TATA COMMUNICATIONS
TRANSFORMATION SERVICES

SECURITY-AS-A-SERVICE (SECaaS)

With digital transformation growing rapidly across the globe, businesses are becoming more dependent and connected to public clouds, partners, private data centres and to an ecosystem of ever interconnected devices.

The boundaries of an enterprise are soon diminishing to an inter-connectedness of business partners traversing a rich communication infrastructure of the Internet and managed VPN networks, like Carrier Ethernet and MPLS. While digital transformation creates higher productivity and automated business processes, a whole new level of complexity is starting to emerge in which cybersecurity is top of mind. A report in 2017 by Ponemon's benchmark cost of a data breach, averages around $3.62 million with a staggering cost to the global economy of more than $6 trillion in damages, annually. Added to the fact that the bad guys can locate themselves anywhere on the planet, out of reach from law enforcement, defense from security breech is becoming more difficult to manage including the staggering regulatory compliance imposed by each country.

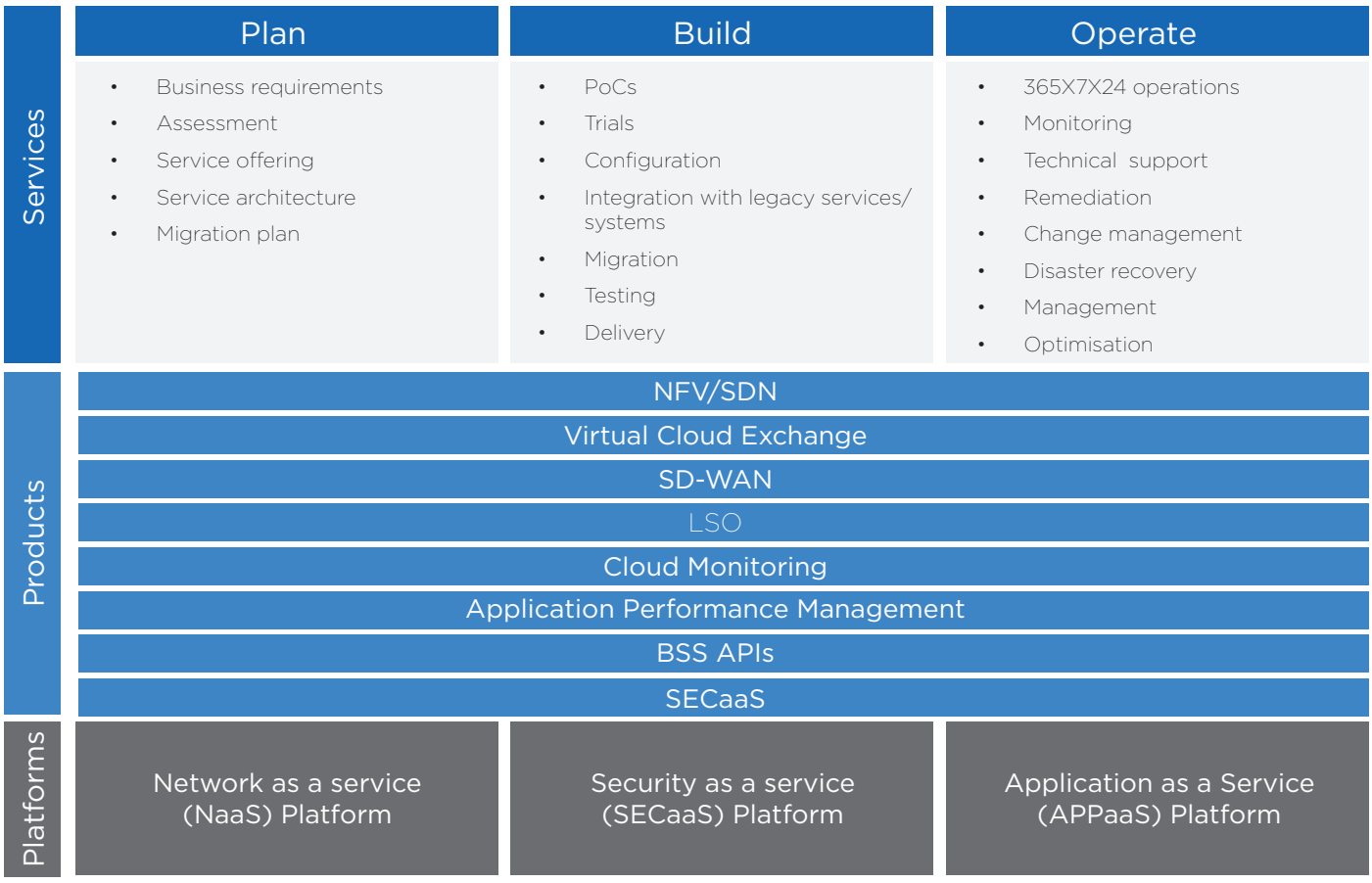
All of this leaves many Chief Information Security Officers (CISO) puzzled on how they are going to protect an organisation from cybercrime with the scare availability of skilled human resources and the complicated defense-in-depth systems available to date. CSO estimates the following IT security facts:

