SERVICE GUIDE

Cybersecurity Services

Alpha Next Inc.

2026 Edition | English Translation

Cloud infrastructure. Cybersecurity. Digital transformation.

ALPHA NEXT

https://blog.wodedmxy.com/

Service Overview

Cybersecurity Solutions

As cyberattacks become more sophisticated, ongoing investment in security is essential. We provide layered defenses, from vulnerability assessments and penetration tests to zero-trust architecture, EDR and SIEM operations, round-the-clock staffed SOC monitoring and incident response with CSIRT support.

Assessments	Web application and platform vulnerability assessments, with findings prioritized by impact and urgency.
Zero trust	Identity-based access design and phased deployment, reducing VPN dependence without assuming immediate removal.
SOC monitoring	24/7 staffed monitoring and first response through two domestic operating locations.
Backups	Retention design, immutable storage separation and recurring recovery exercises.
Training	Targeted-email exercises and incident-based workshops, designed to encourage reporting without blame.

How We Deliver

01 Discovery	We discuss your environment, challenges, budget and schedule. Initial consultation is free.
02 Proposal	We present suitable solutions, indicative costs and options for comparison.
03 Implementation	A dedicated team designs, builds and develops the solution, with regular progress meetings.
04 Testing & migration	We plan quality assurance and production migration to minimize business disruption.
05 Operations	We provide ongoing monitoring and improvement to support long-term reliability.
06 Improvement	We analyze operational data and recommend the next practical steps.

Costs and Engagement

Requirements discussions and initial quotations are free. Detailed assessments, when needed, are quoted separately. Implementation projects use individual contracts. Managed services have a minimum 12-month term, followed by monthly cancellation options.

Implementation payment terms are normally 30% at commencement and 70% on acceptance. Managed-service fees are normally due at the end of the following month. Requirements and terms are agreed individually.

The website's cost estimator provides indicative JPY ranges rather than a quotation. Actual scope, permissible downtime and internal resources affect final costs.

Assessment Delivery

We confirm scope, permitted testing windows and emergency contacts before testing. Remote assessments generally take three days to two weeks, depending on scope. Reports classify findings into three severity levels. A 90-minute online review meeting explains the results; retesting corrected items is available as an option.

Cybersecurity - Questions & Answers

Q How often should vulnerability assessments be performed?

It depends on how frequently the system changes. An annual assessment may suit a system with only a few releases each year. For continuous delivery, we recommend automated checks in the release process, with an annual external assessment as an independent review.

Q Does zero trust eliminate the need for a VPN?

Reliance on a VPN can be reduced gradually, but immediate elimination is uncommon, particularly where legacy business systems support only older connection methods. We start with workloads that can work without the VPN and reduce dependency in stages.

Q What is the first step in preparing for ransomware?

Test restoring your backups. Having a backup that cannot be restored is not unusual. Then check that the backup environment cannot be affected alongside production.

Q What incident response support do you provide?

For managed-services clients, we handle detection, initial response and assessment of the affected scope. Legal responses and disclosure decisions remain with the client; we help establish the technical facts.

Q Can you provide employee training?

We offer targeted-email exercises and workshops based on real incidents. Exercises are designed without blaming participants, with the aim of creating an environment where people can report concerns easily.

Selected Case Studies

Zero-trust infrastructure enabled secure access to business systems from outside the office

We moved to identity-based access control to address VPN congestion and gaps in removing former employees' access rights.

Concurrent VPN connections	Access-review workload	Former employees' accounts remaining active
1,400 to 210	**40 hours/month to 6 hours/month**	**Average 11 days to same day**

Redesigning ransomware-resilient backups established a four-hour recovery objective

Following an incident elsewhere in the healthcare sector, we redesigned backup retention and recovery procedures. Recovery drills confirmed restoration within the target time.

Recovery time objective (RTO)	Recovery drills	Backup protection
Previously undefined to 4 hours	**Scheduled twice a year**	**100% immutable storage**

Embedding routine e-commerce vulnerability checks into the development and release process

We replaced a model based solely on annual external assessments with continuous security checks throughout development.

Detection before production	Findings in external assessments	Pre-release checks
0% to 78%	**64% fewer year over year**	**Run automatically for every release**

Results are measurements from individual client environments and do not guarantee equivalent outcomes.