Protect your business with multi-layered security services from a trusted partner.
Digital technology has transformed the way companies work. It’s easier than ever for staff to get hold of information – and to make use of it. Cloud-first models help businesses to be more efficient and more agile. While big data and analytics help firms to give their customers a more personal service and drive profits.

But while these trends create opportunity, they also create risks. They present hackers and criminals with new and more sophisticated ways to attack your business. At the same time, internal threats like shadow IT have the potential to grow.

Knowing how to tackle these risks is critical. A security breach can cost you more than money. In an instant, you can lose the IP that gives you an edge or the hard-won trust of your customers.
While it’s digital technology creating new security risks, it’s also
digital tools that will protect you. The key is to understand how
mature your business is in terms of security. And put in place the
right measures for where you are and where you want to be.

In this ebook, we share some of our insights from providing
managed security services to businesses across the world.
Read on to learn about the latest trends and solutions in security
and how you can set up an ongoing and multi-layered defence
for your business.
The result is, sensitive data often lives on a range of clouds, servers, files and databases. In turn, employees or partners draw on this data from laptops, desktops, tablets and mobile phones – from anywhere in the world. This is the world in which CIOs and the IT department have to keep their business secure. Their challenge? Protect the enterprise without slowing it down. Later, we’ll look at the types of services that help you to achieve this. But first, let’s look at the current and emerging trends that are affecting how a business needs to protect itself.

To compete, modern businesses need to be agile and give their people the freedom to work when and where they want.

The result is, sensitive data often lives on a range of clouds, servers, files and databases. In turn, employees or partners draw on this data from laptops, desktops, tablets and mobile phones – from anywhere in the world. This is the world in which CIOs and the IT department have to keep their business secure. Their challenge? Protect the enterprise without slowing it down. Later, we’ll look at the types of services that help you to achieve this. But first, let’s look at the current and emerging trends that are affecting how a business needs to protect itself.
More and more businesses are moving core parts of their IT to the cloud. According to Forrester, the global public cloud services market is growing by 22% each year. This shift to the cloud brings new security challenges. Forrester highlights three main issues:

Mission-critical apps are moving to the cloud
As the apps and workloads in the cloud become more important, so does cloud security. As a result, many companies plan to use third-party solutions to protect their data.

Enterprises often work with multiple clouds and providers
This complexity creates challenges, such as: monitoring data, detecting anomalies, and intercepting bad behaviour.

Growth in PaaS/IaaS adds to the complexity
It’s more difficult to track data and keep it safe as it moves across platforms. And IaaS providers often don’t offer cross-platform security support. That’s why some businesses will turn to a centralized cloud security management (CCSM) tool. This can show them activity across their cloud platforms.

\[Source: Forrester Data: Cloud Security Solutions Forecast, 2016 To 2021 (Global); June 8, 2017 \]
These days, people go to work with smartphones and wearables and connect them to the network as a matter of course. Bring your own device has cemented this habit. And smart speakers and kitchen devices are joining the more traditional office devices on the network. They all give hackers more points of attack. And they allow shadow IT to creep up.

With the rise of the internet of things (IoT), the risk from more and more devices touching your network will only grow. By 2020, the installed base of IoT devices is forecast to be almost 31 billion. And IoT security spending worldwide is set to rise too. In 2017 alone, IoT security spending neared 1.2 billion US dollars. In fact, by 2020, 25 percent of attacks are expected to involve the IoT.

Your partners and supply chain face the same threats as you do. And breaches there can cause you as much damage as attacks closer to home. A recent Opus and Ponemon study found that 59% of companies had experienced a data breach that was caused by one of their vendors or third parties.

**What’s on your network?**

**More things to worry about?**

**It’s not just your organisation...**

---

Another factor that makes it important to get security right is regulation. Rules like GDPR demand that companies can keep and dispose of data safely. Failure to comply can result in fines and bad press.

To make matters worse, businesses face a skills gap in IT security. This makes it very hard to bring in the knowhow to tackle digital security. Companies can then struggle to shift from a reactive to a preventive approach. One solution is to draw on managed security services from providers who already have teams of experts in place.

The complication of compliance

Mind the gap

1.8 MILLION
Gap between security openings and skilled people to fill them by 2022*

In the traditional security model, you focused on a hard outside. And left a chewy centre. But the move to the cloud, more sophisticated attacks and internal threats mean that this model doesn’t work today. Forrester recommends the ‘Zero Trust’ model instead. This draws on identity, privacy and behavioural analytics to spread security across your estate.³

To tackle this complex mix of issues, you need a complete security solution. One that covers every part of your business and matches your needs. And a solution that gives you continuous protection. Next, we’ll look at how a managed service from the right provider can give you the right breadth and depth of cover.