- 92% of malware is delivered by email
- 77% of compromised attacks in 2017 were fileless
- 56% of IT decision makers say targeted phishing attacks are their top security threat
- The average ransomware attack costs a company $5 million
- It takes organisations an average of 191 days to identify data breaches
- 88% companies spent more than $1 million on preparing for the GDPR
- 54% of companies experienced an industrial control system security incident
- 61% of organisations have experienced an IoT security incident

The pain of a Do-It-Yourself (DYI) cybersecurity business model is plagued with keeping up with new technology, security training, highly skilled labor, being on-call 24/7, triaging false positives alarms, managing egos/personalities, capital intensive security investments and many other challenging factors. All of this leaves many organisations looking to outsource cybersecurity to experts who are in the business of cyber threat management.

TCTS SECaaS SOLUTION OFFERING

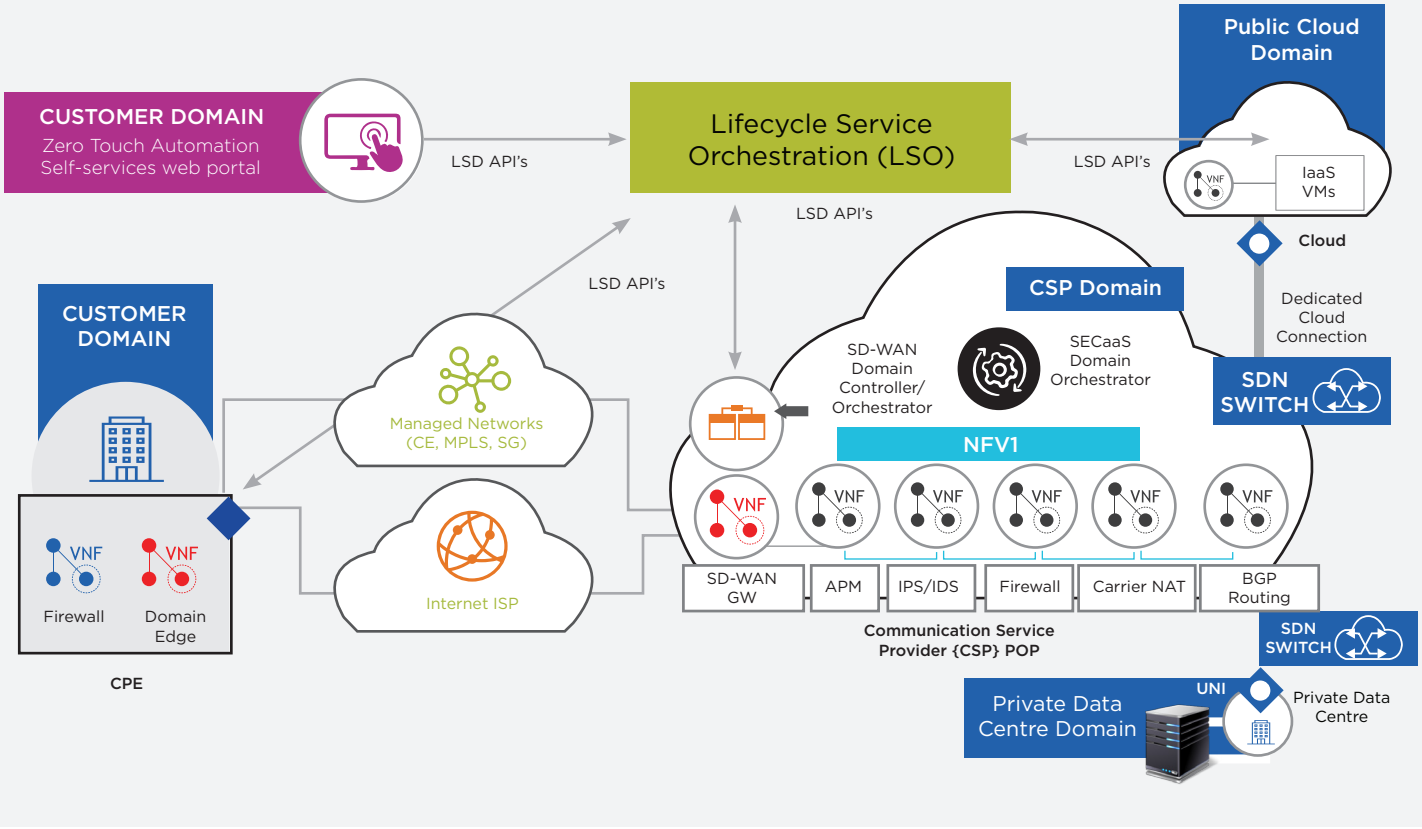
Introducing Tata Communications Transformation Services (TCTS) Security-as-a-Service (SECaaS) solution for Communication Service Providers (CSPs) and Managed Service Provider (MSPs). TCTS SECaaS is based on TCTS transformational platforms called Network-as-a-Service (NaaS) Platform, Security-as-a-Service (SECaaS) Platform and Application-as-a-Service (APPaaS) Platform that utilises the industry's best of breed an choice of product partners with TCTS's award winning next generation transformational consulting, deployment and operation services.



