Centralized Logs Management

Monthly Report · October 2026

SAMPLE REPORT · ALL DATA IS FICTITIOUS

Customer	Example Manufacturing Co., Ltd.
Reporting period	1 – 31 October 2026
Log sources	Next-Generation Firewall
Prepared by	Absolute Network Solution Co., Ltd.

" Let ANS be your ANSWER "

Centralized Logs Management

Centralized Log Management คือระบบจัดเก็บ Log จากอุปกรณ์เครือข่ายทั้งหมดไว้ที่เดียว ให้ตรงตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (เก็บไม่น้อยกว่า 90 วัน) และยังใช้วิเคราะห์การใช้งานอินเทอร์เน็ต รวมถึงตรวจสอบความปลอดภัยของอุปกรณ์ต่างๆ ในองค์กรได้อีกทางหนึ่ง

Contents

1. Executive Summary
2. Summary Total Bytes
3. Top 10 Source IP
4. Top 10 Destination
5. Source & Destination Location
6. Top 10 URL Category
7. Top 10 Application
8. Top 10 Policy
9. Top 10 VPN User
10. Top URL – Allowed & Blocked
11. Threat Detection
12. High-Risk Events
13. Recommendations

Executive Summary

Online	100%	986 GB	2
Firewall log source	Log retention ≥ 90 days	Total download	High-severity events

- มีการใช้งานอินเทอร์เน็ตรวม **986 GB** (download) จาก **8.4 ล้าน sessions** ส่วนใหญ่เป็นบริการทำงานอย่าง Microsoft 365 และ Google
- หมวด **social-networking** ใช้ bandwidth ประมาณ **21%** ของทั้งหมด แนะนำให้ผู้บริหารพิจารณานโยบายการใช้งาน
- พบการ Login VPN จากต่างประเทศ **1 ครั้ง** ตรวจสอบแล้วเป็นพนักงานเดินทางไปทำงาน
- Firewall บล็อกเว็บไซต์ไม่เหมาะสมและเว็บอันตรายได้ตามนโยบาย และพบ **high-severity event 2 รายการ** จากเครื่องเดียวกัน ถูก drop แล้วทั้งหมด

SAMPLE

1 - Summary Total Bytes – Upload and Download

Total Download	Total Upload	Total Sessions
986 GB	118 GB	8,412,370

2 - Top 10 Source IP Address

#	Source IP	Download (GB)	Upload (GB)
1	10.10.100.163	177.06	11.58
2	10.10.20.232	107.36	11.1
3	10.10.100.216	99.46	7.6
4	10.10.20.126	98.79	7.09
5	10.10.100.210	91.55	5.34
6	10.10.100.35	88.69	1.79
7	10.10.100.143	53.55	3.6
8	10.10.100.20	46.38	2.98
9	10.10.100.180	29.02	7.89
10	10.10.100.170	17.48	6.39

#	Source IP	Download (GB)	Upload (GB)
1	10.10.20.152	39.83	32.09
2	10.10.100.13	3.34	30.49
3	10.10.100.131	15.64	27.23
4	10.10.105.91	30.56	19.98
5	10.10.105.97	4.4	13.31
6	10.10.100.227	27.71	8.9
7	10.10.20.29	23.08	8.34
8	10.10.20.205	36.99	5.98
9	10.10.100.28	22.96	4.99
10	10.10.100.227	12.35	3.47

3 - Top 10 Destination (by Service)

