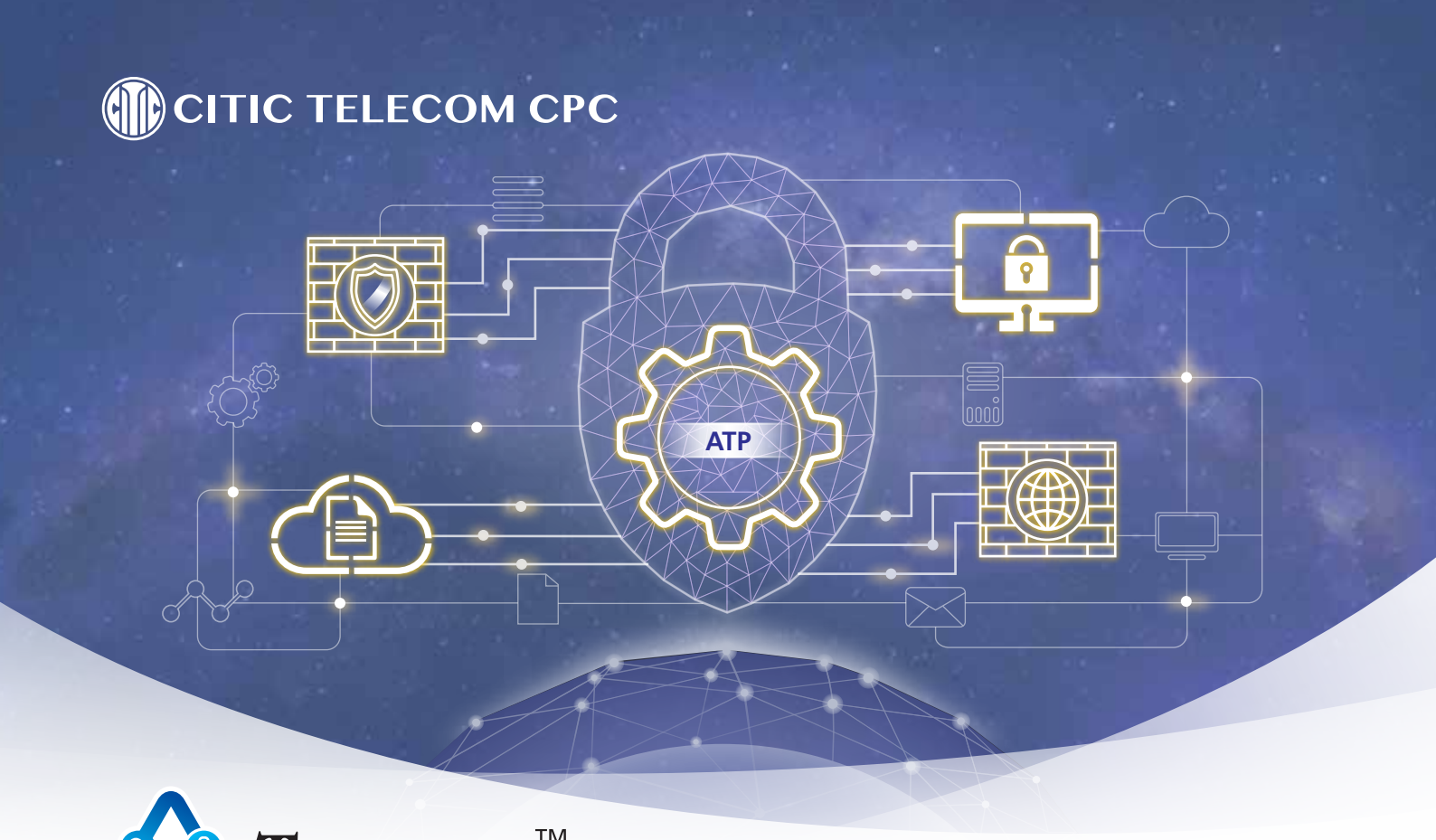
CITIC TELECOM CPC



TrustCSI™ ATP Advanced Threat Protection

Secure your Enterprise with the Superior Synergy of TrustCSI™ ATP

With a wide and growing range of sophisticated threats and attacks on applications and data, the modern enterprise operates in a riskier environment than ever before. The integrated synergy of **TrustCSI™ ATP** comprehensively secures your enterprise against advanced persistent threats across endpoints, networks and servers (eg. file servers, email servers and web servers). This managed ATP solution from CITIC Telecom CPC gives your organization all the benefits of a world-class 24-hour IT security department, without any of the management or cost overhead.

HIGHLIGHTS

- One-stop fully managed security solution efficiently and effectively delivers Advanced Threat Protection.
- Comprehensively handles wide variety of threats across multiple infrastructure layers, with real-time monitoring, proactive threat notification and mitigation.
- Actively detects and blocks new emerging threats and unknown attacks that evade other less sophisticated security solutions.
- Components actively interoperate and communicate with each other for real-time concerted security defense.
- Non-stop layered security protection encompasses Unified Threat Management (UTM), Web Application Firewall (WAF), Secure Email Gateway (SEG), Sandbox, and Round-the-clock Managed Security Services (MSS).