TCTS SECaaS offering is built upon Software Defined Network (SDN) and Network Function Virtualisation (NFV) technologies. It incorporates a defense-in-depth strategy by mitigating against many IT security threats such as

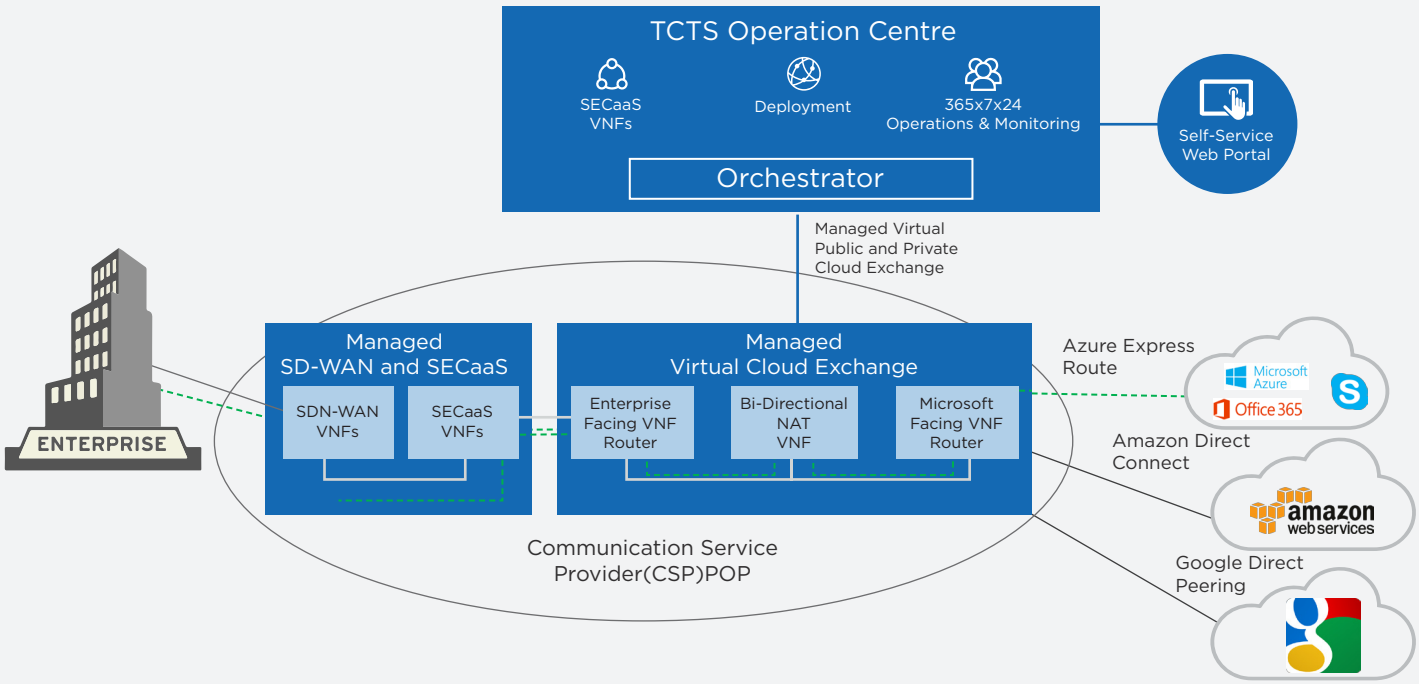
- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MitM) attack
- Phishing and spear phishing attacks
- Drive-by attack
- Password attack
- Zero-day attacks
- Ransomware and destructive malware
- Botnet activity
- Cryptojacking
- IoT vulnerabilities
- Attacks against SCADA and industrial control systems
- Mobile device targeted attacks
- Excessive bandwidth consumption
- Advanced evasion techniques

The innovative TCTS approach to SECaaS utilises Virtualised Network Functions (VNFs) that can be incorporated within NFV environments such as Universal Customer Premises Equipment (uCPE), NFV Infrastructures (NFVI), public cloud Infrastructure-as-a-Service (IaaS) and emerging Multi-Access Edge Compute environments. Most SECaaS deployments will require security operating as VNFs across multiple autonomies such as uCPE at customers sites, NFVI within CSP Points of Presences (PoPs) and IaaS within public cloud providers. All of this will require a single customer portal with zero touch automation that can manage VNFs in all three autonomies utilising a Lifecycle Service Orchestrator (LSO) for E2E managed services. TCTS professional services can also perform custom API integration by supplying or connecting between an existing CSP LSO and TCTS's SECaaS domain orchestrator.

