Cyber Security
Monthly Report
OCTOBER 2026

SAMPLE REPORT · ALL DATA IS FICTITIOUS

Customer:	Example Manufacturing Co., Ltd.
Project name:	Managed Security Service
Product:	Cybersecurity Monthly Report
Reporting period:	1 – 31 October 2026

" Let ANS be your ANSWER "

Table of Contents

1. Document Control 3
2. Executive Summary 3
3. Asset Overview 5
4. EOL / EOS Status 6
5. Firmware & Software Status 7
6. Vulnerability Management (Quarterly) 8
7. Patch & Update Tracking 9
8. Security Monitoring / Incident Summary 9
9. Centralized Log Management 10
10. Configuration & Security Control Review 12
11. Recommendations & Next Steps 13

About this sample. This document shows the structure of the monthly report ANS delivers to Managed Security customers. Customer name, hostnames, IP addresses, serial numbers, user names and all figures have been replaced with fictitious data.

SAMPLE

1. Document Control

Date	Version	Author	Description
29-Oct-2026	1.0	ANS Security Team	Initial content / Final

2. Executive Summary

This month, all core network and security devices operated normally with no security incident that affected business operations. Two items need management attention: the virtualization host and backup server have passed vendor End-of-Support, and the hypervisor version is End-of-Life and no longer receives security patches.

53
Assets monitored

3
Tickets this month

4 / 5
Findings resolved

1
Critical open

System Health & Status

No.	Product	Hardware	Software	Firmware	Remark
1	**Next-Generation Firewall** 1 device	✓	✓	✓	
2	**Virtualization Host (2U rack server)** 1 device	!	✓	✗	Hardware EOS · Hypervisor EOL
3	**Backup Server** 1 device	!	✓	!	Hardware EOS
4	**Core Switch (stack)** 2 devices	✓	✓	!	Firmware update available
5	**Access Switch** 5 devices	✓	✓	✓	
6	**PoE Switch (Wi-Fi)** 1 device	✓	✓	✓	
7	**Wireless Access Point** 4 devices	✓	✓	✓	
8	**Endpoints (PC / Notebook)** 34 devices	✓	!	✓	2 legacy OS

✓ Normal ! Attention / plan required ✗ Action required

SAMPLE

Executive Summary (continued)

Key Findings

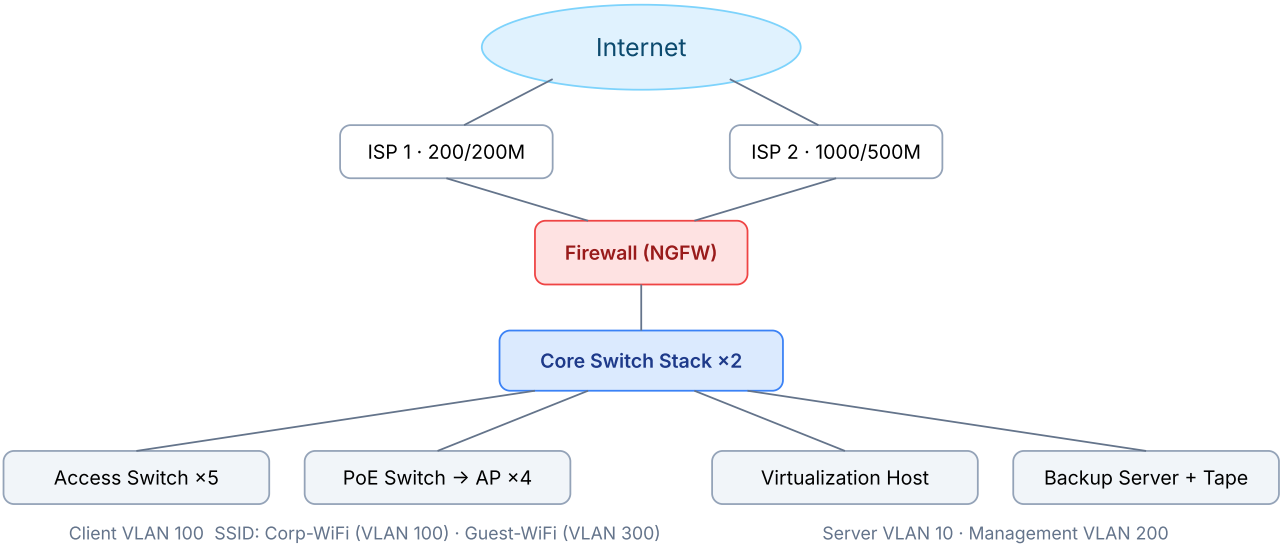
- **Hardware.** Resource utilization of all devices is normal. The virtualization host and backup server reached vendor End-of-Support; spare parts and warranty service are no longer guaranteed.
- **Hypervisor.** The current hypervisor version is End-of-Life and was flagged **Critical** in the quarterly vulnerability scan.
- **Firewall.** Running the vendor-recommended firmware. Antivirus and IPS signatures update automatically.
- **Backup.** Disk backup jobs completed successfully every day. The tape drive reported a hardware error and is awaiting vendor replacement.
- **Endpoints.** 2 of 34 machines still run an operating system that no longer receives security updates.

