Customer Case Study:
SAKURA Internet Mitigates DDoS Attacks with Volt Active Data

Executive Overview

SAKURA Internet is one of Japan's largest data centre operators, providing enterprise-grade hosting, virtual private networks, elastic cloud, and business continuity services. With a modern global data centre powering worldwide operations, SAKURA's core promise is simple: always-on availability, without downtime or data quality loss.

Delivering on that promise requires defeating distributed denial-of-service (DDoS) attacks, malicious traffic floods that keep targeted customers offline. As attack sophistication grew and 5G-enabled IoT devices multiplied potential attack vectors to a million connected devices per square kilometre, SAKURA's traditional perimeter defences were no longer sufficient.

SAKURA turned to Volt Active Data to power a purpose-built, real-time DDoS mitigation engine. Replacing blunt blackhole routing with surgical, source-and-destination filtering, SAKURA collapsed detection-to-decision time from minutes to milliseconds, stopping attacks before customers experience impact and saving upwards of $5,000 per minute in potential losses.

Key Outcomes Delivered:

> Detection-to-decision time: minutes/hours → milliseconds
> $5,000+ per minute in customer losses prevented per attack
> 100% legitimate traffic preserved via source-and-destination filtering
> Full per-source IP profiling with bits-per-second granularity
> Platform deployed at a fraction of the cost of commercial DDoS tools
> SDN-integrated - Volt pushes blocking flows directly to deployed network switches

Real-time decisioning became the defence. Detection without decisioning authority is not protection.

Key Performance Results

Validated in production deployment across SAKURA's backbone infrastructure:

Metric	Before Volt	After Volt Active Data
Detection-to-Decision Time	Minutes to hours	**Milliseconds**
DDoS Mitigation Approach	Blunt blackhole routing (d/rtBh)	**Source-and-destination filtering**
Legitimate Traffic Preserved	Collateral blocking of valid packets	**100% surgical attack isolation**
Financial Impact Prevented	$5,000+ per minute in losses	**Attacks stopped before customer impact**
Expensive commercial platforms	Expensive commercial platforms	**Fraction of cost, scalable, in-house**

Business Challenge: Stopping Attacks in Real Time

DDoS attacks represent one of the most direct and costly threats to data centre operators. One in three US businesses have experienced a DDoS attack. A single attack costs between $2.3 million and $4 million, with a median downtime of 7 to 12 hours. Cybersecurity experts logged 10 million DDoS attacks in 2020, averaging over 27,000 per day.

For SAKURA, the stakes are existential. Enterprise customers whose profitability and survival depend on network availability cannot tolerate downtime. Every minute of outage carries direct financial and reputational consequences for SAKURA's customers and for SAKURA itself. With 5G-enabled IoT devices expanding potential attack vectors to a million connected devices per square kilometre, the threat surface was growing exponentially.

"Keeping customers connected at all times is of vital importance to SAKURA given the ever-increasing range of applications and services being delivered and consumed online," said Tamihiro Yuzawa, SAKURA network engineer. "Unfortunately, large-scale DDoS attacks directed toward service providers and private enterprises have demonstrated all too clearly that traditional perimeter defenses are not enough to combat today's sophisticated DDoS attacks."

SAKURA required a solution that could:

> Ingest massive volumes of sFlow traffic data from backbone infrastructure in real time
> Identify attack sources with per-IP granularity and bits-per-second profiling
> Make allow/block decisions in milliseconds - not minutes or hours
> Preserve legitimate traffic to customers sharing uplinks with attack targets
> Integrate directly with SDN controllers and deployed network switches

Technical Challenges

Three systemic issues defined the need for a new real-time decisioning architecture:

1. Traditional Defences Too Slow for Real-Time Attack Response

SAKURA's existing approach relied on remotely triggered, designation-based blackhole routing (d/rtBh), a blunt instrument that discards all traffic to a targeted destination. This method is reactive, not preventative. By the time routing changes propagate, attack traffic has already reached customers. Worse, legitimate traffic sharing an uplink with the attack target is collaterally blocked, creating secondary outages for uninvolved customers.