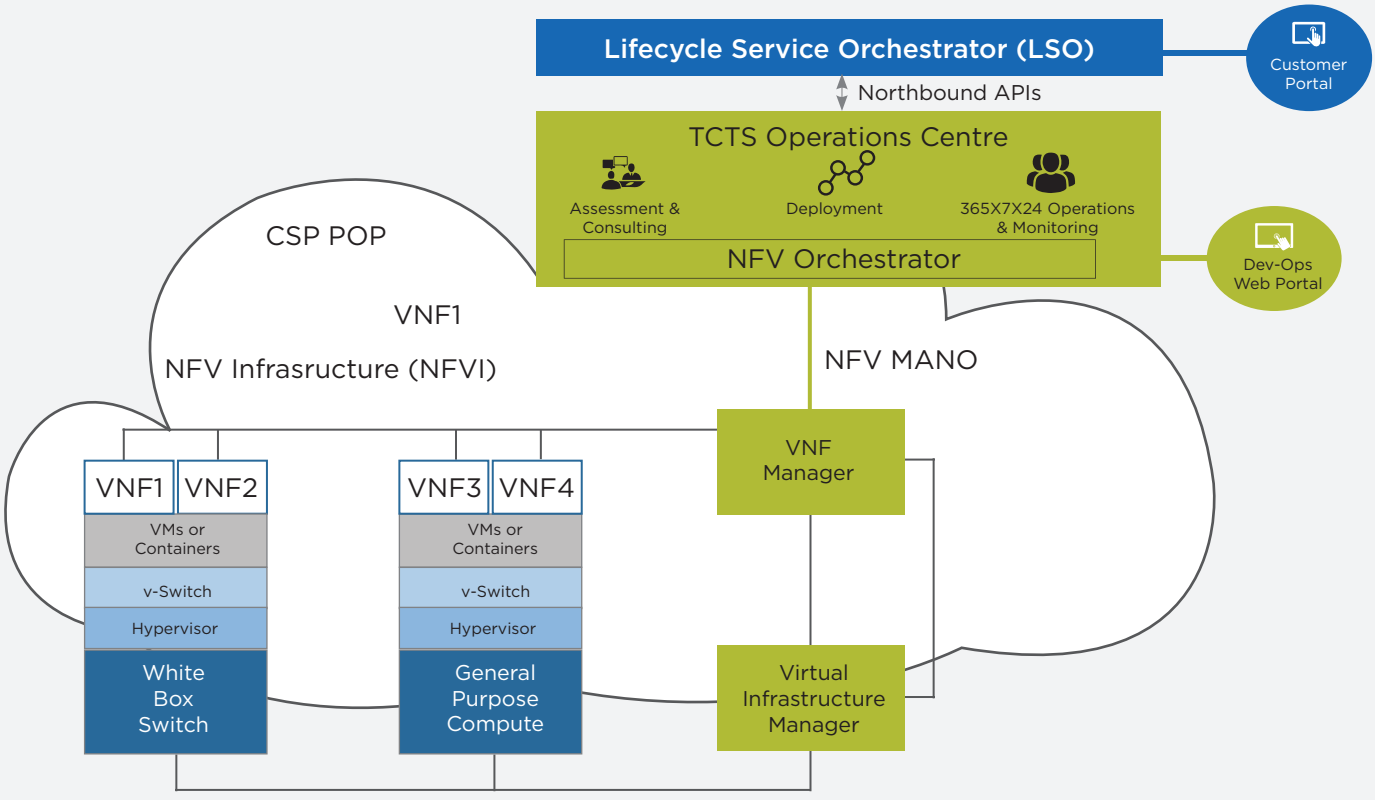


The TCTS SECaaS has been built to coexist with TCTS innovative Virtual Cloud Exchange (VCX) enabling CSPs and MSP to utilise a fully SDN and NFV approach while connecting to clouds. The VCX platform has been created to help CSPs connect with major public cloud providers. The key value propositions of VCX solution include

- All software (SDN) and virtualisation based (NFV) using general purpose CPUs (VNFs)
- Secure Software Defined WAN optimisation
- Route policy redistribution
- Carrier grade NAT
- Runs over any legacy packet and/or optical network
- Zero Touch Automation with tenant portal and APIs
- Multi-tenant based
- Hyperscale to millions of tenants



For CSPs or MSPs that have little or no SDN and NFV environments, TCTS has a synergistic SDN/NFV solution offering for which TCTS SEcaaS can utilise and facilitate SECaaS VNFs anywhere a NFVI is deployed.



