SOLUTION BRIEF

Volterra Multi-layer Cloud DDoS/Web Protection

In a world that is more open and connected than ever, DDOS (Distributed Denial of Service) attacks and security breaches are increasing in frequency and ease for malicious actors. As a results, companies and organizations have to be able to effectively protect online business, reputation and datacenters against the increase in DDoS attacks.

WORLDWIDE CLOUD SECURED BACKBONE

Volterra is an innovative startup that provides a cloud-native environment to deploy, connect, secure and operate distributed applications and data across multi-cloud and edge. Enterprises benefit from greater innovation, faster time- to-service and simplified operations.

To protect SaaS solutions against DDOS attacks, Volterra has deployed the VoltMesh Secured Backbone. Points of Presence (PoPs) globally deployed in Tier-1 IXCs are interconnected across a dedicated, multi-terabit redundant private backbone to maximize performance. Volterra PoPs are densely peered and connected to multiple transit providers to achieve reliable access to applications. Volterra directly connects to multiple cloud providers from the PoPs to provide a reliable and predictable experience across global cloud platforms.

KEY BENEFITS

- Global protection
- Layer 3, 4 and 7 DDoS protection
- Terabit DDoS scrubbing capabilities
- Attack monitoring and mitigation with 24/7/365 SOC
- SLA for DDoS mitigation performance
- DDoS protection with response to attack signature and vector changes with Machine Learning and experimented staff

Volterra Cloud Protection allows companies to protect the entire/subnets network (Layer 3, 4 and 7) against DDoS attacks. Infrastructure protection can be used to protect any key element such as websites, DNS servers, SMTP servers and any IP. This protection uses Volterra's multi-terabit network capacity and capabilities to mitigate the largest and most sophisticated DDoS attacks.

Figure 1: Volterra Secured Backbone

VOLTMESH SECURED BACKBONE PROTECTS YOUR INFRASTRUCTURE

VoltMesh Secured Backbone is designed to handle today's largest and complex DDoS attacks over 3Tbps+. When the attack begins, VoltMesh performs the following actions:

1. Cloud Detection

Volterra Cloud Detection equipment and software detect the attack. Detection is based on a combination of static rules (e.g. volumetric attacks) and personalized rules per customer:

- VoltMesh routers send NetFlow information to Volterra NetFlow collectors and NetFlow analyzers
- NetFlow allows our Cloud Detection to not miss any alert with real- time polling and information collection (e.g. source | destination ASN, IP address, next-hop IP | ASN

2. Customer Alerting

When an attack is detected, our 24/7/365 SecOps Team (Security Operations Center) is notified and will either notify you to trigger the mitigation or trigger the mitigation on your behalf.

3. Cloud Mitigation

You change your BGP announcements to have transit coming through VoltMesh instead of the other transit providers. Volterra steers the traffic using BGP and our scrubbing centers block the attack, only allowing legitimate traffic to go through.

4. Legitimate Traffic Delivery

Only legitimate traffic is carried to your sites.

Protection can be deployed as "Always-On" or "On-Demand" solution. TTM (Time to Mitigation) for customers who subscribe to "Always-On" mitigation is immediate for static rules and takes less than 10 seconds for customer rules.

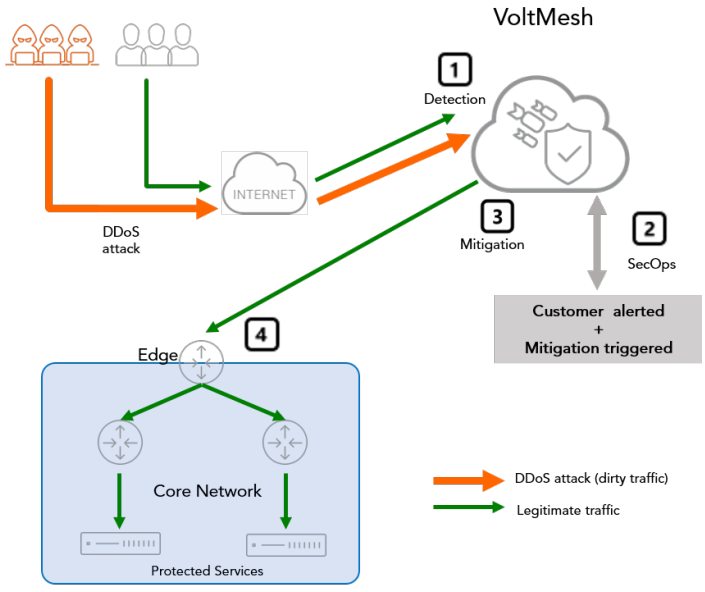
KEY FEATURES

- Advanced client classification engine analyzes all incoming traffic
- Custom rules matching your enterprise security policy
- 24/7/365 Security Operations Center and Support Team
- Automated anti-DoS tools with eyes-on-glass human expertise

KEY BENEFITS

- Pure OPEX
- Mitigation at the nearest origins
- 3Tbps+ mitigation capabilities
- Mitigation time from real-time to a few seconds
- Flexible infrastructure protection from multiple / 22 prefixes down to one single IP

Figure 2: Cloud-based DDoS Protection



VOLTMESH SECURED BACKBONE PROTECTS WEBSITES

VoltMesh Secured Backbone provides Web Application Firewall (WAF) and DDoS protection in one single solution. Easy to deploy and manage, Volterra Cloud Protection is powered by the scale and capability of the global VoltMesh Secured Backbone. Our Web Application Firewall protects your website from major attacks and SQL injection, OWASP-identified vulnerabilities and all threats at the application layer.