2. No Per-Source IP Visibility or Profiling Capability

Effective DDoS mitigation requires knowing exactly who is attacking, at what rate, and from which sources in real time. Legacy monitoring tools operated at too coarse a granularity to support source-and-destination-based filtering. Without per-IP profiling with bits-per-second precision, SAKURA could not distinguish attacker traffic from legitimate traffic with sufficient accuracy to enable surgical intervention.

3. **Ingestion-to-Decision Gap Measured in Minutes, Not Milliseconds**

   At DDoS speeds, a decision that arrives in minutes is functionally equivalent to no decision at all. SAKURA's existing infrastructure could not process sFlow data streams at the velocity required to make real-time blocking decisions. The gap between data ingestion and actionable decisioning was too large and that gap is exactly where DDoS attacks cause maximum damage.

The Volt Solution: Real-Time DDoS Decisioning Engine

Volt Active Data became the high-velocity decisioning engine at the core of SAKURA's new DDoS mitigation architecture. The architectural principle: collapse the gap between ingestion and decision to milliseconds, and move from destination-based blunt blocking to source-and-destination surgical filtering. The same engine that ingests sFlow data, maintains per-IP state, makes the blocking decision, and records the authoritative outcome - all in a single execution path.

Five architectural capabilities define the Volt deployment:

> **Massive sFlow ingestion at backbone scale:** Volt ingests IP traffic-flow data streams directly from SAKURA's backbone communications infrastructure, processing the full volume of network telemetry without batching or delay.

> **Per-source IP profiling:** Volt maintains real-time profiles for every observed source IP address, including incoming bits-per-second rates, enabling the system to identify attack sources with surgical precision.

> **Millisecond detection-to-decision loop:** From data ingestion to blocking decision, Volt's in-memory ACID engine processes events and records authoritative decisions in single-digit milliseconds — before attack traffic accumulates customer impact.

> **Source-and-destination-based filtering:** Unlike blackhole routing, Volt's decisioning enables filtering by both source and destination, allowing legitimate traffic to continue flowing to targeted customers while attacker traffic is blocked.

> **SDN controller integration:** The Volt-powered application communicates directly with SDN controllers, which push updated flows to deployed switches — ensuring data packets reach the correct destination even during active attacks.

Why Volt Active Data?

SAKURA evaluated available approaches before selecting Volt Active Data. No alternative could simultaneously meet the requirements for real-time, inline DDoS decisioning at backbone scale.

1. Sub-10ms Decisioning — The Only Acceptable SLA

DDoS attacks do not wait. Every second of delayed response is another second of customer downtime and lost revenue. Volt's in-memory ACID engine makes authoritative blocking decisions in single-digit milliseconds, inline in the traffic flow. This is the fundamental requirement SAKURA's architecture demanded, and the one most alternative platforms could not meet.

2. High-Scale Ingestion with Real-Time Stateful Decisioning

sFlow data from a data centre backbone generates massive volumes of telemetry continuously. Volt combines high-velocity stream ingestion with stateful per-IP tracking in a single platform — no separate stream processor, no separate database, no coordination latency. The same engine that ingests data makes the decision and records the authoritative outcome atomically.

3. ACID Consistency for Authoritative Decisions

In a security context, an inconsistent decision is worse than no decision. Volt's full ACID compliance ensures that every allow/block decision is made against accurate, current state — with no race conditions, no stale cache hits, no eventual consistency gaps. When Volt says block, the decision is authoritative and immediately enforced across the SDN fabric.

4. Cost-Effective, Scalable Platform

"We were able to implement a scalable monitoring application at a fraction of the cost of expensive commercial applications," said Yuzawa. Volt's architecture eliminated the need for expensive proprietary DDoS appliances, replacing them with a purpose-built, in-house platform that scales with SAKURA's infrastructure without proportional cost increases.

