Service Datasheet
Security Services

Executive Summary

Maxtel's Security service provides organizations with comprehensive protection designed to safeguard infrastructure, data, and operations in an increasingly complex digital landscape. We combine cutting-edge technologies, continuous monitoring, and advanced cybersecurity practices to ensure every layer of your technology environment is protected against internal and external threats. Our approach is based on a unified security architecture, where prevention, detection, and response operate in full coordination. This enables companies to minimize risk, strengthen operational resilience, and comply with local and international regulations, without adding operational burden to internal teams. North, Central and South America (except Brazil, Nicaragua, Cuba, and Haiti), using our data centers in:

Key Features

- Advanced perimeter security: Next-generation firewalls (NGFW), intelligent filtering, granular traffic control, and threat protection.

- Network protection and segmentation: VLAN/VRF isolation, Zero Trust policies, deep packet inspection, and detection of anomalous behavior.

- Identity and Access Management (IAM): Integration with SSO, MFA, LDAP, OIDC, and role-based access control (RBAC).

- Application and API security: OWASP attack mitigation, WAF protection, rate limiting, and validation of critical traffic.

- Data protection: Encryption in transit and at rest, data classification, access audits, and data loss prevention (DLP).

- Security for hybrid and multi-cloud environments: Consistent policies across public clouds, private clouds, container platforms, and colocation environments.

- Incident response: Root-cause analysis, containment, and assisted recovery.

- 24/7 monitoring and alerts: Continuous detection through SIEM/SOAR, event correlation, and intelligent alerting.

Business Benefits

- Greater operational resilience, reducing the risk of disruptions due to attacks or breaches.

- Full visibility into threats, access activity, and anomalous behavior across your infrastructure.

- Lower internal complexity, with security fully managed by experts.

- Adaptive protection for traditional, cloud-native, container-based, and microservices architectures.

- Assured compliance with consistent policies and up-to-date documentation.

- Cost reduction by avoiding investments in multiple tools, equipment, or specialized personnel.

- Immediate response capability, mitigating incidents before they generate business impact.

Datacenter