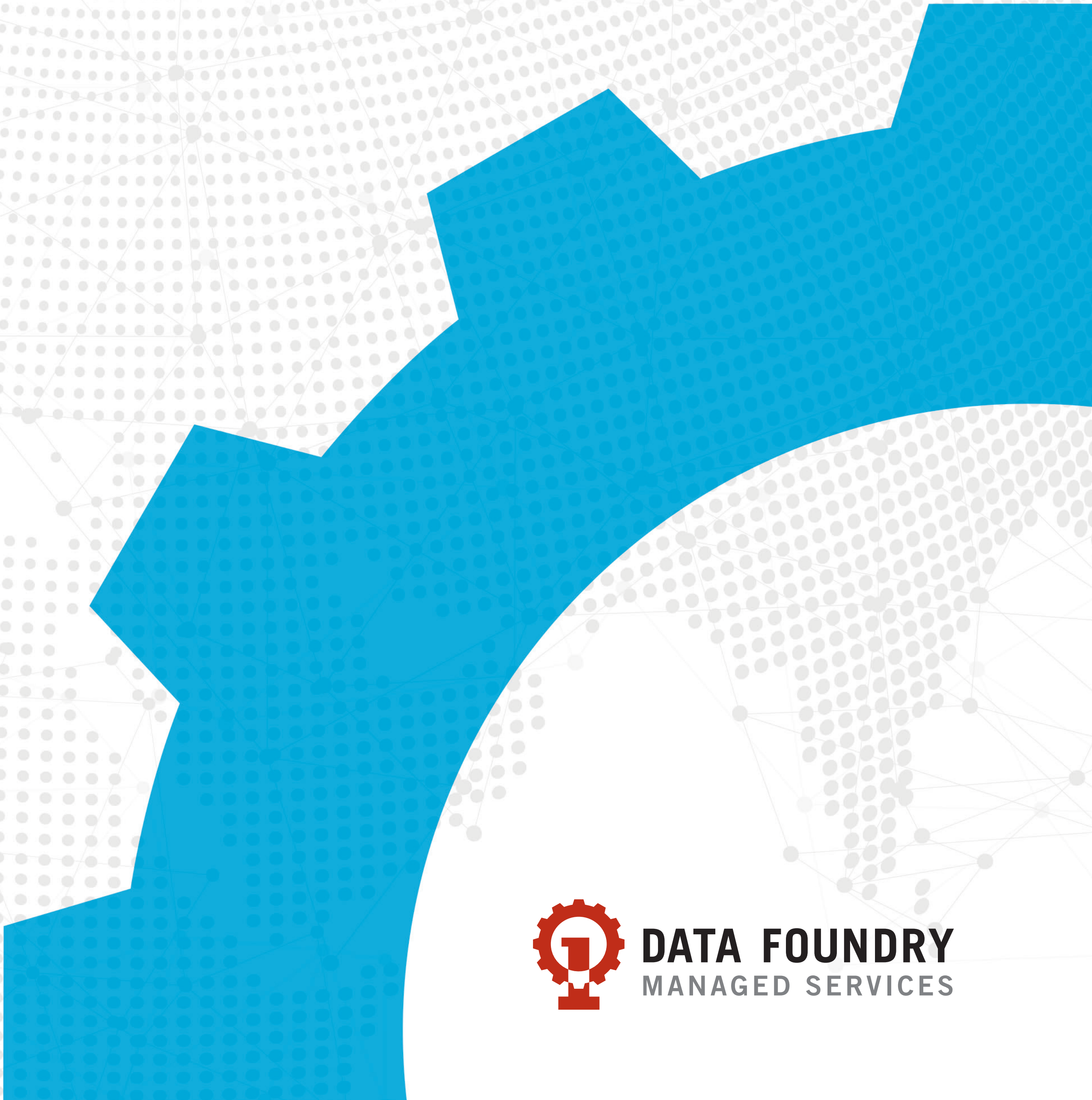
DDOS MITIGATION

Insurance for Your Network



DATA FOUNDRY
MANAGED SERVICES

Data Foundry's DDoS Attack Mitigation

Data Foundry's DDoS Attack Mitigation Service is a sophisticated, network-based cyber attack mitigation solution. It is a fully-managed service and a hybrid solution that harnesses on-premises detection and mitigation technologies in addition to cloud-based volumetric attack-scrubbing measures.

Why Should You Be Concerned With DDoS?

Organizations are challenged by an evolving threat landscape that reduces revenues, increases expenses and damages reputations. Today's cyber attackers use sophisticated methods – often multiple attack vectors in the same attack campaign – to bring down an organization's web presence. The ease of launching DDoS attacks and variety of tools available are reasons why more organizations are suffering from increased attacks.

