



### Sources of Internal Network Threats

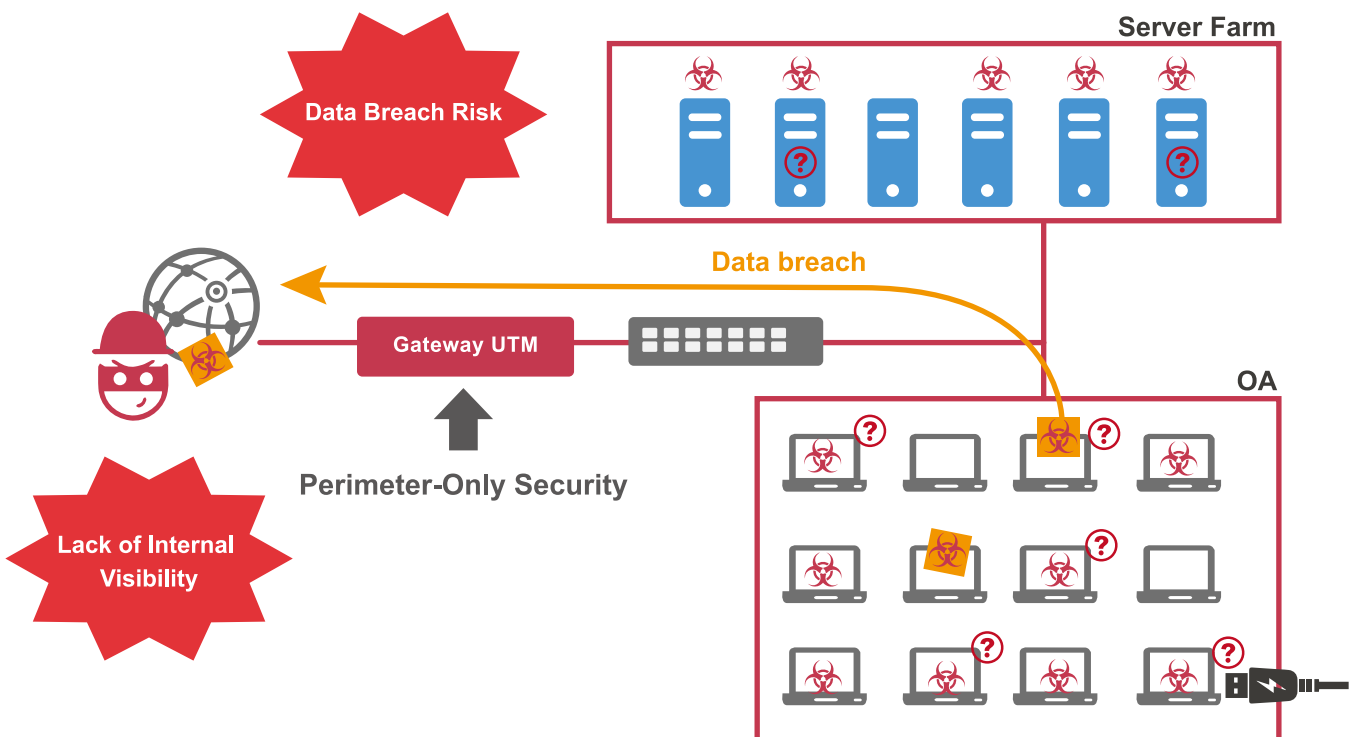
- Account Compromise and Privilege Misuse
- Infected Internal Endpoints or Servers
- Third-Party or Maintenance Access Risks