TrustCSI™ ATP Advanced Threat Protection

TrustCSI™ ATP brings a new approach to protecting your enterprise by combining multiple defense mechanisms, and the world-class resources of CITIC Telecom CPC's extensive security infrastructure and professional services. TrustCSI™ ATP is a complete one-stop solution that protects your network against sophisticated attacks.

Competitive Edges

Tailor-made total security solution

TrustCSI™ ATP will be specifically customized and deployed according to your unique infrastructure, resources, and requirements.

Modules interoperate for strong security synergy

Integration of the various defense mechanisms to identify suspicious activity, ensuring protections interoperate and leave no gaps to be exploited. The advanced UTM, WAF and SEG modules actively and dynamically communicate with the Sandbox module which updates new threat signatures when discovered.

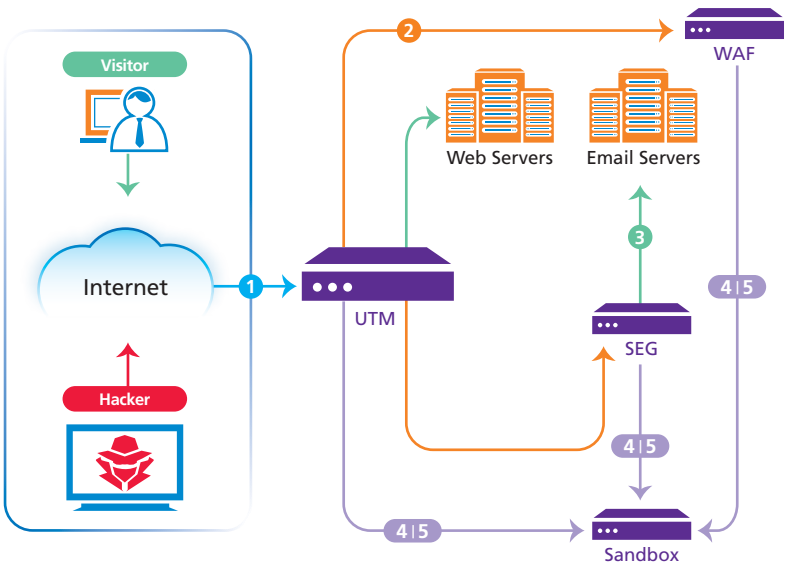
Round-the-clock monitoring and security advice

Your enterprise will be safeguarded by 24x7 security specialist, alerting with notification for any abnormalities , as well as expert recommendations for remedial actions.

Deep visibility into enterprise threat trends

SOCs make use of the Security Intelligence Platform to gain trends insight on threats to your digital resources, withweekly reports on UTM, WAF and SEG activity.

TrustCSI™ ATP Solution diagram



1. When visitors browse Websites, Web traffic arrives at the UTM module which fortifies the network perimeter by inspecting all types of inbound traffic.
2. The web application traffic is passed onto the WAF module which inspects the traffic by signature-based and behavioral-based analysis. Authorized traffic is passed back to the UTM module, while known offending traffic is blocked.
3. Email is passed to SEG module which inspects the content and attachments of message. Network and users are protected from spam and malware.
4. Unknown and suspicious files are passed onto the Sandbox module for quarantine. These files are executed in an emulated and isolated environment.
5. Once malicious or suspicious file is identified, sandbox will notify related module and perform threat response or eradication automatically.

Five major security components of TrustCSI™ ATP

UTM Unified Threat Management : A high performance security gateway that provides comprehensive protection against complex network, content, and application-level threats.

WAF Web Application Firewall : Uses advanced techniques to provide bidirectional protection against sophisticated Web application threats including SQL injection and cross-site scripting.

SEG Secure Email Gateway : Protects against various email security threats including phishing and malicious attachments.

Sandbox Sandbox : Executes suspicious files in a Virtual Machine to determine their true natures and risk levels. Threat mitigation is automated via integration with other security components.

MSS Managed Security Services : Offers full prevention, detection and correction, as well as monitoring and real-time alert services on 24x7 basis. It analyses vulnerabilities and detects real threats through Security Intelligence Platform.

CITIC Telecom CPC

W: www.citictel-cpc.com
Asia Pacific: info@citictel-cpc.com
Europe and CIS: info-eu@citictel-cpc.com

Hong Kong T: 852 2170 7101
Japan T: 81 3 5339 1968
Estonia T: 372 622 33 99
Russia T: 7 495 981 5676
Taiwan T: 886 2 6600 2588
Malaysia T: 603 2280 1500
Poland T: 48 22 630 63 30
The Netherlands T: 31 20 567 2000
Mainland China (Toll Free): 400 651 7550
Singapore T: 65 6220 6606

TAP1910EN