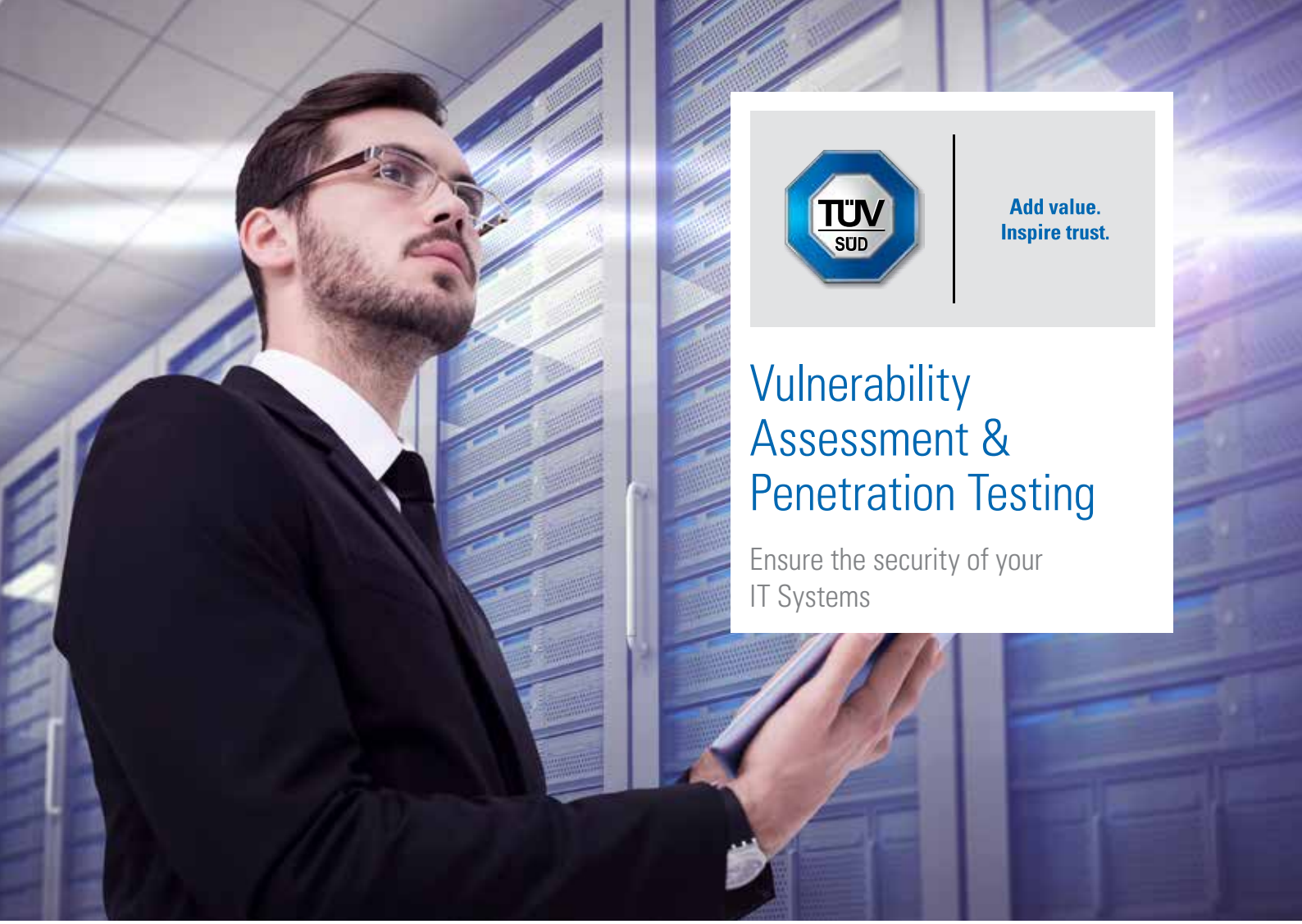

Add value.
Inspire trust.

Vulnerability Assessment & Penetration Testing

Ensure the security of your IT Systems

Your challenges

Technological advancements have enabled businesses to deliver multi-dimensional interfaces for driving innovations, growth and efficiencies. While these advancements have assisted in faster and seamless delivery, they have exposed the systems to cyberattacks, that can not only cause brand repudiation but also put the organisation's reputation, data, intellectual property and business at stake. These attacks could be an outcome of a weakness or slightest loophole in the multilayered IT systems such as operating systems, network, applications, infrastructure or communication devices. A well designed and deployed system with periodic monitoring and testing will help mitigate the risk of cyberattacks.