### Typical Attack Behaviors

- Lateral Movement
- Privilege Escalation
- Data Exfiltration

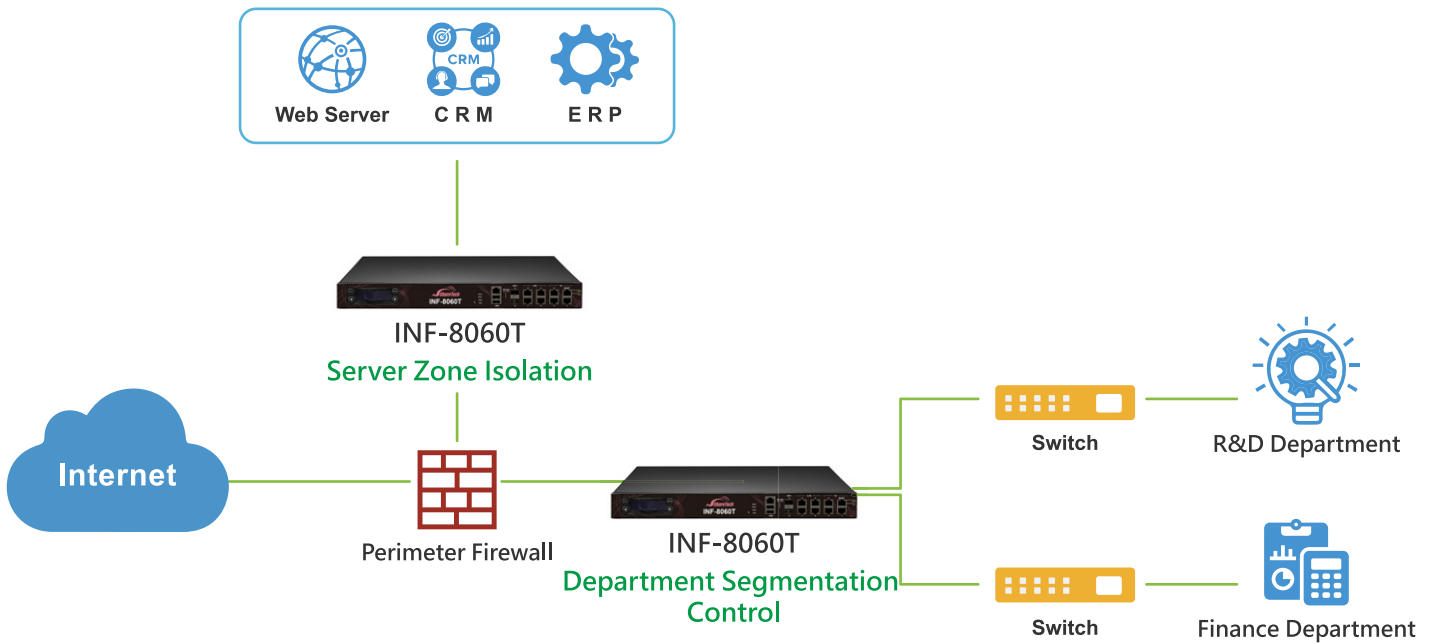
### Management Blind Spots

- Lack of Traffic Visibility
- Absence of Network Segmentation
- Limited Incident Traceability



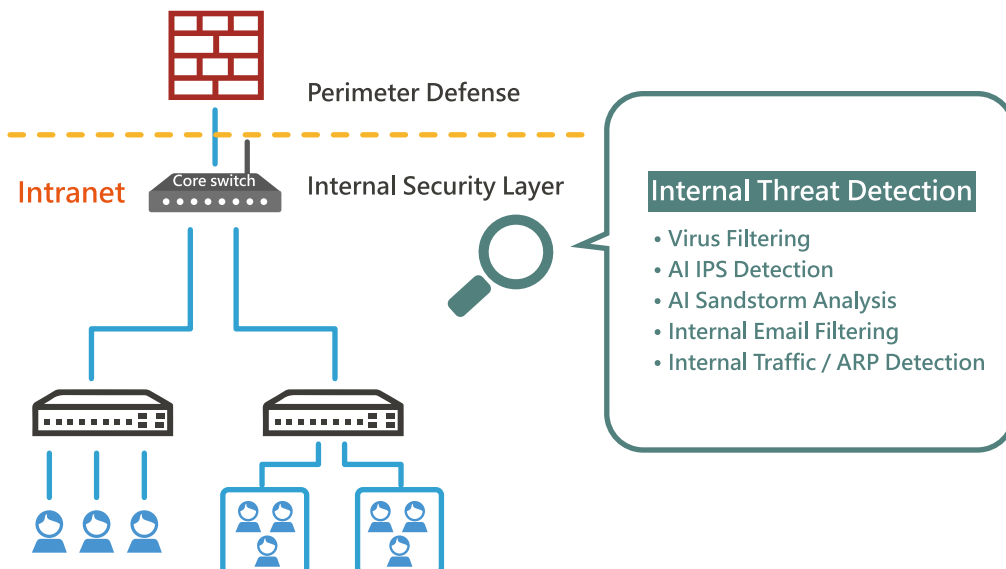
# ShareTech INF Internal Firewall Series Strengthening Internal Network Security

ShareTech Internal Firewall delivers comprehensive protection, detection, threat intelligence, and response capabilities. Built on a next-generation architecture, it extends security beyond the perimeter into the internal network, improving visibility and enabling real-time threat detection. Intelligent defense and real-time alerts help administrators quickly identify and respond to suspicious activities.



