

NTT Communications

IntelliSecurity™



Be Prepared

In today's digital world, your business is susceptible to an array of security threats. There's no question about that. But these threats are often preventable, and there's no reason not to be protected.

At NTT Communications, we offer IntelliSecurity™. It's our complete suite of security solutions. It's proactive, not reactive, security. And that's the way it should be.

We evaluate your current situation and architect your security plan, based on your unique needs. We provide you with our flexible, state-of-the-art security solutions and then we manage those solutions for you. Assess. Detect. Prevent. Sustain. It's our NTT Communications methodology and security management process, designed to keep you secure.

ASSESS: WE'LL FIND YOUR SECURITY VULNERABILITIES

NTT Communications conducts a comprehensive analysis of your security situation. We perform a risk assessment, detailing all of your internal and external security weaknesses, and then we program a plan of action to raise your security level. We can make minor changes to ensure your security meets compliance requirements, or we can do an entire upgrade.

Our Assessment services include:

IntelliSecurity™ Risk Assessment

- Light Penetration Test
- Full Penetration Test
- Vulnerability Scan
- Information Security Assessment

Deployment Consulting Services

IntelliSecurity™ Compliance Assistance

- Protection Policy and Standards Development
- Network Security Architecture Design
- Regulation assistance, including:
 - Gramm-Leach-Bliley Act
 - HIPAA
 - Sarbanes-Oxley Act
 - California Senate Law No. 1386
 - Industry Best Practices (SCADA Systems and Code of Federal Regulations)

NTT Communications

IntelliSecurity™



DETECT: EXPERT, REAL-TIME RESPONSES TO QUICKLY IDENTIFIED THREATS

Once your assessment is complete, the highly trained security experts at NTT Communications will present you with a cost-efficient solution for your security troubles. From simple Firewall implementation to full-scale, integrated plans, NTT Communications will provide the best solution for your security needs. Once our cutting edge technology is in place, we'll notify you at the first sight of suspicious activity. It's reliability. It's control. It's protection.

Our Detection services include:

Managed Firewalls, including IPv6

Intrusion Detection

IntelliSecurity™ SecureEntrance

PREVENT: WE'LL REINFORCE YOUR AREAS OF WEAKNESS

Our assessments often reveal large security gaps that, if exposed, can cost thousands or even millions of dollars. At NTT Communications, we believe that prevention is key. That's why we offer a full suite of Managed Protection services. We'll protect your business, before an incident even occurs. If you choose to increase your level of protection, our experts can custom configure an Intrusion Prevention Service to fit your needs. Beyond that, you can activate additional services through your interactive IntelliSecurity™ service web portal. View device status, read analyst log commentary, and communicate directly with the experts. It's all at your fingertips with NTT Communications.

Our Prevention services include:

Intrusion Prevention

Anti-Virus

Anti-Spam

Content Filtering

Virtual Private Networks (VPN)

NTT Communications

IntelliSecurity™



SUSTAIN: WE'LL KEEP YOUR SECURITY UP-TO-DATE

NTT Communications' IntelliSecurity™ services don't only manage your security system — they constantly update and upgrade as new threats emerge. As your business grows and changes, we'll provide new security measures to meet your demands and to keep up with industry best practices. In fact, we've already developed an added security layer for IPv6 solutions. We'll also provide emergency response services, as needed. From assessment to management, NTT Communications is your partner. We want you to be confident that your data network is fully secure.

Our Sustainment services include:

IntelliSecurityER

- Basic Emergency Response Services
- Comprehensive Emergency Response Services

INTELLISECURITY™ SERVICE DEFINITIONS

Signature Updates (IPS Only): NTT Communications' IntelliSecurity™ will apply all IPS signatures as they are released from the manufacturer and verified stable by NTT Communications' IntelliSecurity™.

Patch/Update Maintenance: Vendors release service patches and updates to their platforms from time to time. NTT Communications' IntelliSecurity™ tracks these releases, tests the updates, and determines the application of these patches/updates to our customer base. For customers who require the updates, NTT Communications' IntelliSecurity™ schedules and applies them. Updates that require greater than 2 hours of technician time will be presented to customers for application at an additional charge.

OS Revision Control: NTT Communications' IntelliSecurity™ maintains consistent revisions of all the devices across a customer's managed environment. When patches/ upgrades are required for a customer, the resulting OS revision is duplicated across the entire customer environment to maintain consistency.

Configuration Backup: Managed devices are regularly backed up to protect against configuration corruption. At a minimum, the last 5 configuration revisions are stored by NTT Communications' IntelliSecurity™ for disaster recovery in the event of device failure.

NTT Communications

IntelliSecurity™



Fault Monitoring: All monitored devices are regularly checked to ensure they are still online and functioning properly. When a negative or failed response is received, customers are notified that their hardware is in a down state.

Maintenance Contract Control: NTT Communications' IntelliSecurity™ will track the maintenance agreement and notify the customer when it's time to renew (for customer provided equipment) or automatically renew the agreement for NTT Communications' IntelliSecurity™ provided equipment.

Hardware Vendor Management: When equipment fails altogether, NTT Communications' IntelliSecurity™ has management categories that provide management of the vendor maintenance agreement to have hardware replaced. The timing of the replacement is entirely dependent upon the maintenance selected by the customer. NTT Communications' IntelliSecurity™ works on the customer behalf to ensure the equipment is replaced in the most expedient fashion possible.

Security Service Reports: NTT Communications' IntelliSecurity™ collects syslog information from every monitored device in a customer's infrastructure. This information is passed to the NTT Communications' IntelliSecurityView reporting system and made available for online review. Multiple reports are generated against the specific platform and services being monitored. Report details are presented within the Service Description of each individual service.

Security Event Validation: When an event is discovered, an NTT Communications' IntelliSecurity™ security engineer will validate the event to ensure it is "real". This process is limited for Monitoring-only customers because administrative access is not available. When events are validated, notification begins.

NTT Communications

IntelliSecurity™



Security Event Notification: Validated events result in customer notification. Notification provides customers with details about the security event. Monitoring-only customers must then determine their own course of action to respond. Management customers will receive remediation assistance.

Security Event Remediation: For Management customers, validated events will result in a recommended course of action. NTT Communications' IntelliSecurity™ presents this recommendation and gains customer consent to make all the necessary and appropriate changes. Should a customer desire a different course of action, NTT Communications' IntelliSecurity™ will work with customer recommendations and security best-practices to rapidly determine the most agreeable response.

Change Request Validation: When customer business requirements or network modification result in managed service configuration changes, NTT Communications' IntelliSecurity™ receives these change requests and validates that implementing the change does not conflict with the security best-practices, nor will it have a negative affect on customer traffic.

Change Request Application: Once change requests have been validated, NTT Communications' IntelliSecurity™ will apply the changes in alignment with NTT Communications' IntelliSecurity™ SLAs.

Contact us today to get started.

Phone: 1-877-8-NTT-NET

Email: Sales@us.ntt.net

Web: www.us.ntt.net

NTT America, NTT Communications, the NTT Communications logo are trademarks and/or service marks of NTT Communications in the United States and other countries. ©2008 NTT America. All rights reserved.



NTT America