Architecture and Implementation Highlights

The transformation from reactive blackhole routing to real-time surgical filtering represented a fundamental shift in where decisioning authority lives in the security stack:

Legacy DDoS Approach	Volt Active Data
Destination-based blackhole routing	**Source-and-destination-based filtering**
Minutes to hours from ingestion to action	**Milliseconds — inline decisioning engine**
Legitimate traffic collaterally blocked	**Surgical isolation — valid packets forwarded**
Expensive commercial monitoring tools	**Cost-effective, scalable in-house platform**
Reactive — respond after damage begins	**Preventative — stop attacks before customer impact**

The key shift: decisioning authority moved to the data layer. Blocking decisions became authoritative outcomes recorded in real time, not delayed responses to pre-accumulated damage.

Business Outcomes and Benefits

The results of the Volt Active Data deployment are immediate, measurable, and structural to how SAKURA protects its customers:

Minutes to Milliseconds
Detection-to-decision time collapsed from minutes or hours to milliseconds — enabling intervention before customers experience any impact.

$5,000+ Per Minute Protected
DDoS attacks cost SAKURA's customers upwards of $5,000 per minute. Volt's real-time decisioning stops attacks before losses accumulate.

100% Legitimate Traffic Preserved
Source-and-destination filtering replaced blunt blackhole routing. Valid packets continue reaching customers even during active attacks.

Scalable at a Fraction of the Cost
SAKURA deployed a production-grade, scalable monitoring platform at a fraction of the cost of equivalent commercial DDoS tools.

Surgical Per-IP Attack Isolation
Per-source IP profiling with bits-per-second granularity enables precise identification and blocking of attack traffic with no collateral damage to other customers.

SDN-Integrated Defence Network
Volt-powered application communicates directly with SDN controllers, pushing flows to deployed switches and ensuring correct packet delivery during active attacks.

Conclusion: The Decisioning Foundation for Always-On Infrastructure

DDoS attacks are not a future threat. They are a present operational reality. For data centre operators like SAKURA, the question is not whether attacks will occur, but how fast and how precisely they can be stopped.

The evidence is in production. By deploying Volt Active Data as the core decisioning engine, SAKURA collapsed detection-to-decision time from minutes to milliseconds, eliminated collateral blocking of legitimate traffic, and built a scalable DDoS mitigation platform at a fraction of the cost of commercial alternatives.

"By using Volt, we've been able to narrow the gap from the point of data ingestion to the point of decision-making from minutes, or even hours, to milliseconds," said Yuzawa. "What's more, we were able to implement a scalable monitoring application at a fraction of the cost of expensive commercial applications."

With Volt Active Data embedded at the core of its security architecture, SAKURA delivers the always-on experience its enterprise customers depend on:

> **Attack prevention, not remediation** — decisions made before damage accumulates
> **Surgical precision** — attackers blocked, legitimate customers unaffected
> **Real-time economics** — $5,000+ per minute in potential losses stopped per attack
> **Operational simplicity** — scalable, in-house platform at a fraction of commercial costs

Volt's unique combination of ACID transactions, in-memory speed, massive ingestion throughput, and sub-10ms decisioning makes it the engine of choice for mission-critical, always-on security infrastructure.

Real-time security is no longer a function of expensive appliances. It is a function of architecture.

Ready to stop DDoS attacks before they reach your customers?

Volt Active Data is purpose-built for the latency, throughput, and determinism demands of real-time security decisioning. Whether you are modernising DDoS mitigation, fraud prevention, or network security operations, Volt gives you the platform to decide correctly, at any scale, in real time.

Talk to a Volt Solutions Architect today.

Visit www.voltactivedata.com, email info@voltactivedata.com or contact your Volt account team to arrange a briefing and proof-of-concept scoping session.