## Feature 1: Reducing Internal Zero-Day Attack Risks

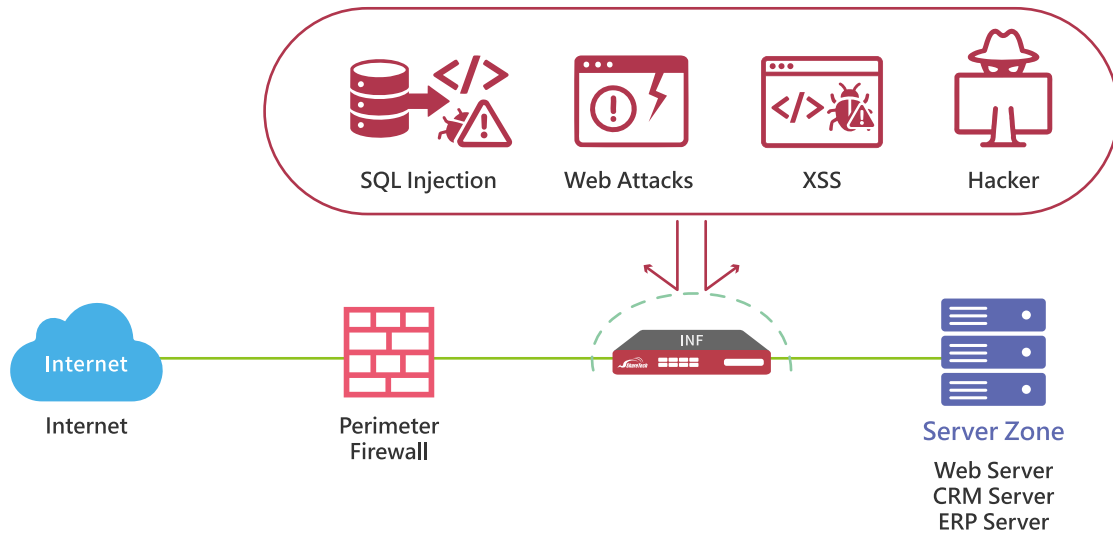
ShareTech Internal Firewall enhances internal network visibility and detects abnormal activities in real time. By combining IPS detection, Sandstorm threat analysis, virus filtering, and internal traffic monitoring, it helps identify suspicious behaviors and mitigate potential zero-day threats.



## Feature 2: Protecting Critical Servers and Hosts

ShareTech Internal Firewall detects and blocks various web application attacks, including SQL injection, cross-site scripting (XSS), and other malicious threats. With its built-in WAF (Web Application Firewall), it performs deep inspection at the application layer to enhance protection beyond traditional perimeter firewalls.

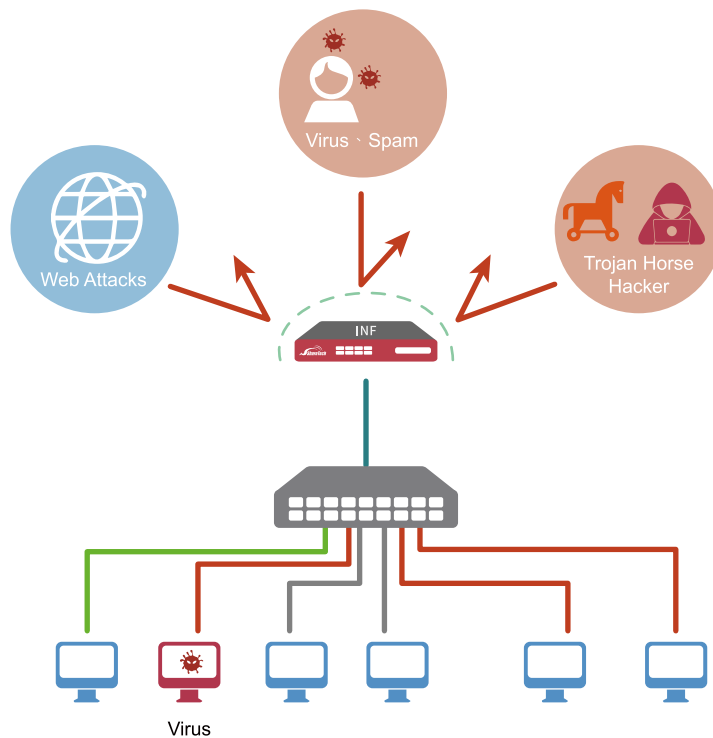
By analyzing connection behavior, only legitimate traffic is allowed to access critical servers and hosts, helping prevent potential threats from reaching internal systems.



## Feature 3: Integrated Protection with Network Switches

When abnormal activities are detected, the internal firewall can identify the attack source and automatically block or isolate the threat. By integrating with network switches, administrators gain better visibility into network topology and device connections, enabling faster detection and response to potential internal threats.