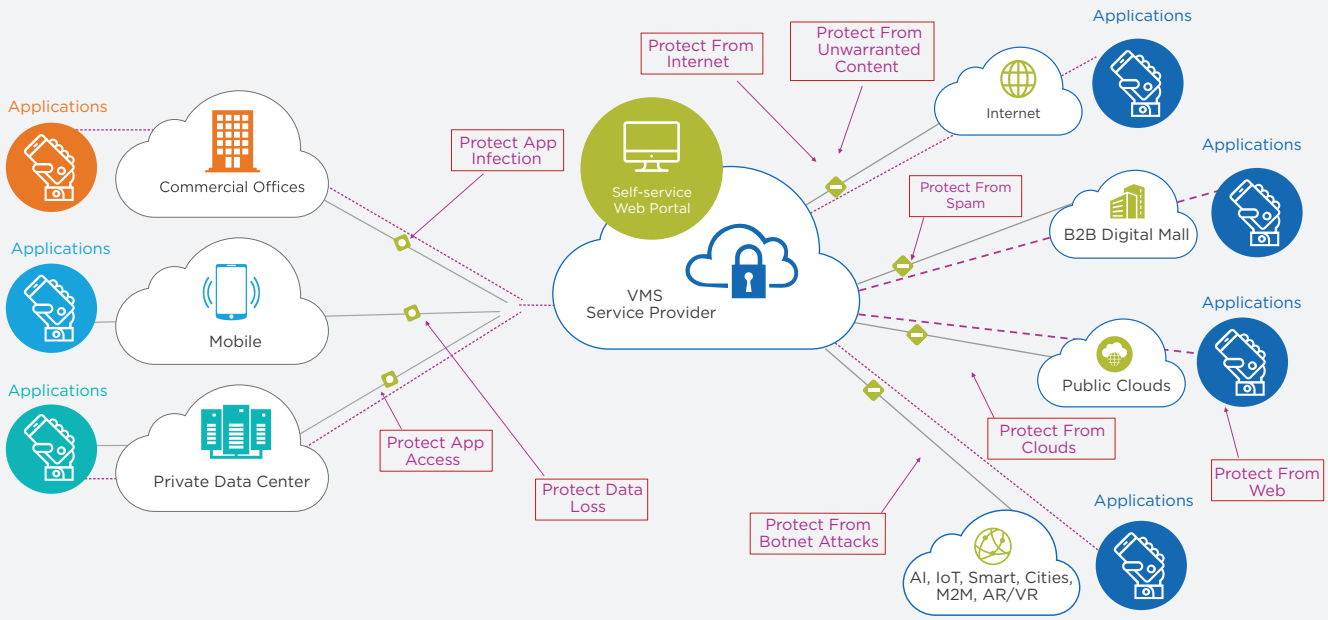
TCTS SECaaS offering can utilise TCTS uCPE managed service offering for CSPs that want to move to an uCPE model, eliminating vendor lock-in and facilitating an open CPE platform at customer sites for various multi-vendor VNFs while ensuring VNF isolation and protection.

TCTS SECaaS offering utilises a fully cloud native model in which the following security functions are offered as VNFs:

- Intrusion Prevention - controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet
- Next Gen Firewall - monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet
- Data Loss Prevention – advanced method of examining and managing network traffic with specific data or code payloads to prevent data theft
- Anti-Virus – software designed and developed to protect computers and networks from malware like viruses, computer worms, spyware, botnets, rootkits, keyloggers and such.
- Application Control - fine-grained access control based on applications, device and users
- IP Reputation and Anti-Botnet – protects from malicious source IP data and provides up-to-date threat intelligence about hostile sources
- Distributed Denial of Service (DDOS) - a Denial of Service (DoS) attack where multiple compromised systems are used to target a single system causing outage
- Web Filter - allows an enterprise IT Pro to block out pages from websites that are likely to include offensive content, spyware, viruses, and other objectionable content
- Anti-Spam - solutions that focus on blocking and mitigating the effects of unwarranted emails
- Web Security - application based firewall for web servers, including Machine Learning for automated configuration
- Endpoint Vulnerability - securing endpoints from access to an enterprise network that can be exploited by malicious actors.
- VNF Isolation Protection - ensuring VNFs are isolated from other VNFs in VM and containers via the hypervisor
- Zero Day Behavioral Analytics – prevention from software/hardware vulnerabilities that can be exploited before a developer has an opportunity to create a patch to fix the vulnerability
- Cloud Access Security Broker (CASB) - security policy enforcement point that is placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed
- Malware and phishing scrubber

The VNFs can be deployed in which threat mitigation from clouds, sites, devices, internet, partners, etc are all covered. TCTS SECaaS is a multi-tenant offering that allows a customer to specify, by policy, their desired security posture utilising a zero-touch automation model. A customer gains access to their own dedicated portal where the following security postures can be expressed with complete visibility and control. TCTS SECaaS Domain Orchestrator will automatically place the correct VNFs at the right locations with the correct security configurations downloaded by a pre-defined and updated profile template. Some examples are depicted below:

