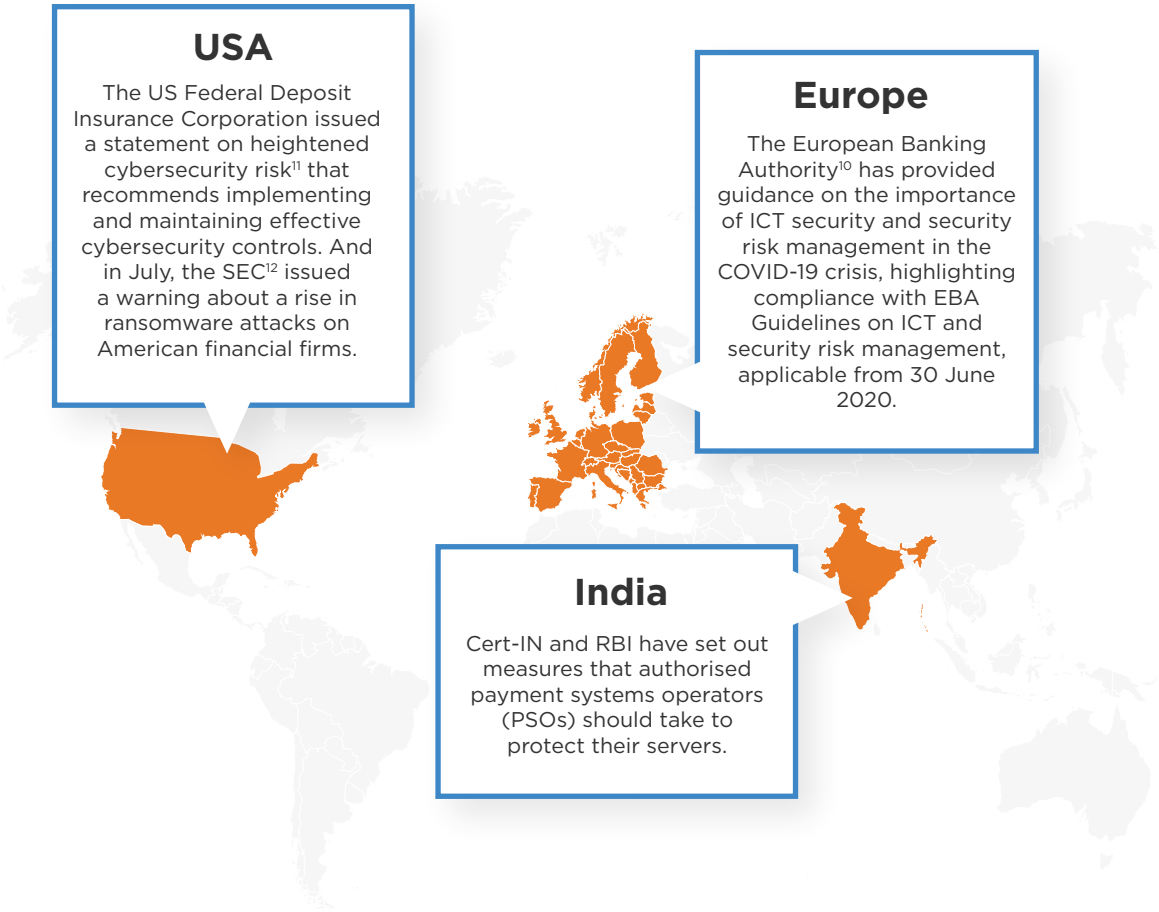
1, 2. https://www.bankinfosecurity.com/global-financial-industry-facing-fresh-round-cyberthreats-a-15409#:~:text=Although%20the%20global%20financial%20industry,Carnegie%20Endowment%20for%20International%20Peace
3. https://www.businessinsider.in/slideshows/biggest-data-breaches-of-2019/slidelist/72465909.cms#slideid=72465983
4. https://www.businesswire.com/news/home/20200630005295/en/DDoS-Attacks-Increase-542-Quarter-over-Quarter-Pandemic-Nexusguard/
5. https://tech.hindustantimes.com/tech/news/ddos-attacks-against-educational-resources-grew-by-350-in-h1-2020-71599653043082.html
6. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline
7, 8, 9. https://fortunly.com/statistics/data-breach-statistics/

THE THREAT TO THE BFSI SECTOR IS GLOBAL

Banking authorities around the world clearly recognise the increased threat of cyberattack, and are issuing advisories to help the BFSI sector respond.

