



Managed Security Services

Intelligent Security Gateway

Achieve secure digital transformation and secure hybrid working using zero trust; NTT ISG (Intelligent Security Gateway) enables business agility, compliance and protects organizations from emerging threats for every device at any location.

Challenge

Cloud and mobility are empowering digital transformation, and hybrid workplaces have quickly become the new normal. Digital transformation cannot be achieved without both network and security transformation. With that comes several challenges:

- Users require a seamless hybrid working experience and it must be secure
- There are more locations, devices (IT, OT, IOT) and applications than ever before.
- Shifting to a Zero Trust architecture is difficult with existing technology stacks
- The cloud and network attack surface is expanding
- The management and the monitoring of network and security products inhouse is becoming more complex and expensive

Secure Access Service Edge

With the advent of Secure Access Service Edge (SASE) the market has seen the convergence of Network and Security capabilities (such as FWaaS, SWG, CASB, ZTNA) into cloud delivered SASE solutions. SASE enables security teams to deliver a rich set of secure network-security services supporting digital business transformation, edge computing and hybrid working.

SASE can reduce security complexity through consolidation of security services leading to the reduction of technology stacks, whilst transforming to cloud-delivered security. SASE is a digital business enabler bringing speed, security and agility allowing secure access to applications, services, APIs and data from any location.

Value

- Secure hybrid working delivered seamlessly
- Cost and complexity reduction in technology and operational overheads across network and security
- NTT's dynamic block list provides rapid containment and disruption of threats
- Zero Trust access to applications, services, APIs and data
- Business agility with a scalable solution that evolves with the threat landscape

Approach

The NTT Intelligent Security Gateway (ISG) provides security capabilities in a SASE service further enhanced by NTT's 24x7 Threat Detection service, as well as management by NTT's policy-based security service. With the NTT ISG service, be transitioned to a cloud delivered Zero Trust architecture that supports hybrid working, business agility and digital transformation. NTT ISG fully managed service:

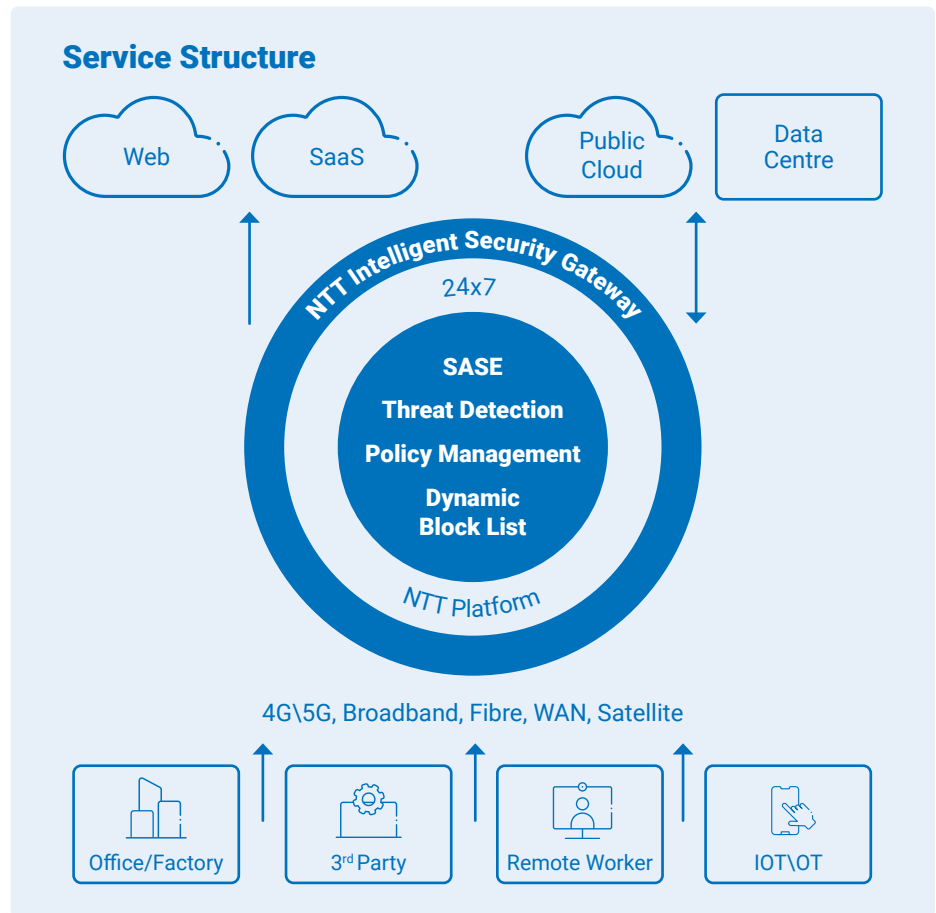
- Secures access to the internet including SaaS applications, which includes a cloud-delivered firewall
- Provides seamless zero trust access to private applications running on public cloud or within the datacentre.
- Includes advanced threat detection capabilities of the ISG and the NTT SOC