Cyber Security Policy (examples)	Mapping to SECaaS VNF(s)
PROTECT application(s) <application group> from data loss	Data Loss Prevention
PROTECT application(s) <application group> from infections	Intrusion Protection Service, Zero Day Behavioral Analytics and Web Security
PROTECT application(s) <application group> and site(s) <site group> from the Internet	Next Gen Firewall and Web Security
PROTECT application(s) <application group> from unwarranted cloud traffic	Cloud Access Security Broker, Intrusion Protection Service and Distributed Denial of Service protection
PROTECT application(s) <application group> and site(s) <site group> from unwarranted content	Malware and phishing scrubber, Anti-SPAM Filter and Web filter



TATA COMMUNICATIONS
TRANSFORMATION SERVICES

TCTS SECAAS PROFESSIONAL SERVICES

TCTS offers a set of cybersecurity services called Plan, Deploy and Operate for TCTS SECaaS offerings. This allows CSPs or MSPs worldwide to augment or outsource the needed expertise and get their SECaaS out to the market rapidly. The following are the set of SECaaS services TCTS offers:

Plan

- Business requirements
- Assessment
- Migration plan
- Security strategy consulting
- Secure architecture
- Governance, risk & compliance

Deploy

- PoCs
- Trials
- Configuration
- Integration with legacy services/systems
- Migration
- Training
- Migration and optimisation
- Cyber security assurance program
- Device security testing
- Penetration testing

Operate

- 365X7X24 operations
- Monitoring
- Technical support
- Remediation
- Change management
- Privilege access management
- Security monitoring and device management
- New product & services integration
- SOC with capability review
- SIEM and SEM alarm management

Managed services for network and business operations across Telco lifecycle areas, as well as consultancy and business enablement services, to global enterprises and telecommunications companies, via a global delivery model

7000+

6 Global delivery centres include on-site customer delivery centres

Multi domain/vendor agnostic network specialist across multiple technologies

- Field Operations
- Network Operations
- Submarine Network Operations
- Network Design
- Network Rollout
- UCC/SFB
- Lab As A Service (LaaS)
- Network Audit

- B2B Enablement
- Service Monetisation
- Customer Operations Management

- M2M/IOT
- SDN/NFV
- Self-Optimising Networks
- MVNO
- Hetrogeneous Networks
- Smart City Solutions

- Field Operations
- Network Operations
- Submarine Network Operations
- Network Design
- Network Rollout
- UCC/SFB
- Lab As A Service (LaaS)
- Network Audit

- Telecom Security Consulting/ Professional Services
- Telecom Security Testing
- Security Design & Implementation services
- Managed Security

- Business Process Consulting
- Technology Transformation
- Operational Transformation

Accelerate time-to-time
with proven experience and expertise

Simplify complexity
by improving process efficiency

Reduce cost by optimising
people, processes and technology

Improve end customer experience
by enhancing service availability

TATA COMMUNICATIONS
TRANSFORMATION SERVICES

TATA

About Tata Communications Transformation Services (TCTS)

Tata Communications Transformation Services (TCTS), a 100% subsidiary of Tata Communications Ltd, provides leading business transformation, managed network operations, network outsourcing and consultancy services to telecommunication companies around the world. TCTS delivers operational efficiency, cost transformation and revenue acceleration solutions for all the stages of the carrier process lifecycle including but not limited to network engineering and design, implementation and operations functions.

TCTS is a part of the USD $100+ billion Tata group. Tata group comprises of over 100 operating companies in seven business sectors. TCTS leverages the market expertise of Tata group's global telecom operation capabilities and globally established IT, process and consulting skills. It carries the rich traditions and business ethics of the Tata companies.

For more details on TCTS and how we can help your company build, operate and transform, please contact us at tcts.marketing@tatacommunications.com or visit www.tatacommunications-ts.com. To hear more from TCTS experts, join us on LinkedIn https://www.linkedin.com/company/tata-communications-transformation-services and follow us on Twitter https://twitter.com/Tata_TCTSL.