Security in an uncertain world

Disruption in the wake of COVID-19 pandemic has brought a fresh slew of challenges for the BFSI sector, with personal and corporate banking customers a natural target. There has been a significant rise in the number of COVID-19-themed phishing attacks – emails to customers that appear as if they are offering financial support from the bank, but are in fact fraudulently asking customers to provide or validate their account or identity information. Other emails may contain malware that downloads onto a customer's system once a link is clicked.



> "Cyberattacks against the financial sector **increased by 238%** from February to April 2020, amid the COVID-19 surge."[13]

Source:

10. https://eba.europa.eu/sites/default/documents/files/document_library/Risk%20Analysis%20and%20Data/Risk%20Assessment%20Reports/2020/932012/JC%202020%2067%20Autumn%202020%20Report%20on%20Risks%20and%20Vulnerabilities.pdf
11. https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-5a.pdf
12. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline
13. https://www.helpnetsecurity.com/2020/06/17/cybercriminals-sophisticated/

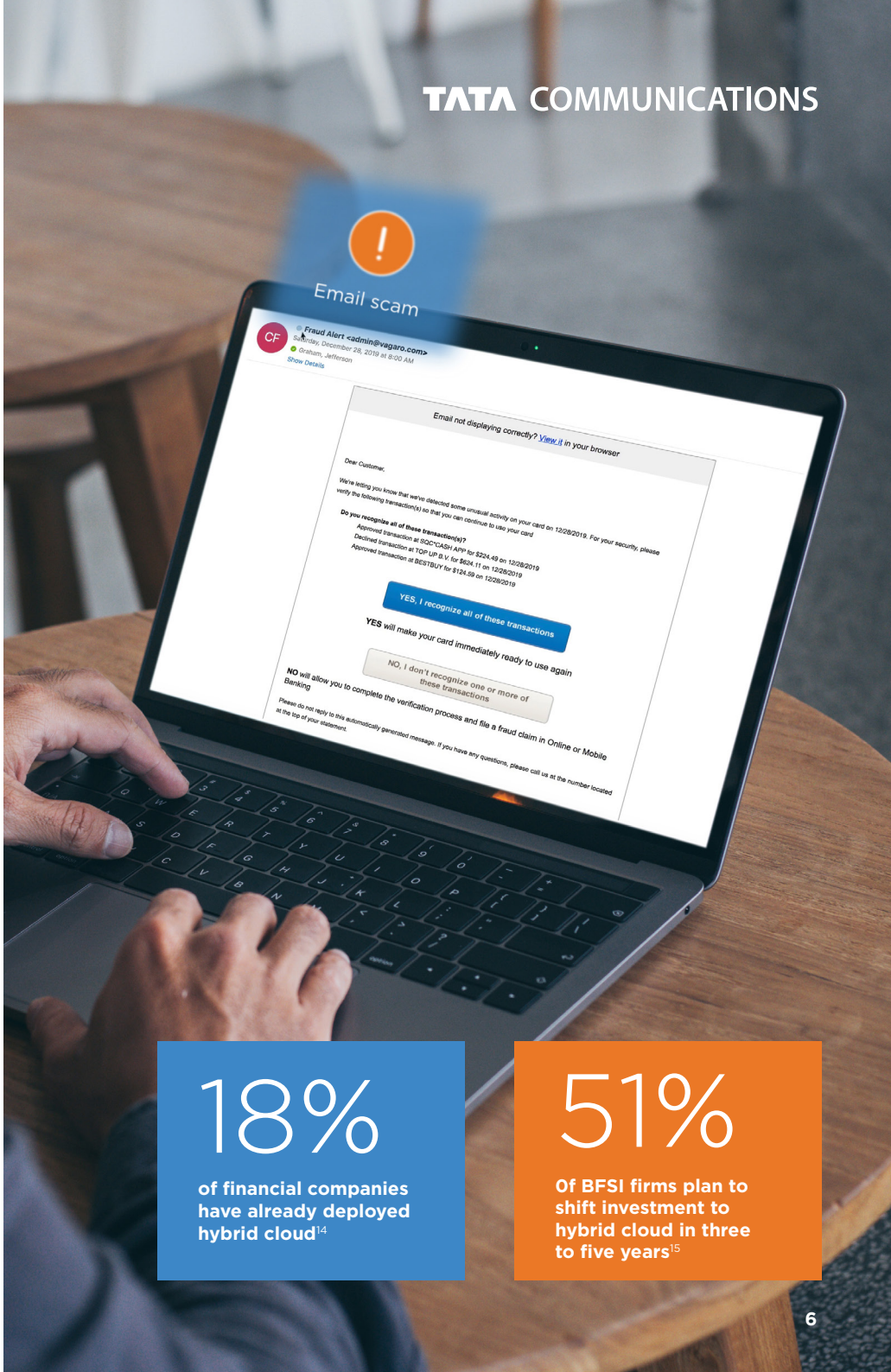
OPERATING ON THE FRONT FOOT

Where does this leave security teams working to navigate increased threats, with the added challenges of a global pandemic? As today's threat landscape becomes increasingly complex, traditional, prevention-focused security tools are simply not enough.

Security solutions must flex for a continually evolving digital environment, where new applications and workloads in the cloud blur the corporate perimeter. Now enterprises must protect both legacy and new cloud infrastructure, moving towards detection and response, and to net-new infrastructures.

While the Internet brings its own challenges – with expanding attack surface and vectors causing local breakouts that are difficult to secure and increase complexity – the right security strategy can become an enabler for change, rather than a barrier.

> "It is time for a **new perspective on cyber security** – one that puts it at the heart of digital transformation efforts."



Source:

14, 15: https://www.expresscomputer.in/news/financial-companies-embrace-hybrid-cloud-with-security-and-flexibility-top-of-mind/57846/

THE CHALLENGE

How many of these limitations feel familiar?

Disparate technologies and products:
With an average of 25 security OEM vendors in the enterprise environment, enterprises lack unified control – lowering productivity levels and adding to the complexities of managing such a vast security infrastructure.

Increase in cloud workloads:
Like most enterprises, banks are increasingly moving data to the cloud – opting for private over public cloud in most cases. The need to quickly migrate to new IaaS cloud environments often increases risks, through access point misconfiguration.

