airtel business

Ease Your Network Security Burden with

Airtel's Security Device Management Service

airtel business

Airtel Secure

The Roadblocks **to Becoming Cyber Resilient**

Can your enterprise network withstand attacks of any magnitude? Even the best firewalls can fall to repeated and targeted attacks. Setting up a robust security perimeter has become necessary to nip potential disasters in the bud. Keep reading to understand why perimeter security is vital to your business, why you should test it before someone else does, and how can you secure your network boundary.

Cybersecurity threats are expected to cause massive financial and reputational losses to businesses in the coming years. The start of 2019 alone witnessed the leak of over 1.76 billion records, many of these through compromised networks.

To secure themselves, organizations are investing in perimeter security devices such as intrusion detection and prevention systems (IDS/IPS), unified threat management (UTM) systems, and firewalls. But threats often take advantage of internal vulnerabilities like missed security patches and configuration gaps. As such, deploying perimeter security devices, while essential, may not be enough to achieve effective network security.

Organizations need to constantly monitor a multitude of factors — managing security devices, updating policies and signatures, maintaining updated threat intelligence on external elements like zero-day threats, and compliance with industry-specific security standards.

Tasks for the IT support team often include:

- Real-time monitoring
- Vulnerability identification and patching
- Configuration backup and maintenance
- Device configuration per guidelines
- Performance and availability management
- Continuous device management and maintenance
- Regularly updating devices with relevant threat intel

Challenges faced by organizations include:

- Lack of skilled resources with adequate knowledge of cyber threats and new developments
- Limited visibility into the impact of changes made to security device policies
- Inadequate access to latest threat intelligence

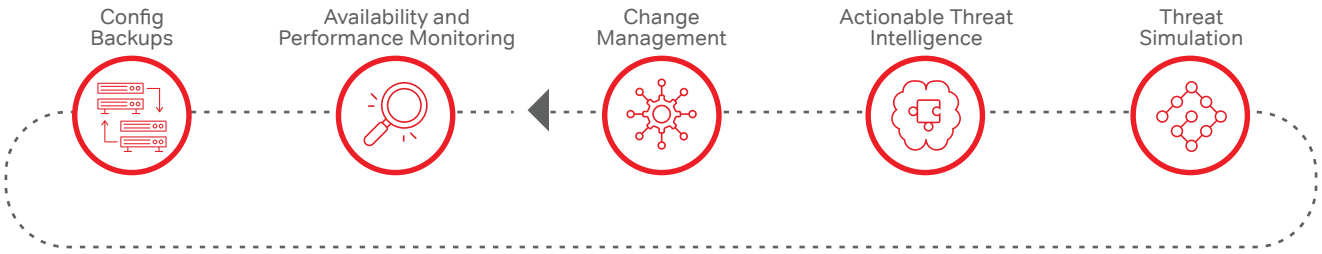
So how do you keep these external challenges at bay? By leveraging Airtel's end-to-end security solutions, while you focus on what's important – your business goals.

1. **IT Governance Blog,** https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-january-2019-1769185063-records-leaked
2. **CSO Online,** https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Airtel Security Device Management (SDM): **A Holistic Solution**

Our SDM services are designed to safeguard your business' privately owned network by creating a security perimeter. This means you are prepared for all your security needs, from compliance to advanced threat detection using next-generation technologies.

Gain complete ownership over your security device management lifecycle, encompassing:



Enhance Security Framework **with Extensive Compatibility**

Airtel SDM supports your existing network security infrastructure from Day Zero and ensures compatibility with various security point solutions and devices including:

Firewalls

FORTINET
JUNIPER NETWORKS
Check Point SOFTWARE TECHNOLOGIES LTD
CISCO
paloalto NETWORKS

UTM Devices, NextGen Firewalls and Specialist Devices

paloalto NETWORKS
FIREEYE™
SONICWALL™

IPS/IDS

SOURCEfire
SNORT
hp TippingPoint
PROVENTIA
Check Point SOFTWARE TECHNOLOGIES LTD
CISCO

Choose the plan that works for you:

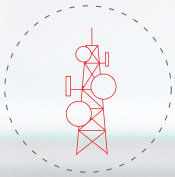
Features	Secured	Advanced Secured
Device health status check	✓	✓
Warranty status check	✓	✓
Change management	✓	✓
Configuration backup	✓	✓
Threat intelligence	✓	✓
Threat simulation		✓
Threat intelligence consumption		✓

Why Choose **Airtel**?

Stay ahead of security threats as we manage and reconfigure your security devices in line with your service requests and identification of security incidents. By choosing Airtel, you can leverage our:

Robust Infrastructure

- Industry-leading security specialists and cutting-edge infrastructure
- Strong vendor partner ecosystem
- Largest integrated SOC-NOC operating in the APAC to accommodate growing regional needs for managed services

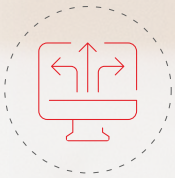


Vast Telecom Experience

- Third largest automated self-securing telecom assets
- Zero tolerance towards threats
- Highly regulated environment
- Stringent policy adoption and compliance

Strategic Partnerships

- Partner network of leading global security OEMs
- Customized effective B2B solutions for customers across verticals and market segments
- Base platform built using best-in-class technologies from ServiceNow, SolarWinds, Palo Alto, and more



Complete Ownership, Seamless Delivery

- End-to-end SLA-backed solutions
- Encompass all aspects from network security to last-stage device management
- Uninterrupted service with professionals working 24*7*365
- Focused business vertical to build world class infrastructure for clients

Global Recognition

- Certified Ethical Hacker (CEH) certification awarded by the EC Council
- Certified Information Security Manager (CISM) awarded by the Information Systems Audit and Control Association (ISACA)
- Recognized as Certified Information Systems Security Professional (CISSP) by (ISC)², a leading IT and cybersecurity organization

To know more visit: https://www.airtel.in/business/b2b/cyber-security

Write to us at: airtelforbusiness@airtel.com

Get in touch with your Airtel account manager