Data sheet

Security | India

Zero Trust Solutions

The next-generation approach to enterprise security

Our Zero Touch Solutions secure your backbone DNS and enable “need-to-know” access and monitoring, **Nalong with secure application access, enabling improved control and compliance.**

Service overview

Traditional security principles trust everything inside the organization’s protected area or perimeter, and distrust anything from outside. But with new business models, it’s difficult to set these boundaries. A highly mobile workforce and borderless technologies like cloud are forcing organizations to adopt a zero trust approach to security.

Our Zero Trust Solutions include secure application access, securing your backbone DNS, and solutions that enable need-to-know access and monitoring.

A **highly mobile workforce** and borderless **technologies like cloud** are forcing organizations to **adopt a zero trust approach** to security.

Key features

Privileged Identity Management Service

Improve control and compliance by monitoring privileged activities.

Misuse of privileged user IDs can prove costly– which is why compliance requirements are becoming more stringent across the industry. With our Privileged Identity Management Service, you can minimize data breaches and outages associated with uncontrolled access, reduce your risk of exposure to abuse or error, and improve control and compliance.

We work with you to create, implement and enforce privileged account security policies to:

- Protect against unauthorized use of privileged ID
- Isolate and control uncontrolled access and sessions
- Lower or optimize the total cost of ownership (TCO) for your enterprise password vault solution

The service also includes maintaining tamper-proof logs of user access and 99.95% availability of our privileged identity management infrastructure.

Enterprise Application Access

Limit user and device access to reduce the risk of attack.

The definition of a “user” has evolved to mean much more than an employee in an office. It now also include endpoints, contractors, mobile workers and newly acquired employees of an acquisition. But legacy network security tools haven’t kept pace with changes that affect secure access, leaving organizations vulnerable to attack from formerly trusted users.

Enterprise Application Access is a unique cloud architecture that closes all inbound firewall ports, while ensuring that only authorized users and devices have access to the specific internal applications they need, instead of the entire network. It enables:

- Fast and secure access to internal apps over the internet
- Application delivery and security architecture transformation based on zero trust principles
- Unified access with single sign-on (SSO) across on-premises, IaaS and SaaS applications
- DevOps and user acceptance testing (UAT) access for remote employees without the need for a virtual private network (VPN)
- Application modernization/ migration to IaaS for any internal HTTP/S application

Database Activity Monitoring (DAM) as a Service

Quickly identify data risks to protect against internal and external threats.

To detect unauthorized actions or suspicious activities by privileged insiders and potential hackers, our DAM as a Service continuously monitors all data access in real time, giving you:

- Complete visibility and granularity across databases
- A secure audit trail to support segregation of duties
- Real-time security alerts through integration with our security information and event management (SIEM) platform
- Customizable compliance workflows and built-in reporting

In addition, quick and multiple deployment options and out-of-the box integration help to reduce TCO.

User behavior analytics

Detect insider threats by identifying abnormal user behavior.

User behavior analytics assesses user activity to detect malicious insiders and determine if a user's credentials have been compromised.

As an integrated component of the security intelligence platform, user behavior analytics leverages out-of-the-box behavioral rules and machine learning (ML) models to add user context to network, log, vulnerability and threat data to detect attacks quickly and accurately. It's built on top of the app framework to use existing data in SIEM to generate new insights.

This allows security analysts to:

- Easily identify risky users and view their anomalous activities
- Drill down into the underlying log and flow data that contributed to a user's risk score
- Automate compliance and auditing
- Vulnerability assessment; encryption: data at rest

> Enterprise Threat Protector is a **cloud-based secure web gateway** that helps security teams **ensure that users and devices can safely connect to the internet,** regardless of where they're connecting from, **without the complexity** of legacy approaches.

Enterprise Threat Protector

Safely connect users and devices to the internet.

The volume and sophistication of targeted threats continues to grow dramatically. Users want internet access from everywhere, and organizations are struggling to keep pace with this new threat landscape. If you have an emerging approach to security, you need to quickly deploy robust and effective security solutions that do not require disruptive changes to your network and need minimal management.

Enterprise Threat Protector is a cloud-based secure web gateway that helps security teams ensure that users and devices can safely connect to the internet, regardless of where they're connecting from, without the complexity of legacy approaches.

Recursive DNS combined with industry-leading threat intelligence provides an additional layer of protection for on- and off-network. And, because it's an entirely cloud-based solution, it can be configure and deployed globally in minutes, with no disruption for users.

Enterprise Threat Protector can:

- Identify and block access to malicious domains, and prevent access to inappropriate content
- Offer proactive protection against malware, phishing and DNS-based data exfiltration
- Enforce acceptable use policies
- Improve security defenses by proactively blocking malicious communication and potential threats, effectively and consistently

Why NTT?

Extensive global track record

Our security specialists mitigate billions of security threats every year.

Financial stability

We're a leading global technology services company.

Superior client experience

Our clients benefit from comprehensive analytics, service delivery and ongoing process development.

Deep investment

We invest in innovative solutions and groundbreaking service development.

Get in touch

If you'd like to find out more about our Zero Trust Solutions, speak to your Client Manager or visit our website.