Lack of visibility, control, and compliance in a hybrid environment:
Lack of context arising from not having a clear view of distributed systems, combined with high intelligence and alert load, causes high volumes of false positives.

Vulnerable security posture and readiness to manage breaches:
Due to weak detection, response and breach handling capabilities and processes.

Lack of automation/orchestration for prioritising alerts:
Implementing automation and orchestration beyond rudimentary tasks can be difficult, but the resulting shift to manual operations is labour-intensive, inefficient and makes prioritising higher risk alerts harder.

Struggling resource strategy (headcount and competency):
High cost of in-house SOC management and a lack of skilled security staff to keep pace with technological advancements.

The complication of compliance:
BFSI enterprises tend to be geographically widespread. As a result, they must comply with multiple international/regional regulations and compliance requirements – with data compliance differing across continents, countries, and even states.

Inability to manage complexity:
Disparate tools, working in silos, with inconsistent processes and low/non-existence of a priority matrix don't support a unified control and execution model, causing a delay in mean time to detect (MTTD) and mean time to respond (MTTR).

THE SOLUTION

OVERCOMING TODAY'S SECURITY CHALLENGES

Financial organisations need to go beyond simply securing the perimeter in order to protect a growing digital infrastructure that is global, scalable, dynamic and mobile. Effective cyber security demands the right tools, frameworks, policies, and processes – all held together by a specialised skillset that will build confidence in security operations, and security teams.

With a greater understanding of the forces at work, organisations can optimise their security operations, moving from reactive to proactive, in order to protect their business, and their digital ambitions. By harnessing next-generation tools, advanced automation and threat intelligence, enterprises can proactively detect and mitigate attacks before they take hold.

Five ways to bring security up to speed – right now

Leverage proactive security frameworks, automation and analytics

Make use of hybrid SOC to stay ahead of alerts

Secure remote access for internal and external stakeholders

Secure the cloud environment

Secure the endpoints

Click to expand each step towards enhanced security...

Through Advanced Threat Management

It's critical to invest in new automated tools that leverage the latest threat intelligence, analytics and cloud-based resources and skills to actively seek out intrusions. While Red Team exercises are key to reducing exposure from Zero-Day attacks.