With ISG, organizations can detect and protect against advanced threats, monitor and enforce security policies and fulfill compliance reporting.

NTT SOC

All traffic transiting through the cloud delivered gateway generates logs and events that are analyzed by the NTT threat detection platform which includes machine learning and extensive threat intelligence.

Suspicious events are further analyzed by highly skilled NTT security analysts that investigate if the event is a false-positive or if it is a true security incident. Our security analysts leverage a rich set of tools and procedures for threat hunting to provide clients detailed incident reports for validated incidents with actionable recommendations and incident lifecycle support.



Make good detection even better

Our ISG service provides cloud security that supports your digital transformation:

- **NTT's Advanced Analytics** detects threats by combining our unique global threat intelligence and our extensive machine learning (ML) framework. We train ML models, extract features for new ML models, create behavior and pattern signatures and generate Indicators of Compromise (IOCs). Therefore, more security incidents are initially detected by our methods than by the native detection capabilities of any single technology. The addition of client event sources or an NTT Cyber Threat Sensor (CTS) further amplifies the detection capabilities.
- **NTT's Dynamic Block List** provides proactive and rapid response into ISG from NTT's extensive Threat Intelligence combined with human validated analysis, contains and disrupts threats.

- **Accelerated threat hunting** by security analysts uses a digital evidence sandbox combined with other log sources. Our analysts hunt for threats as they pivot from one piece of evidence to another until they find an attack path that leads to a security incident. Once an incident is validated, we provide an actionable incident report with recommendations and incident lifecycle support until the incident is closed.
- **Our certified security engineers provide security policy management** for the NTT ISG service that streamlines security policy design and enforcement. We apply rules and best practices effectively, efficiently and consistently. With our ISG you can enforce the same security policy and detect threats across today's hybrid working environment.

Empower your business

- Deliver higher user productivity through a seamless and secure hybrid worker experience
- Mitigate and control risks with protection against sophisticated threats supported 24x7 by expert NTT SOC analysts and engineers
- Achieve Zero Trust while reducing cost and complexity
- Increase business agility
- Fully managed outcome driven cloud service
- Increased visibility through the correlation of logs from all the NTT Services you make use of
- Policy management by certified security engineers
- Actionable security incident reports with clear recommendations

NTT Intelligent Security Gateway (ISG)

Cloud Delivered Services		NTT Security Operations Centre		
SASE Firewall	App. Visibility & Control	Highly-skilled analysts	Kill chain modelling	Event based hunting
Secure Web Gateway	IPS/Sandbox	Evidence data evaluation	Triage capabilities	Threat Intelligence
Cloud Access Security Broker	SSL Inspection	Policy management	Real-time correlation	Long-term correlation
Data Loss Prevention	ZTNA	Incident validation	Extensive ML training data	Zero-day detection
DNS Security	Browser Isolation	Incident investigation	Forensic analysis	Compliance reporting

Why NTT?




CREST Certified for Cyber Security Incident Response, Penetration Testing and SOC



Leader IDC MarketScape: Asia Pacific Cloud Security Services 2021 Vendor Assessment

- 
Global scale
 We deliver services in over 200 countries across five regions.
- 
Reduce business risks
 We mitigate two billion security threats every year.
- 
Full lifecycle
 Turn goals into outcomes through a lifecycle of services.
- 
Next-generation automation capabilities
 Access to comprehensive analytics, service delivery and process development.



Get in touch

To find out more or book an assessment, speak to your client manager or **contact us**.