

Security

DDoS Protection

Large-scale Network Traffic Attack Detection & Protection

DDoS Protection service detects and blocks DDoS (Distributed Denial of Service) attacks, which cause service failure by creating a high volume traffic. Continuous monitoring detects and blocks external traffic attacks and protects servers within the Samsung Cloud Platform. In the event of a DDoS attack, the availability of web services is ensured by minimizing the traffic load of servers in the Samsung Cloud Platform through the means of blocking attack traffic.

Prompt Detection

In case of large inbound traffic, real-time detection of DDoS attacks is provided. Continuous updates on DDoS defense mechanisms allow staying on top of the latest attack tactics.

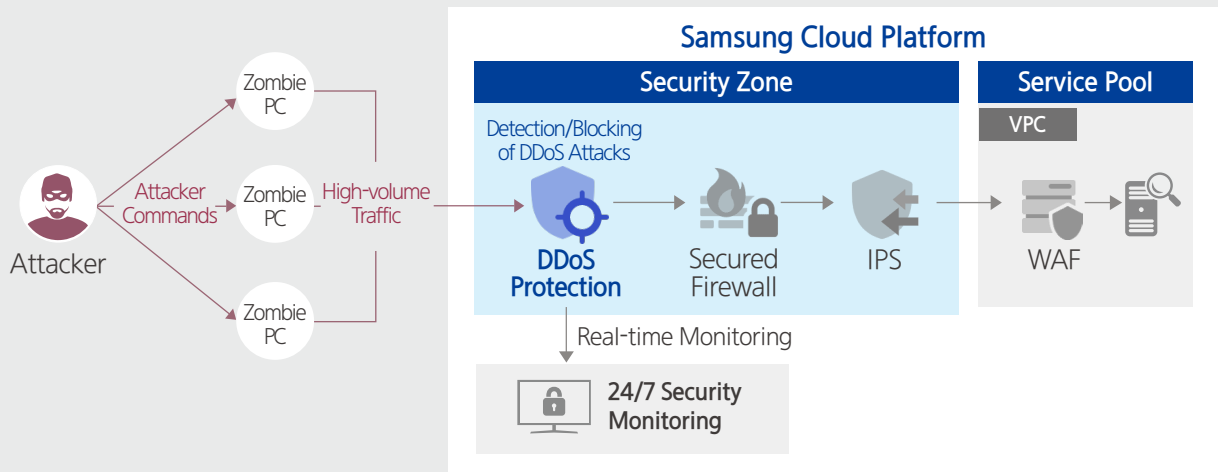
Effective Blocking

Real-time DDoS attack detection and attack traffic blocking can ensure service availability and allow legitimate users to access the website.

Reliable Web Service Operations

DDoS Protection can effectively protect against external security threats through 24/7 security monitoring based on security operations experience with large network environment. It alerts you when detecting a DDoS attack, and event information is available in the monthly report.

Service Architecture



Key Features




- **Intrusion detection and analysis**
 - 24/7 event monitoring
 - Automatic DDoS attack detection
- **Intrusion mitigation**
 - Learning-based detection and blocking of various Layer 3 and Layer 4 DDoS attacks
- **Monitoring reports**
 - Provide monthly reports (alert list and information, etc.)

Pricing

- **Billing**
 - Based on the number of public IPs (1 IPs included by default)
 - Charged for each additional IP

FOR MORE INFORMATION

SAMSUNG SDS

 www.samsungsds.com / cloud.samsungsds.com
 contact.sds@samsung.com / scp_sales@samsung.com
 youtube.com/samsungsds