Recommendation Summary

Priority	Item	Recommendation	Target
Critical	Hypervisor EOL	Upgrade to a supported version or migrate to an alternative platform	Q1 2027
High	Server hardware EOS	Plan replacement, or move workloads to cloud	Q1 2027
High	Legacy endpoint OS	Upgrade or isolate the 2 machines	Next month
Medium	Core switch firmware	Schedule upgrade in maintenance window	Next month
Medium	Tape drive	Follow up vendor replacement (RMA)	In progress

SAMPLE

3. Asset Overview



Network & Server Devices

No.	Type	Hostname	Model	Serial
1	Firewall	FW-01	Next-Generation Firewall	XXXX-XXXX
2	Core Switch	CORE-SW-01	L3 Managed Switch 24G	XXXX-XXXX
3	Core Switch	CORE-SW-02	L3 Managed Switch 24G	XXXX-XXXX
4	Access Switch	ACC-SW-01...05	L2 Managed Switch 24G (×5)	XXXX-XXXX
5	PoE Switch	POE-SW-01	PoE+ Switch 24G	XXXX-XXXX
6	Access Point	AP-01...04	Wi-Fi 6 Indoor AP (×4)	XXXX-XXXX
7	Virtualization Host	VH-01	2U Rack Server	XXXX-XXXX
8	Backup Server	BK-01	Tower Server + LTO Tape	XXXX-XXXX

Endpoints & Virtual Machines

Operating System	Devices	Status
Windows 11 Pro	26	Supported
Windows 10 Pro (ESU)	6	EOS < 12 months
Legacy OS	2	End of Life

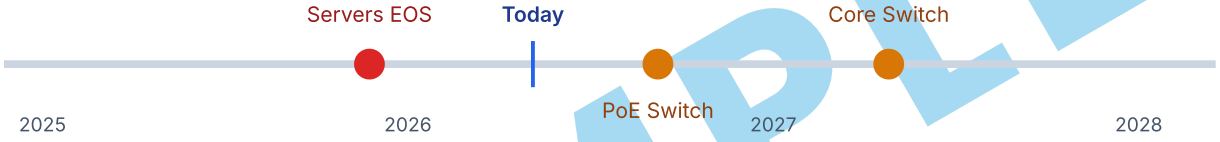
Virtual Machine	Role
VM-DC01	Domain Controller
VM-FS01	File Server
VM-AV01	Antivirus Console
VM-APP01	ERP Application

4. EOL / EOS Status

Devices past End-of-Support (EOS) no longer receive spare parts, warranty service or security fixes from the vendor. ANS tracks every asset so replacement can be budgeted in advance rather than after a failure.

No.	Product	Status	EOS date
1	Next-Generation Firewall	Supported	—
2	Core Switch ×2	EOS < 12 months	Q3 2027
3	Access Switch ×5	Supported	—
4	PoE Switch	EOS < 12 months	Q1 2027
5	Wireless Access Point ×4	Supported	—
6	Virtualization Host	EOS reached	Dec 2025
7	Backup Server	EOS reached	Dec 2025
8	Hypervisor software	End of Life	—

Lifecycle Timeline



SAMPLE

5. Firmware & Software Status

Firmware and software versions are compared each month against the vendor's recommended release, not simply the newest one, to balance security fixes with stability.