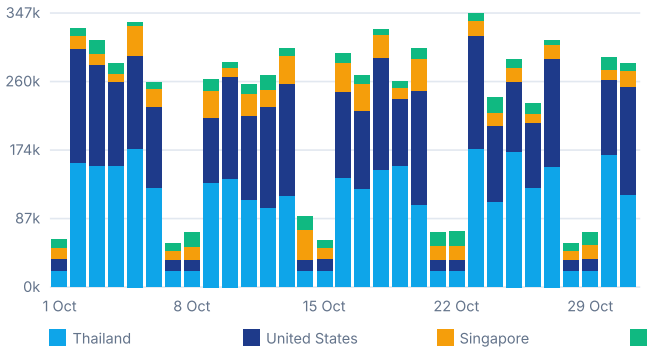
#	Service	Destination IP	Download (GB)
1	Google	142.250.x.x	71.4
2	Microsoft 365	52.97.x.x	58.9
3	Meta (Facebook)	157.240.x.x	44.1
4	Akamai CDN	23.4x.x.x	39.2
5	YouTube	172.217.x.x	33.7
6	Apple iCloud	17.248.x.x	21.3
7	LINE	147.92.x.x	18.6
8	Windows Update	13.107.x.x	16.2
9	TikTok	161.117.x.x	11.8
10	Amazon AWS	54.x.x.x	9.4

Destination IPs are partially masked. Internal IP addresses in this sample are fictitious.

SAMPLE

4 - Top 10 Source Location and Destination Location

#	Destination Country	Connections	Share %
1	Thailand	3,912,450	44.1
2	United States	3,105,882	35.0
3	Singapore	702,311	7.9
4	Japan	298,104	3.4
5	Hong Kong	187,560	2.1
6	Malaysia	120,045	1.4
7	India	64,210	0.7
8	Others	478,808	5.4



5 - Top 10 URL Category

#	URL Category	Download (GB)	Traffic Share %
1	computer-and-internet-info	241.3	24.5
2	social-networking	207.6	21.1
3	search-engines	139.2	14.1
4	content-delivery-networks	88.4	9.0
5	business-and-economy	61.7	6.3
6	streaming-media	47.9	4.9
7	online-storage-and-backup	29.3	3.0
8	medium-risk	12.6	1.3
9	news	10.8	1.1
10	shopping	8.9	0.9

6 - Top 10 Application

#	Application	Download (GB)	Traffic Share %
1	ssl	268.4	27.2
2	google-base	171.9	17.4
3	facebook-base	139.6	14.2
4	ms-update	72.1	7.3
5	ms-office365	66.5	6.7
6	youtube-base	44.8	4.5
7	line	38.2	3.9
8	tiktok-base	29.4	3.0
9	web-browsing	27.7	2.8
10	zoom	18.3	1.9

SAMPLE

7 – Top 10 Policy (Rule Name)

#	Rule Name	Sessions	Unique Source IPs	Share %
1	Internet-Services	4,712,055	92	56.0
2	Allow-Web	2,301,662	98	27.4
3	WiFi-Staff-To-Internet	812,470	61	9.7
4	Mgmt-Update-Firewall	402,118	1	4.8
5	VPN-Remote-Access	98,316	14	1.2
6	Mail-Services	52,930	74	0.6
7	Allow-LINE	32,819	88	0.4

8 – Top 10 VPN User

#	VPN User	Connections	Download (GB)	Source Country
1	user-01	32,616	1.50	Thailand
2	user-02	24,927	2.22	Thailand
3	user-03	21,934	1.02	Thailand
4	user-04	6,404	3.00	Japan ⚠
5	user-05	3,799	0.32	Thailand
6	user-06	3,698	1.68	Thailand
7	user-07	2,893	2.24	Thailand
8	user-08	2,672	2.71	Thailand

⚠ user-04 Login จากญี่ปุ่น ตรวจสอบกับพนักงานแล้ว เป็นการเดินทางไปทำงาน (ทุก User เปิด MFA แล้ว)

9 – Top URL – Allowed and Blocked

Top Allowed Domain	Category	Visits
*.microsoft.com	computer-and-internet-info	312,440
*.trendmicro.com	computer-and-internet-info	288,102
*.google.com	search-engines	144,876
*.line-apps.com	computer-and-internet-info	98,233
*.facebook.com	social-networking	87,410
*.icloud.com	online-storage-and-backup	64,915

