IT Infrastructure Setup and Maintenance

Prepared for: **Mr. Casper Tvede, Mr. Keita Kawasaki, Kysmaq**

Date: January 27, 2026

Dear Kysmaq Leadership Team,

Thank you for taking the time to discuss your IT modernization goals with us. We understand the challenges you're facing—email security vulnerabilities, fragmented systems, and the friction of coordinating DNS changes through NTT.

We're pleased to present our proposal for **M365 Security Essentials plus Cloudflare Protection** closely followed by **Ongoing IT Support**, designed to address your immediate security concerns while laying the foundation for a modern, manageable IT environment.

What this means for Kysmaq:

- Your staff can work confidently knowing email phishing and spoofing threats are blocked before reaching their inbox
- Your website gains protection against attacks without requiring constant NTT coordination
- You gain direct control over your DNS, eliminating delays and dependencies
- Your team of 11—including your two roaming sales staff—can collaborate seamlessly with proper M365 licensing

We've structured this as a phased approach, beginning with the security and infrastructure fundamentals that will protect your business and enable future improvements.

We look forward to partnering with you on this journey.

Respectfully,

Rick Cogley
eSolia Inc.

Scope

Secure Kysmaq's email and web infrastructure, establish DNS independence, and prepare the environment for full Microsoft 365 adoption. Provide ongoing IT professional visits for user support and planning next steps.

Introduction

eSolia is a Tokyo-based B2B IT professional services firm. Since 1999, we have provided bilingual IT support to international companies operating in Japan, functioning as their local IT department with the same skills and expertise as a dedicated in-house team.

What sets us apart:

- **Team-based approach** — We never dispatch single engineers. Our team provides comprehensive coverage across helpdesk, infrastructure, security, and project management.
- **Bilingual professionals** — Native-level English and Japanese communication, bridging headquarters and Japan operations seamlessly.
- **25+ years of experience** — Established operational processes, thorough documentation, and proven track record with multinational clients.
- **Vendor neutral** — We recommend solutions based purely on your needs, not vendor relationships.

We focus on solving your problems, not just providing IT services. Our mission is to deliver practical, durable solutions while maintaining the highest standards of professionalism and confidentiality.

Thank you for the opportunity to present this proposal.

— eSolia Inc.

M365 Security Essentials

Foundation-Level Protection for Modern SMBs

Service Package: M365 Security Essentials + Cloudflare Protection
Target Audience: SMBs (10-100 employees) with Microsoft 365 Business Premium
Implementation Time: 2-3 weeks
Regular DNS and Email Security Monitoring: via eSolia Periodic

---

The Challenge

Your business runs on Microsoft 365 and cloud services. But out-of-the-box settings leave critical gaps that attackers actively exploit—misconfigured email authentication, exposed admin accounts, and endpoints connecting from anywhere without verification.

Think of it like moving into a new office building: the doors lock, but you haven't installed the security cameras, programmed the access cards, or set up the alarm system.

This package activates your *digital security system*.

What You Get

1. Microsoft 365 Business Premium Hardening

We configure the security features already included in your license—features that protect nothing until properly set up.

Security Control	What It Does	Business Impact
Multi-Factor Authentication (MFA)	Requires phone verification for all sign-ins	Blocks 99.9% of account compromise attacks
Security Defaults Optimization	Enforces baseline protections across all users	Eliminates common configuration gaps
Admin Account Protection	Dedicated, MFA-enforced admin accounts	Prevents privilege escalation attacks
Legacy Protocol Blocking	Disables outdated authentication methods	Closes backdoors that bypass MFA
Conditional Access (Basic)	Location and risk-based access policies	Blocks suspicious sign-in attempts automatically
Defender for Office 365	Anti-phishing, Safe Links, Safe Attachments	Catches threats that basic filtering misses
Data Loss Prevention (Basic)	Prevents accidental sharing of sensitive data	Reduces compliance exposure
Audit Logging Configuration	90-day activity retention (default)	Provides investigation trail

Note on Advanced Features:
M365 Business Premium includes Intune for device management. Full device compliance policies, app protection, and endpoint configuration require Intune enrollment—a separate phase that takes 4-6 weeks for proper rollout. This package establishes your security foundation; Intune deployment is available as a follow-on engagement.

Features requiring Intune (not included in this package):

- Device compliance enforcement in Conditional Access
- Mobile Application Management (MAM) policies
- Windows Autopilot device provisioning
- BitLocker enforcement and recovery key management
- Endpoint configuration profiles

---

2. Cloudflare Pro + DNS Migration

Your domain is your digital identity. We migrate DNS management to Cloudflare, adding enterprise-grade protection to your existing website and email infrastructure.