Component	Current	Recommended	Status
Next-Generation Firewall	11.1.x	11.1.x (recommended)	Up to date
Core Switch ×2	2.5.0	2.5.9	Update available
Access Switch ×5	4.1.7	4.1.7	Up to date
PoE Switch / Access Point	Auto update	Auto update	Up to date
Hypervisor	6.7	Unsupported	End of Life
Backup Software	12.3	12.3	Up to date
VPN Client	6.2.x	6.2.x	Up to date

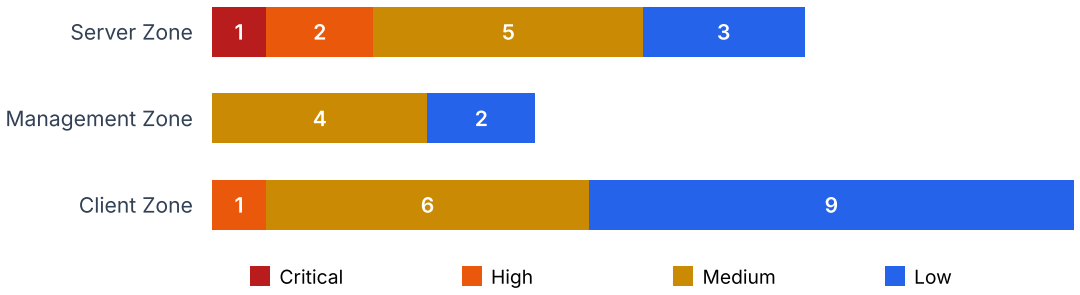
Security Signature Updates (Firewall)

Signature	Schedule	Last installed	Status
Antivirus	Daily 00:00	28-Oct-2026	✓
Application & Threat (IPS)	Weekly (Wed)	28-Oct-2026	✓
URL Filtering	Cloud lookup	Real-time	✓
Device Dictionary (IoT)	Weekly	29-Oct-2026	✓

SAMPLE

6. Vulnerability Management (Quarterly)

A full authenticated vulnerability scan is performed **every quarter**, plus an extra scan after major changes or when a critical vendor advisory affects the customer's equipment. This report contains the **Q4 2026** scan.



Severity Definitions & Target Remediation Time

Severity	Meaning	Target
Critical	Can be exploited remotely with little effort; may lead to full system compromise.	Within 7 days
High	Serious weakness; exploitation is likely if left open.	Within 30 days
Medium	Requires specific conditions or internal access to exploit.	Within 90 days
Low	Minimal impact; fix during normal maintenance.	Next cycle

SAMPLE

7. Patch & Update Tracking

No.	System	Zone	Finding	Severity	Action	Status
1	Hypervisor	Server	Version End-of-Life	Critical	Upgrade / migrate	Open
2	Legacy database server	Server	Unsupported version	High	Decommission	Resolved
3	Windows Servers (×6)	Server	Weak TLS cipher (SWEET32)	Medium	Disable 3DES cipher	Resolved
4	Firewall	Management	Default SNMP community	High	Change community / use SNMPv3	Resolved
5	Server BMC (IPMI)	Management	Service exposed on LAN	High	Restrict to management VLAN	Resolved

8. Security Monitoring / Incident Summary

Case No.	Date	Description	Type	Status
INC-0001	05-Oct-2026	Server room power strip could not supply all outlets; replaced with rack PDU	Implementation	Resolved
INC-0002	23-Oct-2026	Tape drive hardware error; vendor RMA opened (approx. 14 days)	Ticket support	Pending
INC-0003	29-Oct-2026	Vendor security advisory for VPN gateway; firewall firmware and VPN client updated	Ticket support	Resolved

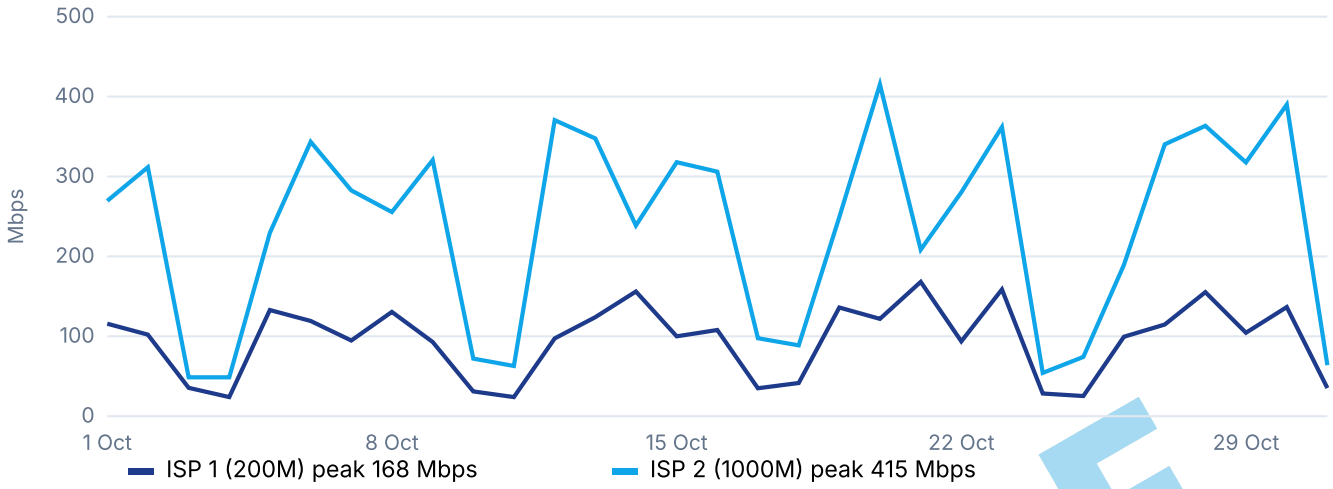
No malware outbreak, data leak or unauthorized access was detected during this period.