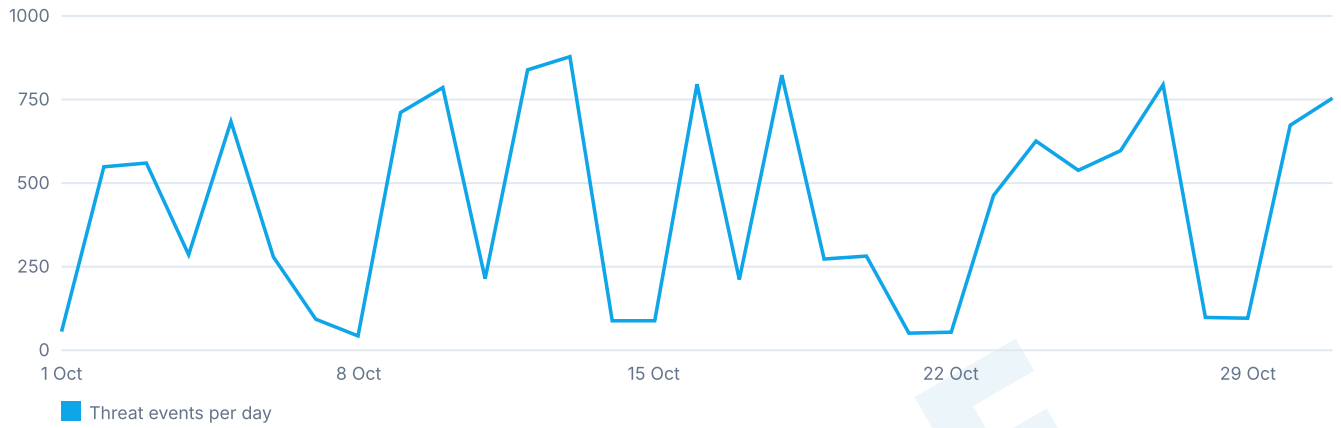
Blocked Category	Blocked Count	Unique Users
adult	4,812	6
gambling	219	3
malware	41	2
phishing	17	2
weapons	12	1
proxy-avoidance	9	1

Blocked domain names are omitted in this sample. The real report lists each blocked URL and source IP for follow-up.

SAMPLE

10 – Threat Detection – IPS / Spyware / Virus / Sandbox

#	Threat	Type	Count	Severity	Action
1	Proxy / anonymizer service	spyware	9,812	low	alert, drop
2	Suspicious DNS query	spyware	4,105	low	alert, drop
3	Parked domain lookup	spyware	1,377	informational	alert
4	Known C2 domain lookup	spyware	612	medium	drop
5	Squatting domain	spyware	208	low	alert, drop
6	Malicious URL in e-mail link	virus	41	medium	block



11 – High Risk – Critical and High Severity Events

Source IP	Destination	Severity	Count	Threat	Action	First seen
10.10.100.143	Known C2 host (masked)	high	2	Command-and-control DNS lookup	drop	22-Oct-2026 11:07

เครื่อง 10.10.100.143 พยายามติดต่อโดเมนที่เป็น Command-and-Control Firewall drop ได้ทั้งหมด ทีม ANS แจ้ง IT ของลูกค้าให้สแกนเครื่องด้วย Antivirus แล้ว ผลสแกนพบ Adware 1 ตัวและลบออกเรียบร้อย

Recommendations

1. พิจารณานโยบายการใช้ Social Media ในเวลางาน (ใช้ bandwidth ~21%)
2. ตั้งเวลา Windows Update (ms-update ~7%) ของเครื่องลูกข่ายให้อยู่นอกเวลางาน
3. บล็อกหมวด **medium-risk** สำหรับผู้ใช้ทั่วไป หลังได้รับอนุมัติจากผู้บริหาร
4. คงการเปิด MFA สำหรับ VPN ทุก User และทบทวนรายชื่อ VPN User ทุกไตรมาส

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