Capability	What It Does	Business Impact
DNS Zone Protection	DDoS mitigation, DNSSEC signing	Prevents domain hijacking and DNS attacks
Website Security	WAF rules, bot management, SSL/TLS	Protects public-facing web properties
Performance Optimization	Global CDN, caching, image optimization	Faster site for visitors worldwide
Always Online™	Cached version during origin failures	Maintains availability during outages
Analytics & Insights	Traffic patterns, threat intelligence	Visibility into who's accessing your domain

Migration Process:

1. Audit current DNS records and TTLs
2. Replicate zone in Cloudflare
3. Coordinate nameserver cutover (minimal downtime)
4. Verify all services resolve correctly
5. Enable security features progressively

---

3. Email Security Configuration (SPF, DKIM, DMARC)

Email spoofing is trivially easy without proper authentication. We implement the full email security stack—configured for maximum protection, not just "passing" compliance checks.

Protocol	What It Does	Our Configuration
SPF (Sender Policy Framework)	Lists authorized sending servers	Strict `-all` policy (fail unauthorized)
DKIM (DomainKeys Identified Mail)	Cryptographically signs outbound email	2048-bit keys, proper selector rotation
DMARC (Domain-based Message Authentication)	Policy for handling failures	`p=reject` (ultimate goal), phased rollout

DMARC Rollout Phases:

1. **Week 1-2:** `p=none` with monitoring (collect data, identify legitimate senders)
2. **Week 3-4:** `p=quarantine` (suspicious mail to spam)
3. **Week 5+:** `p=reject` (block all unauthorized mail)

Why "p=reject" matters: Anything less lets spoofed emails through. Many implementations stop at `p=none` — which does nothing except generate reports.

---

4. Ongoing Monitoring via eSolia Periodic

Security isn't a one-time setup. We continuously monitor your configuration through our **Periodic** monitoring platform at periodic.esolia.co.jp.

Monitoring Area	Check Frequency	Alert Threshold
DNS Zone Integrity	Every 15 minutes	Any record change (A, MX, TXT, CNAME)
SSL/TLS Certificates	Every 15 minutes	Expiry <30 days, chain issues
Website Availability	Every 15 minutes	Downtime detected
Domain Reputation	Daily	Blacklist appearance
DMARC Report Analysis	Regular (typically daily)	Unauthorized senders detected

Monthly Reports Include:

- DMARC report summary (volume, pass/fail rates, unauthorized senders)
- DNS change log
- Uptime statistics
- Recommendations for improvement

---

5. Cloudflare Zero Trust (Endpoint Protection)

Traditional VPNs trust everything inside the network. Zero Trust verifies every connection, every time—without requiring full device enrollment.

Capability	What It Does	Business Impact
WARP Client	Encrypted tunnel for all device traffic	Protects data in transit everywhere
Gateway DNS Filtering	Block malicious domains at DNS layer	Prevents malware callbacks, phishing sites
Secure Web Gateway	HTTP/S inspection and policy enforcement	Blocks downloads from risky categories
Access Policies	Identity-aware application access	SaaS apps protected without VPN complexity
Device Posture (Basic)	OS version, disk encryption checks	Baseline security verification

Deployment Without Intune:
This package deploys WARP clients manually or via simple installer distribution. For automatic deployment, compliance enforcement, and advanced posture checks, Intune integration is recommended as a follow-on phase.

What's included:

- WARP client deployment to company devices
- Gateway DNS and HTTP policies
- Basic device posture rules
- Access policies for critical applications

What requires Intune (future phase):

- Automatic client deployment via MDM
- Strict device compliance enforcement
- Certificate-based device trust
- Conditional access integration

What Comes Next

This package establishes your security foundation. Common follow-on engagements include:

Phase	Focus
Intune Deployment	Full device management, compliance policies
E5 Security Upgrade	Advanced threat protection, insider risk
ISO 27001 Preparation	ISMS documentation, certification readiness
Incident Response Planning	Playbooks, tabletop exercises

eSolia IT Support Services

Reliable, professional IT support tailored to your organization's needs:

TotalSupport — Comprehensive Managed IT

Your virtual IT department. We handle all aspects of your IT operations:

- Help desk for end-user support
- System administration and maintenance
- Vendor management and coordination
- Project planning and execution
- Strategic IT consulting
- Regular reporting and reviews

Ideal for organizations that want to outsource IT operations entirely.

Co-Support — Collaborative Partnership

Work alongside your existing IT team:

- Augment your team's capabilities
- Provide specialized expertise
- Handle overflow and after-hours support
- Knowledge transfer and training
- Backup for vacations and absences

Ideal for organizations with internal IT that need additional capacity or expertise.

Support Delivery

- Bilingual support (English and Japanese)
- Business hours and after-hours options available
- Remote and on-site support
- Work tracking

eSolia's support team brings decades of combined experience supporting businesses in Japan, with deep knowledge of both local and international IT environments.

Next Steps

- **Review** — Review this proposal and let us know any questions
- **Discussion** — Schedule a call to discuss details
- **Agreement** — We prepare the MSA and SoW documents
- **Signatures** — Both parties sign
- **Kickoff** — Begin onboarding

We are flexible and can adjust scope and terms based on your feedback.

In Closing

Thank you for considering eSolia. We look forward to supporting your IT needs in Japan.

Please contact us anytime with questions.

eSolia Inc.

Tel: 03-4577-3380
Email: hello@esolia.co.jp
Web: https://esolia.co.jp/en