SAMPLE

9. Centralized Log Management

All firewall, VPN and network device logs are forwarded to the ANS Centralized Log platform and retained for at least **90 days**, in line with the Thai Computer-related Crime Act. Beyond compliance, the same logs show how the network is actually used.

Internet Bandwidth Usage



Usage follows working hours with low weekend traffic. ISP 1 peaked at 84% of capacity, so the current links are sufficient. No sustained saturation was observed.

SAMPLE

Centralized Log Management (continued)

Top URL Categories (Download)

#	Category	GB	Share
1	computer-and-internet-info	412.6	26.1%
2	social-networking	288.4	18.2%
3	search-engines	201.7	12.7%
4	content-delivery-networks	150.2	9.5%
5	business-and-economy	96.8	6.1%
6	streaming-media	71.3	4.5%
7	online-storage-and-backup	44.9	2.8%
8	medium-risk	18.6	1.2%

Note: "medium-risk" sites were allowed with logging; ANS recommends blocking this category for non-IT users.

Remote Access (VPN) Usage

User	Connections	Download (GB)	Source	Remark
user-01	4,812	2.3	Home ISP	
user-02	3,955	6.1	Home ISP	
user-03	2,140	0.9	Mobile	
user-04	1,702	0.4	Overseas	⚠ Verified with user (business trip)
ans-support	612	0.2	ANS SOC	Maintenance

Log & Backup Health

Check	Result
Log collection from all sources (12/12)	✓
Log retention ≥ 90 days	✓
Daily backup to disk	✓
Weekly backup to tape	✗ Tape drive under RMA

SAMPLE

10. Configuration & Security Control Review

Each month ANS reviews key security controls and keeps an off-device copy of every network configuration, so any device can be restored quickly after failure or misconfiguration.

No.	Control	Result	Detail
1	Firewall configuration backup (monthly snapshot)	✓	Snapshots kept: May – Oct 2026
2	Core switch configuration backup	✓	Stored encrypted, off-device
3	Administrator accounts review	✓	No unused admin accounts
4	Firewall policy review (unused / any-any rules)	!	2 unused rules proposed for removal
5	VPN multi-factor authentication	✓	Enabled for all VPN users
6	Guest Wi-Fi isolation	✓	Guest VLAN cannot reach internal networks
7	Management access restricted to management VLAN	✓	Verified after finding #5
8	Time synchronization (NTP) on all devices	✓	Required for accurate log timestamps

SAMPLE

11. Recommendations & Next Steps

1. **Replace or migrate the virtualization platform (Critical).** The host hardware is past EOS and the hypervisor is End-of-Life. Options: (a) new server with a supported hypervisor, (b) open-source virtualization to reduce license cost, or (c) move workloads to cloud. ANS can prepare a cost comparison.
2. **Upgrade or isolate legacy endpoints (High).** Move the 2 legacy-OS machines to a restricted VLAN until they are replaced.
3. **Upgrade core switch firmware (Medium).** Proposed maintenance window: Saturday after 18:00.
4. **Restore tape backup (Medium).** Follow up vendor RMA; until then, keep one extra copy of critical data on separate storage.
5. **Block "medium-risk" URL category (Low).** Apply to non-IT users after management approval.

Next Quarterly Vulnerability Scan

Scheduled for **January 2027**, followed by a re-scan of any Critical/High findings after remediation.

Absolute Network Solution Co., Ltd.
www.ansnetworksolution.com · LINE @anssolution
This sample report contains fictitious data for illustration purposes only.

SAMPLE