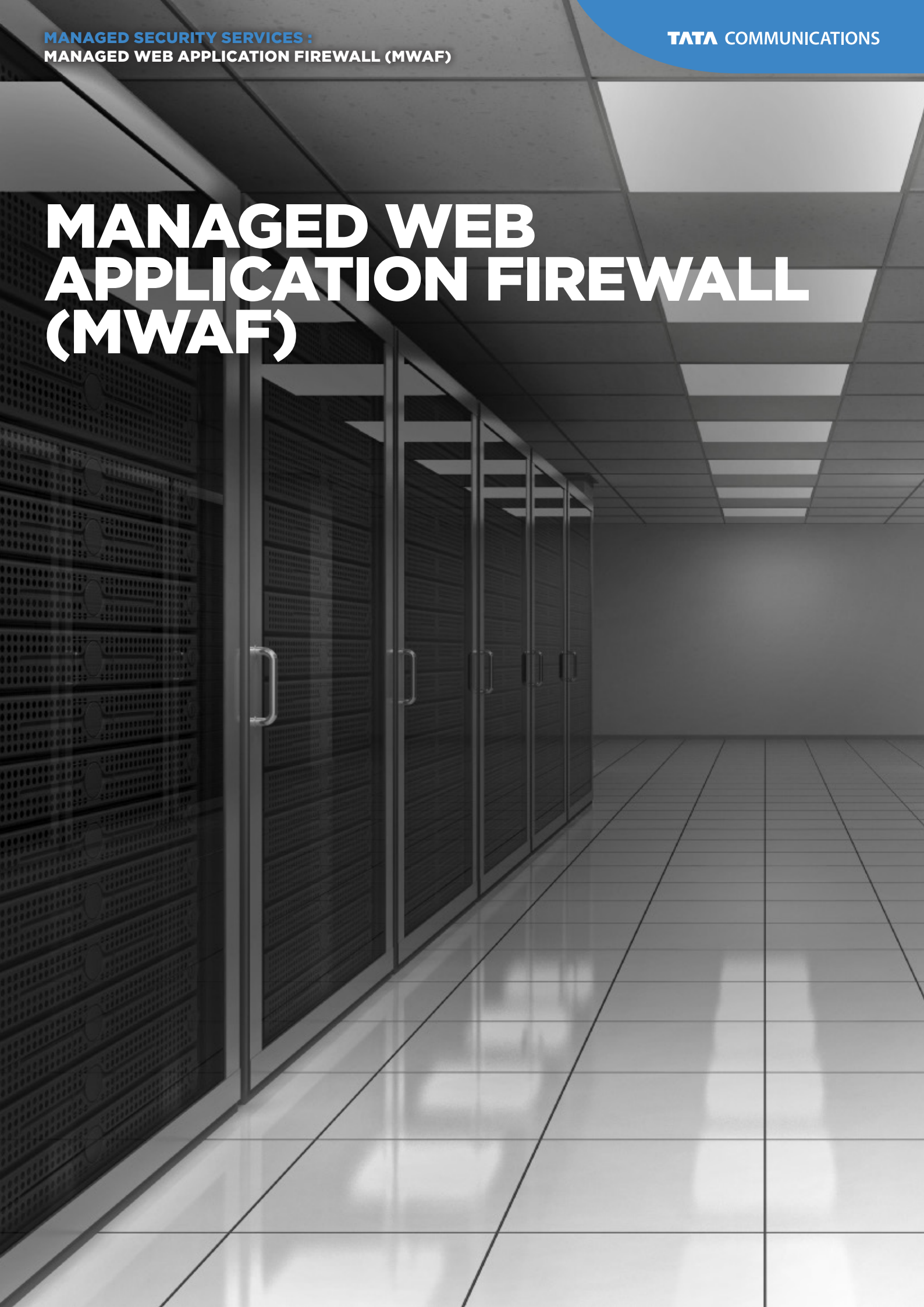
TATA COMMUNICATIONS

MANAGED WEB APPLICATION FIREWALL (MWAF)



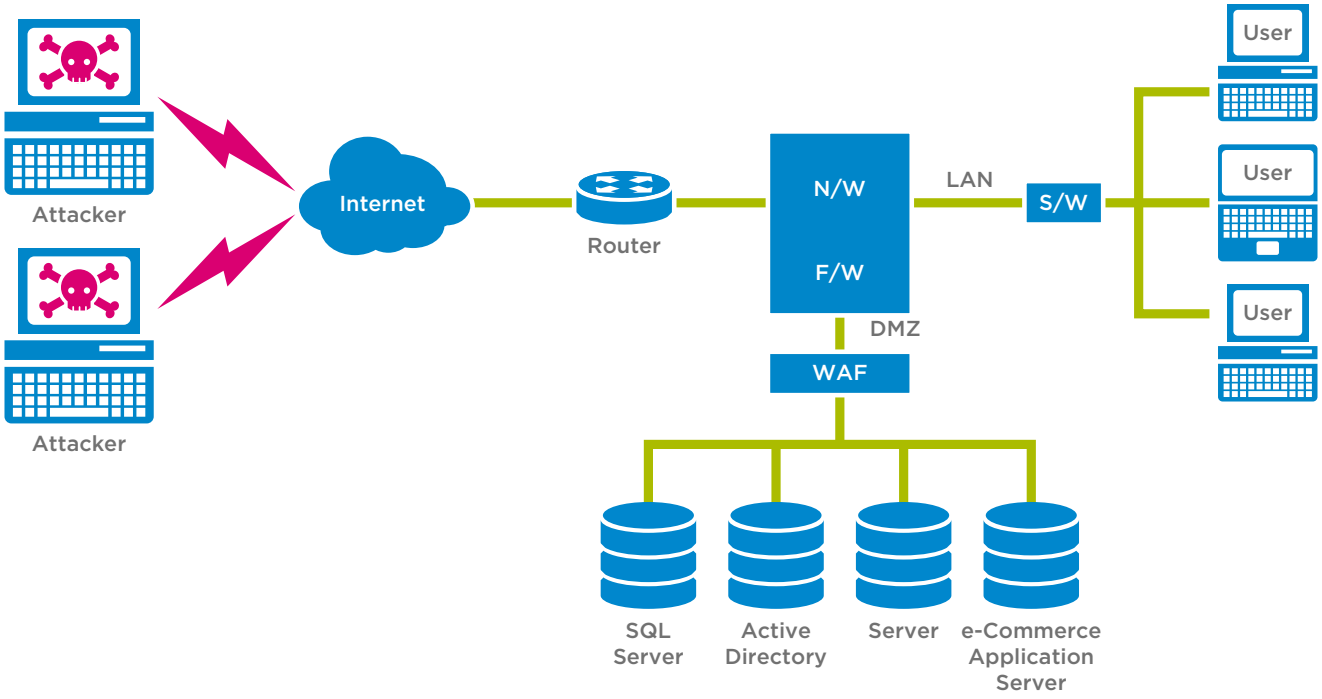
Organisations today rely heavily on web applications for supporting their business processes and faster operations. Web applications are an integral part of the IT environment that connects customers, vendors, and employees but unfortunately it also a prime target for hackers and cybercriminals.