Threat intelligence can provide critical quality and context, with artificial intelligence, machine learning and UEBA capabilities, next-generation security analytics and managed detection and response (MDR) capabilities enabling anytime, anywhere monitoring of remote workers and their endpoints. So you can actively, proactively seek out intruders - for faster detection and remediation of threats.

Source: https://www.expresscomputer.in/news/financial-companies-embrace-hybrid-cloud-with-security-and-flexibility-top-of-mind/57846/

THIS ISN'T A CHALLENGE YOU NEED TO FACE ALONE

Digital security threats are global, but their impact can be felt keenly at a local level. Tata Communications' Managed Security Services deliver a holistic approach to security, equipping you with the intelligence, technology and knowhow you need to protect your business from modern threats.

By working closely with BFSI organisations, we've put in place the systems to stay safe and compliant. Our comprehensive solutions cover IT infrastructure end to end, giving you the confidence that you're securing your networks, endpoints, applications, data, and identity.

Flexible services work best when they have a strong framework to underpin them. We provide a multi-layer information security strategy that includes a Confidentiality, Integrity and Availability (CIA) model built on the three pillars of people, process and technology.

Introducing the powerful platforms, integrated solution frameworks and managed services to simplify cyber security complexities across the digital estate.

Intelligent, integrated solutions

Our advanced threat detection and management is driven by analytics and machine learning, informed by our global Big Data lake.

Powerful, pervasive platforms

Our integrated native platforms are built to deliver next-gen services, including SOAR as a Service, Catalyst Platform, DDoS Scrub Farm and globally deployed honey pots.

Experienced, expert support

Our security teams have demonstrated the expertise to seamlessly weave security across network, cloud, storage and more, for 24/7/365 support.

THE SOLUTION

COMPREHENSIVE SECURITY FOR COMPLETE PEACE OF MIND

DISCOVER TATA COMMUNICATIONS' MANAGED SECURITY SERVICES

Complete security, always-on conectivity

Dynamic solutions for dynamic enterprises

Safeguard your reputation and data

Advanced protection against advanced threats

Click to explore the four stages of 360-degree security...

One-stop cloud, content & identity security

Our multi-layered security framework protects against application layer attacks (for both cloud and on-premise), while ensuing the right people always have access.

- Public Cloud Security
- Hybrid Cloud Security
- Cloud Access Security Broker
- Cloud Security Management Platform
- Web Application Firewall
- Data Leak Prevention
- Identity as a Service
- Privilege Access Management
- Multi-Factor Authentication

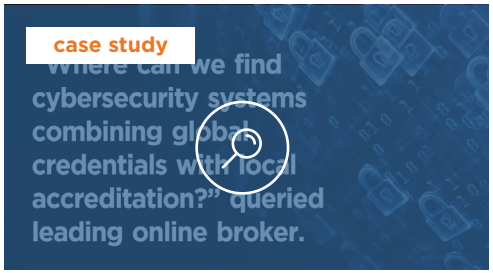
NOW'S THE TIME TO MAKE THE RIGHT INVESTMENT

Digital transformation offers incredible opportunities for growth. But any vulnerabilities in your approach give cyber criminals the opportunity to take advantage too. As you look to navigate an increasingly contactless economy, driven by post-pandemic uncertainty, now is the time to upgrade your cyber security programme. So that you can continue to embrace the innovation that will deliver the anywhere, anytime service today's customers demand.

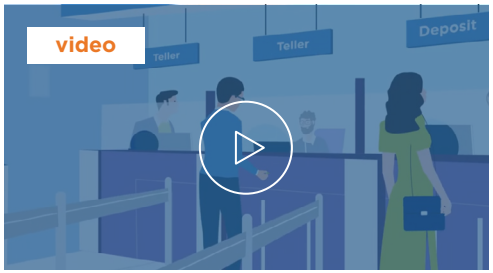
As the leading digital ecosystem enabler with a truly global footprint, Tata Communications has the experience – and the experts – to deliver the next-generation security solutions you need. To protect your customers, your business and your transformation ambitions.