Organizations using Volterra Web Protection route their website traffic by changing a simple DNS record. This enables Volterra to inspect each and every request sent to the website and filter out malicious activity.

1. Web Traffic Analysis

Users and attackers connect to web applications through VoltMesh Secured Backbone.

2. Cloud Mitigation / Web Application Firewall

Servers inspect inbound traffic for DDoS and web application attacks and block any that are detected. Machine learning algorithms update your security protections based in the latest threats.

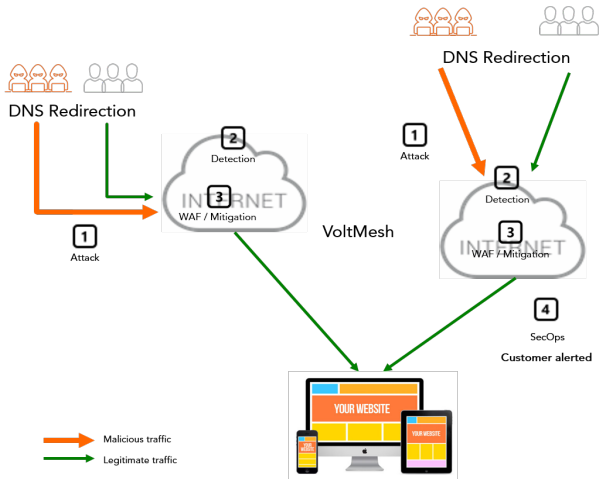
3 - 4. Legitimate Traffic Delivery and Customer Alerting

Only legitimate traffic is carried to your sites.

KEY FEATURES

- Cloud deployment with no hardware or software required
- Automatic protection from diverse threats, including OWASP Top 10 Protection Layer
- JavaScript Challenges for advanced filtering under attacks
- Analytics per bot and protection against bots
- Analytics on L3/L4 in addition to L7
- Customized export of logs
- Advanced customer portal, including API
- HTTPS included: TLS certificate handled

Figure 3: Cloud Web Protection

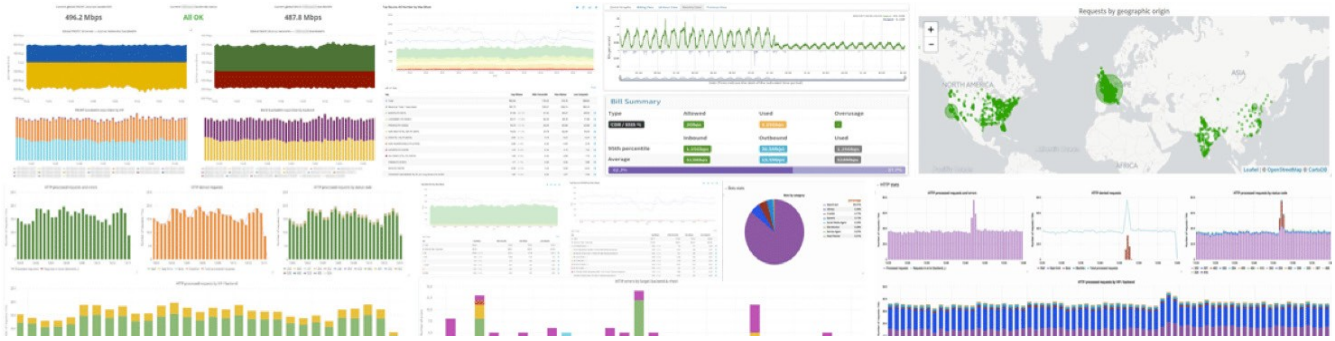


KEY BENEFITS

- Pure OPEX
- Deploy quickly
- Easy to manage
- Real-time protection

Volterra Cloud Protection		
	Volterra DDoS Protection	Volterra Web Protection
Cloud-based PoP/Scrubbing Center Locations	• Americas: New York, San Jose, Seattle, Ashburn, Sao Paulo • Europe: Paris, Frankfurt, London, Amsterdam • Asia: Singapore, Tokyo • Cloud scrubbing capacity of 3Tbps+	
Services Profiles	Clean Traffic (95 percentile) 100Mbps, 200Mbps, 300Mpbs, 500Mbps, 800Mbps, 1Gbps, 2Gbps, 4Gbps, 8Gbps, 10Gbps, 40Gbps, 100Gbps	
Services Included	On-demand mitigation with 18 mitigations per year, 90 attack hours with direct BGP peering or BGP over GRE tunnel	• DNS redirect with 5 VIP • Real-time Web protection with WAF (OWASP Top 10 Protection Layer)
Options	• Always-on Customer traffic always stays on Volterra Cloud • Additional on-demand mitigation hours	• DNS redirect: additional VIP or 5 VIPs as a bundle

Figure 4: Volterra Console



About Volterra

Volterra provides a comprehensive SaaS platform to deploy, connect, secure and operate distributed applications and data across multi-cloud and edge sites.

Learn more about Volterra cloud security solutions

Visit: volterra.io

Contact Technical Sales: sales@volterra.io