No more chewy centres

The elements of good security
Our Managed Security Services give you a holistic approach to security. They give you the intelligence, technology and knowhow you need to protect your business from modern threats. By working closely with you, we put in place the systems you need to stay safe and compliant. A joined-up solution, it can cover every part of your IT. So you know you are securing networks, endpoints, applications, data, identity, and infrastructure.

Flexible services work best when they have a strong framework to underpin them. Next, we'll introduce our holistic security framework. And show how it keeps your security relevant and adaptable.
Our comprehensive service is based on the Tata Communications Security Framework:

**MULTI-LAYERED**
Our multi-layered security framework defends you from attacks on:
- Networks
- Endpoints
- Applications
- Data
- Identity
- Infrastructure

**INTEGRATED**
Our security models are joined up. Across data centres, on-premise servers or clouds (both public and private), we help you ensure that your IT is up-to-date, secure and compliant.

**SECURE**
Our secure operations feature:
- 5 global Cyber Security Response Centres (CSRCs)
- Facilities certified to international standards
- 300+ skilled security experts
- Strong partnerships with leading providers

**TRUSTED**
Businesses across the globe use us because we:
- Work with the best vendors to tailor a model for you
- Can scale cloud-based security, fast
- Visualise the data we base decisions on

Our security model helps you get the most out of your digital technology – while keeping your business one step ahead of threats.
Here are some real-world examples of our Managed Security Services in action.

CREATING A SECURE AND COMPLIANT ENVIRONMENT FOR BANKING

The client: A large, government-run bank

The challenge
Create an in-house Security Operations Centre (SOC) with 25 advanced controls. And then continue to monitor the bank’s security. This was one of the largest SOC setups in the region.

The solution
We worked closely with the customer to understand their business needs and issues. As a result, the client selected a flexible and cost-effective model that helped them meet security and compliance requirements. We used a top-down approach to build an enterprise security architecture, before deploying a range of core technologies, such as SIEM, GRC, APT protection, decoy services etc. This created multi-layered coverage. We also made use of existing security systems to reduce the need for upgrades.

Results
The bank has first-class security products and services in place. It has therefore been able to mitigate cyber attacks. And it complies with local regulations with ease.
Tata Communications did everything as quickly as possible to mitigate the network attack. They instantly grasped the extent of the situation and deployed a DDoS solution, even before a contract was signed.

NIKUNJ KAMPAANI, IT DIRECTOR, SYSCON INFOWAY

THWARTING NETWORK ATTACKS FOR A MAJOR ISP

The client: Syscon Infoway

The challenge
Customers rely on their ISP for bandwidth. If that bandwidth is unavailable because it is under attack, customers will look elsewhere. We worked with this ISP to thwart attacks in record time.

The solution
We deployed a managed DDoS service at rapid speed. We redirected infected traffic to scrubbing farms to remove infections. This freed-up bandwidth and restored critical services.

Results
With our DDoS service in place, the provider can fend off attacks and maintain network performance. It has round-the-clock support. And it avoids downtime when under attack.
LOOKING OUT FOR A RETAILER, THROUGH THE CLOUD

The client: A leading retailer

The challenge
Our client was struggling to manage security in-house as the needs of its users grew. A government initiative to promote digital payments saw retail payments jump by more than 300% from January 2016 to December 2017 – and our client’s multiple vendor solution wasn’t providing them with the level of protection they required in this new landscape.

The solution
We set up a security information and event management (SIEM) system, with a SOC. The SIEM system collected data from three different data centre locations, amounting to 25,000 Events Per Second (EPS). This allowed us to monitor and manage security full-time. Other services included:

- A cloud DDoS solution
- A firewall to protect key apps
- A secure web gateway
- Up to 300 devices integrated for identification of security events
- 31 security dashboards, 29 security reports and 32 security event monitoring use cases

Results
The retailer now has a consolidated view of security. It is free to focus on its business. And it has the expertise in place to respond to future challenges.
CREATING A SECURE, CENTRALISED NETWORK FOR AN ENGINEERING FIRM

The client: An engineering and technology business with 17,000 people

The challenge
Our client had a decentralised legacy technology infrastructure – islands of separate networks that used multiple service providers. Different service level agreements (SLAs) with each provider created manageability issues, and making business-critical applications safely available to users became a significant challenge. This environment created a high risk for potential cyber attacks and network availability was lower than expected.

The solution
We chose our Global VPN to link disparate networks and offices with a single platform. We then used vProxy unified threat management to protect the client’s IT and network. As a cloud-based solution, there was no need to buy new hardware for this managed service.