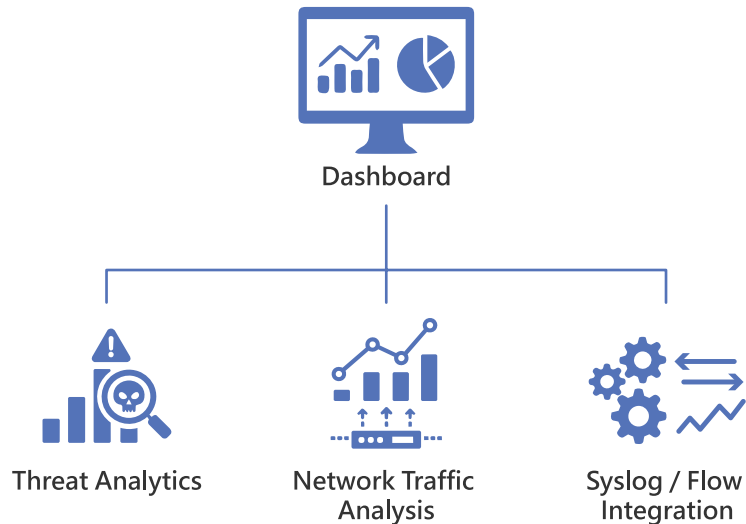
Detect threats and block attack sources through switch integration.



The switch instantly confirms the blocking status of abnormal devices.

## Feature 4: Comprehensive Threat Intelligence Visibility

ShareTech Internal Firewall includes a built-in threat intelligence dashboard that centralizes security events and network data for analysis. With visualized monitoring of threat trends, traffic activity, and system events, administrators can quickly identify abnormal behaviors. By integrating Syslog, Flow data, and threat intelligence for correlation analysis, the system helps trace potential attack sources and provides comprehensive logging, auditing, and reporting to strengthen internal network security visibility.



## Specifications

NEW

Model	INF-8400H	INF-8060T	INF-8700C	INF-8700F
<b>Hardware</b>				
Form Factor	1U	1U	1U	1U
Network Interface	6 x Giga Ports	4 x Gigabit 4 x 2.5 Gigabit 2 x 10G SFP+	14 x Giga Ports	6 x Giga Ports 8 x 1G SFP
Watchdog Bypass	•	•	•	•
LAN Bypass	1 pair	1 pair	2 pairs	2 pairs
Supported Mode	Bridge			
Recommended Number of Users	Under 50	Under 100	200-300	200-300
<b>System Performance</b>				
Firewall Throughput	4.2 Gbps	27.2 Gbps	13 Gbps	13 Gbps
Max. Concurrent Sessions	900,000	3,900,000	3,000,000	3,000,000
New Sessions Per Second	65,000	100,000	350,000	350,000
Threat Protection Throughput (IPS, Anti-Virus, and Web Filtering)	550 Mbps	2.5 Gbps	1.2Gbps	1.2Gbps
Anti-Virus Performance	750 Mbps	2.5Gbps	1.6Gbps	1.6Gbps
IPS Throughput	600 Mbps	5 Gbps	1.2Gbps	1.2Gbps
<b>Software Security</b>				
Virus Engine	ClamAV	ClamAV	ClamAV	ClamAV
ShareTech Anti-virus Engine	Subscription	1-year support	1-year support	1-year support
FTP Virus Scan	•	•	•	•
Spam Filtering	•	•	•	•
Mail Audit	•	•	•	•
AI IPS	Subscription	1-year support	Subscription	Subscription
AI Sandstorm	Subscription	1-year support	Subscription	Subscription
WAF	•	•	•	•
Advanced Application Control & Database	1-year support			
Advanced URL Control & Database	1-year support			
Anomaly Flow Analysis	•	•	•	•
Co-Defense (With Switch)	•	•	•	•
AP Management	•	•	•	•
Intranet Protection	•	•	•	•
Geo IP	•	•	•	•
Network Testing Tools	•	•	•	•
Log	•	•	•	•
QoS	•	•	•	•
Offline Update	•	•	•	•
Dashboard	Optional	•	•	•
UPS	•	•	•	•
Eye Cloud/CMS (Client)	•	•	•	•

## Collaborative Defense – Supported Models

Brand	Models	
ShareTech	ML-9324E	
Zyxel	GS2210-24	
	GS2210-24HP	
	GS2210-48	
	GS2220-28	
	GS2220-50	
	XGS2210-52	
	XGS3700-24	
	XGS3700-48	
	XGS2210-28	
	XS3800-28	
	GS2220-10HP	
	Cisco	C2960L-24TS-LL
		Cisco3560e
Cisco3750		
PROSCEND	850G-12I	
	850X-28	
Other	Juniper-EX2200	

## AP Management – Supported Models

Brand	Models
Zyxel	NWA50AX
	NWA50AX PRO
	NWA90AX
	NWA90AX PRO
	NWA110AX
	NWA110BE
	NWA130BE
	NWA210AX
	NWA210BE
	WAX510D
	WBE510D
	WBE530
	WAX610D
	WBE630S
	Netgear

## UPS Supported Models

Brand	Models
APC	Smart-UPS 3000
	Back-UPS Pro 700
	Back-UPS 1100
Flight Technic	FT-1000BS
EATON	5E 650

## 3G / 4G / 5G USB Modem – Supported Models

Brand	Models
HUAWEI	E3372h
	E161 ( 3G only )