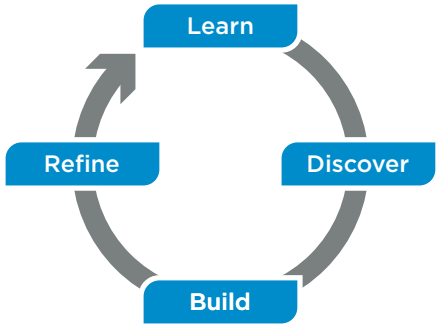
Hackers are increasingly using exploits to gain unathorised access to applications with the intent to pilfer data or to render the application inoperable thereby disrupting the company's operations. While traditional firewall appliances are able to perform an adequate job in scanning network traffic, evolving application level attacks require dedicated measures for higher security.

What is Web Application Firewall?

A Web Application Firewall is a device with ability to analyze Layer 7 application traffic. Unlike generic firewalls, a WAF is specifically 'tuned' to monitor only the target applications, inspecting all inbound and outbound application traffic, including encrypted traffic (https traffic).

Due to the dynamic nature of web applications, WAF's need to be continuously managed and regularly tuned in order to recognize and monitor appropriately traffic. This often calls for trained manpower for ensuring a balance between availability and security.





Building Security Policies — Process Lifecycle

Tata Communication Managed Web Application Firewall

Tata Communications' extensive experience in delivering managed security services coupled with a pervasive global Tier 1 network, allows us to provide support for WAFs during the complete lifecycle for

- Solution and design deployment
- On-going policy tuning and configuration management
- Real-time monitoring and analysis
- Security and compliance reporting

Service Features

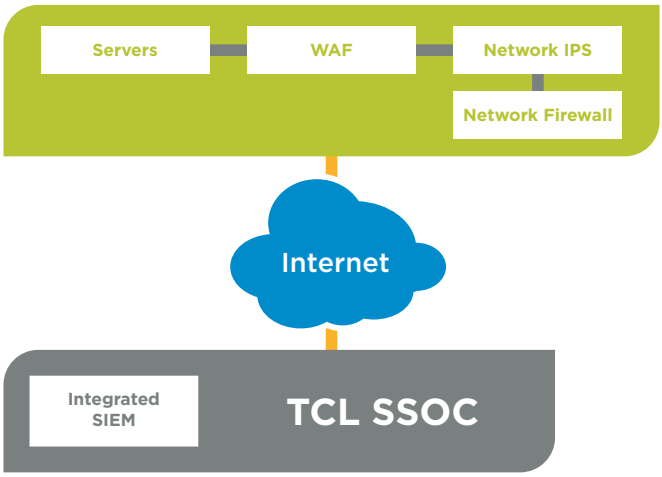
- Advanced web application security including coverage of OWASP Top 10 web application attacks
- Inspection of all inbound and outbound application traffic including encrypted traffic
- Facilitates compliance with PCI DSS requirements
- 24x7 remote monitoring from N+1 redundancy SoC's (Security Operations Center) ensuring WAF is always on and performing optimally
- Pre-integration with SIEM (Security Incident and Event Monitoring) platform for log management and correlation
- Detailed report and analytics via online portal
- Protects websites from hacking, by blocking harmful requests
- Counter emerging threats and 0Day attacks
- Complements network security devices such as IDS/ IPS
- Supported platforms: Imperva — Secure Sphere, Radware — Appwall, F5 — ASM, Fortinet — Fortiweb, Barracuda

Benefits of the service

- Lower TCO (Total Cost of Ownership) and high ROI by leveraging Tata Communications' MSSP expertise & rich experience
- No CAPEX as all hardware, licensing, support and monitoring costs are combined in to a monthly OPEX based pricing
- Reduced learning curve as you only require minimal expertise for tuning and maintaining, while our security experts handle the rest

Customer Portal
- Real-time Visibility
- Exhaustive Reporting for Compliance and Security

SSOC Facilities
- 24x7 SOC with Real-time Monitoring
- Certified Security Experts
- Integrated SIEM for Log Management and Correlation Analysis



Deployment and Management
- Solution Design
- Policy Tuning
- Continuous Monitoring and refinement
- Inspection of Encrypted Traffic
- Protection against OWASP Top 10 Web Application Attacks