Results
The business has a robust and secure network for users and clients. Plus, central control. Benefits include:

- Close to 100 percent availability
- An estimated 50 percent increase in speed to market
- The IT and network team are 50 percent more productive
- CapEx reduced by 80 percent; OpEx reduced by 30 percent

“This collaboration has made innovative solutions available to both users and customers. Through our strong relationship with Tata Communications, we have laid a solid foundation to our expanding business.”

PRINCIPAL CONSULTANT
Protect your perimeter
With our network security in place, you can spot and stop intrusions and fend off DDoS attacks. We use machine learning to predict threats. And to take action quickly. We can also audit and optimise your firewalls.

Apps and access
We apply the latest tools to secure your cloud services and web apps. This includes identity as a service (IaaS) - to give your people a single, safe sign-on to all applications.

Keep data safe (wherever it is)
Data loss can cost your business dear. We help you identify the data you have, monitor it and secure it. So you can protect your IP, keep customer trust and stay compliant.

Global coverage, local services
We monitor your business 24/7 through our network of local CSRCs. Through a full range of services, we assess your security posture, spot gaps, manage threats and respond to events.
HOW TATA COMMUNICATIONS CAN HELP

SECURITY ON THE GROUND

Digital security threats are global. Yet Tata Communications understands the impact they can have at a local level. Our focus is on helping governments, enterprises and citizens combat cyber attacks or breaches. So we are establishing a network of Cyber Security Response Centres (CSRCs) around the world.

We have five CSRCs across the globe, with more on the way. Alongside these, we also have a showcase center in Chennai. Here, clients can look at the sophisticated tools available to mitigate security risks. Further CSRCs in Singapore, Dubai (UAE) and Europe will be followed by a US facility in 2019. This means we can provide global security services with deeper local expertise.

This is just part of our long-standing commitment to tackling cyber threats. We have also joined with SASTRA Deemed University in India to establish a cyber security lab. This partnership will address today’s security challenges. It will also build skills and capabilities for tomorrow. There is a global skills gap in cyber security and the threat landscape is becoming ever more complex. With these investments, we aim to boost the ability to tackle new and emerging security risks head-on.
WHAT WE OFFER

Security for digital platforms
- Integrated and seamless security for digital platforms across cloud, SDWAN and mobility
- Solutions to secure the connected IoT and OT environments

Drive threat analysis and visibility
- Unparalleled visibility of global network traffic flows and embedded attack patterns to issue threat intelligence advice
- Globally dispersed but localised Cyber Security Response Centres (CSRC)

Flexible and scalable security
- A global cloud infrastructure, to deliver on-demand, opex based solutions
- Security seamlessly integrated with service management and orchestration layers to drive automation

Cyber defence across boundaries
- Alignment with business drivers and emerging cyber security standards for better risk profiling
- Collaboration with federal and private organisations for critical asset protection

DIGITAL REWARDS COME WITH DIGITAL RISKS

THE CHANGING FACE OF IT SECURITY

SECURING SUCCESS

THE SCIENCE BEHIND SECURITY

DEFENDING YOUR INFRASTRUCTURE

HOW TATA COMMUNICATIONS CAN HELP

SUPPORTING A MORE SECURE YOU

“Tata Communications makes cyber security the starting point for digital transformation.”

OVUM12
You can manage the technology risks across your entire business with our Managed Security Services. From one partner, you get a complete solution. One that combines:

- **Network and infrastructure security**
  Predict and prevent breaches with real-time detection. Learn more

- **Secure application and access**
  Keep connected. Stay secure. Learn more

- **Threat management**
  Minimise the risk from emerging threats and attacks. Learn more

- **Risk and compliance**
  Prevent breaches and protect data. So, you can comply and avoid losses. Learn more

- **Content security and privacy**
  Protect your business with the latest traffic solutions and secure internet gateways. Learn more
A SECURITY SHOWCASE

In 2018, we launched a state-of-the-art Cyber Security Response Centre (CSRC) in Chennai, India. This is where customers can experience our MSS capabilities first-hand.

The CSRC hosts demos of security processes and technologies. Technical teams can see our SIEM platform in action. We take people through our cyber threat intelligence and cloud-based security practices. We also highlight our latest innovations. For example, our advanced attack predictions platform driven by machine learning. Key personnel can also view a live dashboard, which provides a business-aligned view of cyber security.

Just like Chennai, all our CSRCs are places where people can learn more about the latest tools we use to combat security risks.
A strong security solution supports a range of boardroom aims. It ensures business continuity. It gives you audits to stay compliant. And it gives you a solid base from which you can innovate.

To learn more about how we can partner with you on your digital journey, contact us on business@tatacommunications.com

How secure is your business?

Get a clear picture of your security posture with our maturity tool. So, you can see the best way to protect your business.

Take the survey >