Cyber security landscape

Cyber security landscape encompasses various aspects such as strategy, governance and architecture, C.E.R.T. professional services with active defense services, security implementation, threat and vulnerability management, risk and compliance, incident management, managed services and identity and access management. As the threat landscape and attack vectors change, there is a constant need for security assessment. Vulnerability Assessment and Penetration Testing (VAPT) services help in evaluating the existing status of the security, identifying exact flaws and advising a remedial action plan to safeguard the system.

Why is Vulnerability Assessment and Penetration Testing (VAPT) important for your business?

VAPT puts your IT systems and security measures to test for vulnerabilities against the potential external and internal threats. A combination of automated and manual tests put the IT systems through various simulated scenarios that potential hackers may exploit to gain access to your information. Based on the findings, a detailed risk assessment report is delivered along with actions required to mitigate the risk. By addressing these security flaws, you can then be assured of the best possible protection. Revalidation can be performed to ensure closure of the identified vulnerabilities.

How can we help you?

TÜV SÜD's VAPT services are designed and delivered to achieve enhanced security and added economic value for your business. The precise scope of VAPT and the approach adopted, are customised to your requirements. The scope covers all aspects of IT infrastructure. Based on your requirements, you can avail any of the services, individually or in combination.

Scope of VAPT services

The scope of VAPT covers all levels of IT systems and access points:

- **Web applications**
  This involves thorough scrutiny of web applications to find out vulnerabilities and exploit them when accessed from multiple devices and locations. Testing is conducted to rate your security and a remedial plan is extended to mitigate the risks. The test is carried out in accordance with various guidelines such as OWASP, SANS 25, PCI DSS.

- **Network testing**
  Unauthorised network and data access are the key risks that are evaluated under network testing. VAPT and configuration review will be performed for routers, switches, firewalls, and wireless access points. Based on the findings, remedial measures will be recommended.

- **IT systems**
  This includes testing the external and internal systems such as servers, endpoints, databases, security systems and IOT devices that can be accessed from within and outside the organisation and propose measures to deal with risks. The test is carried out in accordance with OSSTMM.

- **Mobile applications**
  We follow OWASP guidelines for testing mobile apps for all platforms including Android, iOS and Windows systems. Our tests detect vulnerabilities in mobile applications that can be easily exploited, leading to manipulation of systems and access to personal information stored on these devices.

Your business benefits

- **Protect confidential data and reputation** – by ensuring that your confidential data is safe from cybercriminals, giving you and your customers peace of mind.
- **Improve business continuity** – by safeguarding your IT systems against potential attacks.
- **Enhance productivity** – by being proactive rather than reactive, thus helping to reduce the time for system restore and incidents closure.
- **Optimise cost** – with fully transparent and competitive costs, leaving your in-house IT staff free, to focus on their core functions.

Why choose TÜV SÜD?

Though organisations today have ramped up their IT risk management strategies, they face a constant need to evaluate their existing cyber security measures as the threat landscape keeps on altering dynamically.

TÜV SÜD's state-of-the-art penetration testing laboratory, located at Mumbai, India is fully-equipped with biometric access and dedicated connectivity to ensure 100% client data privacy. Our cyber security team comprises of certified penetration testers, capable of carrying out advanced simulations to determine security weaknesses. As a CERT-In empaneled regulatory auditor our cybersecurity team.

We deploy standardised global delivery processes to provide penetration testing services across the globe. The report is presented in a standard TÜV SÜD reporting format with details of the testing performed, vulnerabilities unearthed and recommended fixes. By addressing these security flaws found through VAPT, you can then be assured of the best possible protection against attacks from criminal hackers.

Our Head Offices in South Asia, ASEAN, Middle East and Africa Region

INDIA
Tel: +91 1800 212 2000
Email: info.in@tuvsud.com
www.tuvsud.com/in

SINGAPORE
Tel: +65 6778 7777
Email: info.sg@tuvsud.com
www.tuvsud.com/sg

ABU DHABI
Tel: +971 2 676 7600
Email: info.me@tuvsud.com
www.tuvsud.com/ae

AFRICA
Tel: +27 13 244 1330
Email: info.za@tuvsud.com
www.tuvsud.com/za

Follow us on social media linkedin.com/company/tuvsud

TÜV SÜD South Asia Pvt. Ltd. Solitaire, 4th Floor, ITI Road, Aundh, Pune - 411 007, Maharashtra, India.
1800-212-2000 **info.in@tuvsud.com** **www.tuvsud.com/in**