A PARTNER YOU CAN TRUST

Delivering security for leading businesses worldwide



DDoS protection for Sharekhan



A fully managed SOC for a leading banking services firm in India

Hybrid DDoS solution for a leading banking group in India

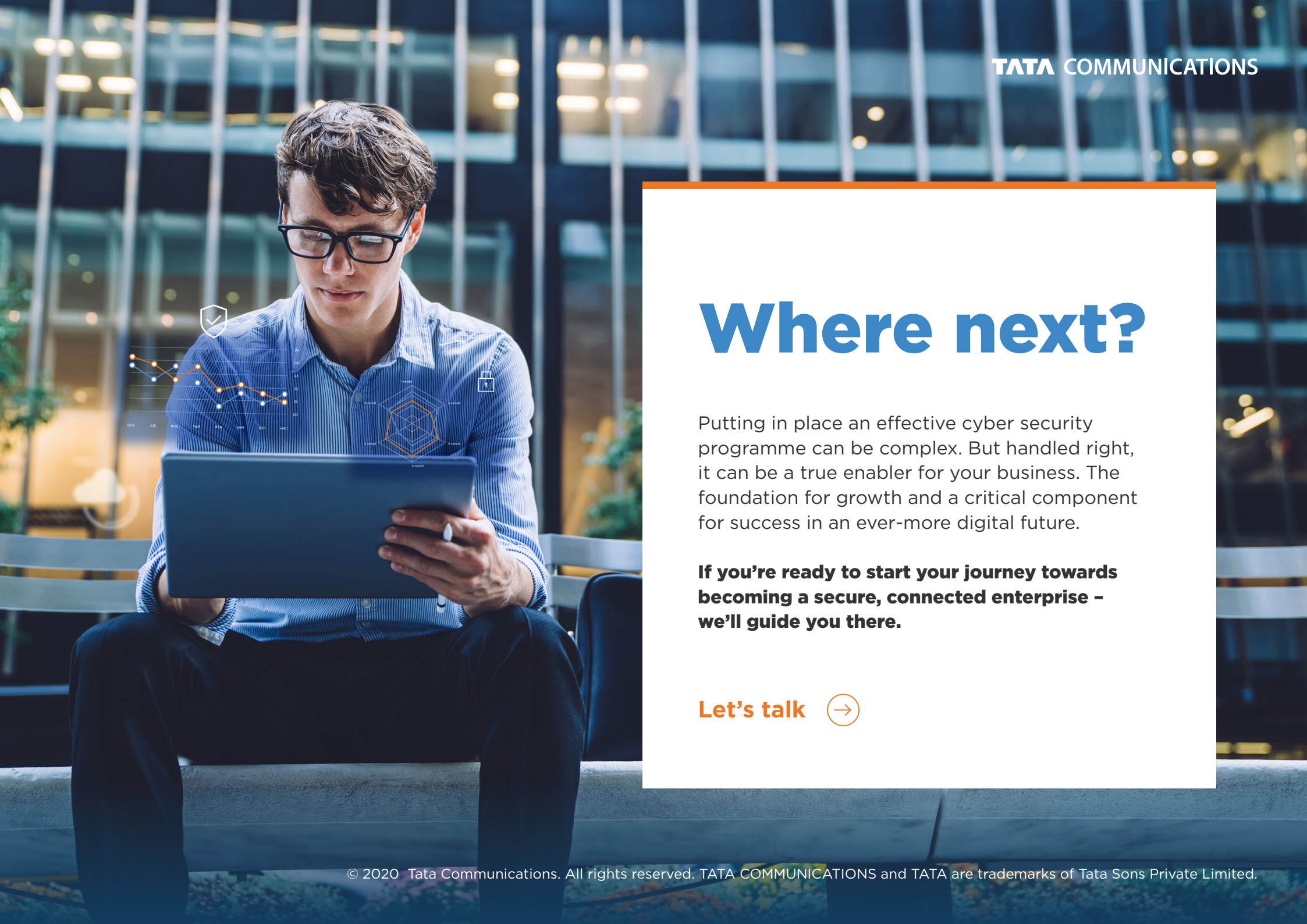
SIEM solution for a Major Financial Services Firm

Hybrid SIEM solution raises the bar for a financial services provider

A best-in-class SIEM solution for a global securities depository

Mitigating DNS Water Torture for a leading bank in India

Mitigating a multi-vector DDOS attack for a large bank in India



TATA COMMUNICATIONS

Where next?

Putting in place an effective cyber security programme can be complex. But handled right, it can be a true enabler for your business. The foundation for growth and a critical component for success in an ever-more digital future.

If you're ready to start your journey towards becoming a secure, connected enterprise – we'll guide you there.

Let's talk