1/3

of all downtime incidents are caused by DDoS attacks[1]

OVER **90%**

of organizations experienced cyber attacks in 2015[2]

176%

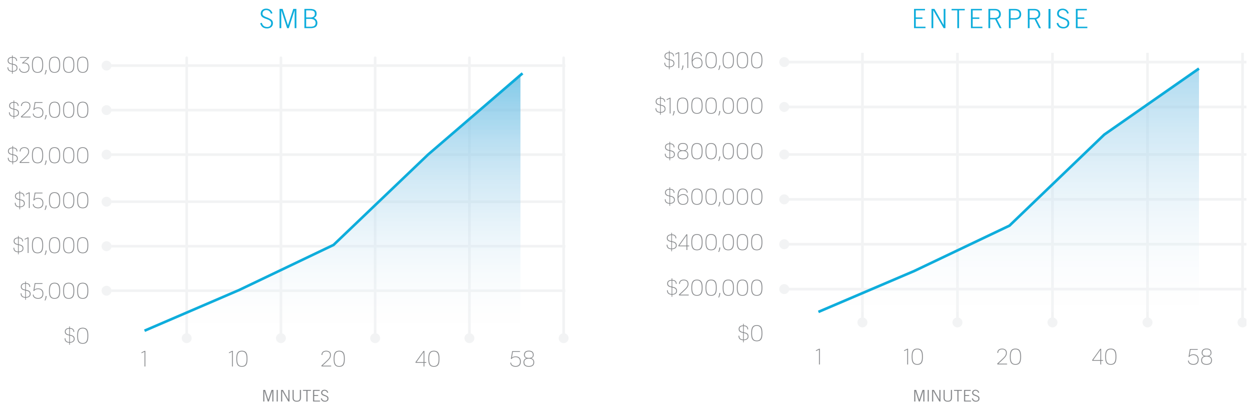
increase in total DDoS attacks YOY from 2014–2015[3]

58 min

the average duration of DDoS attacks for 2015[4]

*Attacks come in bursts and often occur over a period of 24 hours or more.

Cost of DDoS Attacks Over Time[5]



1. Verisign/Merril; 2. Akami; 3. Radware; 4. ATLAS; 5. Arbor Networks, 2015

Insurance for Your Network

Always-on, Inline Attack Mitigation Solution

Our solution provides instantaneous coverage, accurate detection and shortest time to protection. Zero-day attacks can be learned and mitigated in less than 18 seconds, all with sub-millisecond latency added. By protecting enterprises against known and emerging network and application threats in real-time, Data Foundry's layered approach is designed to help organizations mitigate attacks and offer a security solution that combines detection and mitigation tools.

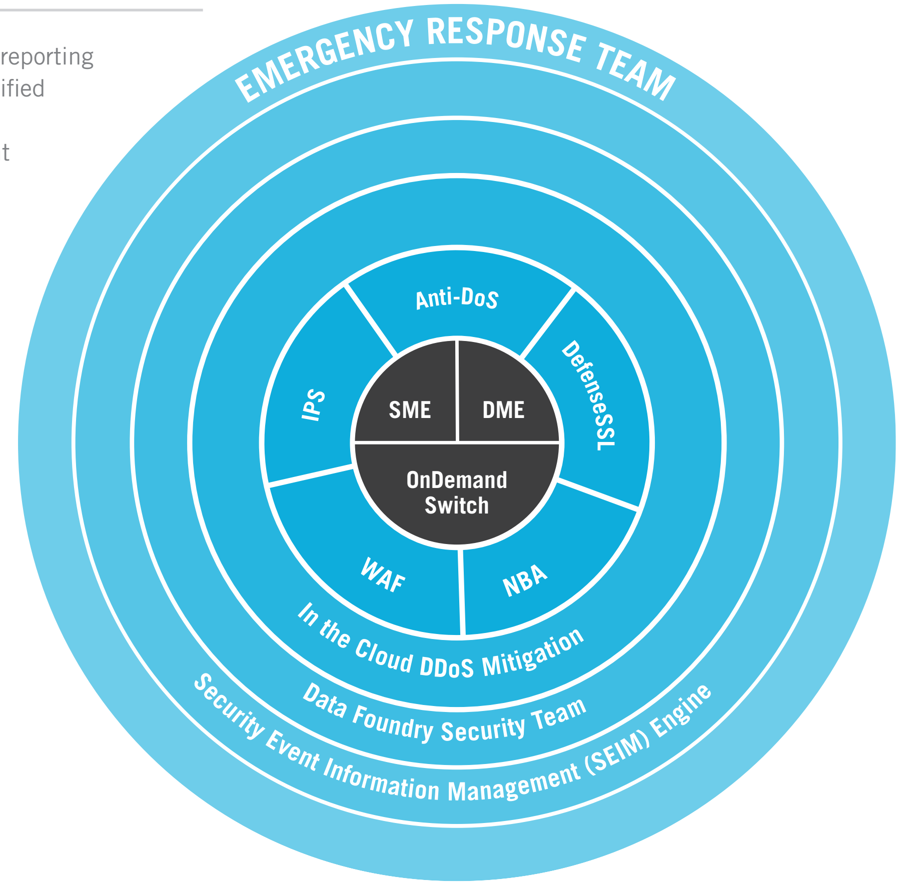
Protection from Multi-Vector Attacks

Data Foundry's attack mitigation solution includes multi-vector attack detection and handles network layer and application-based attacks, malware propagation and intrusion activities. Complete with anti-DoS, Network Behavior Analysis (NBA), SSL defense, IPS, WAF and in-the-cloud DoS mitigation in one integrated system, the solution is supported on dedicated hardware designed to fight multiple attack vectors simultaneously.

DDoS Protection

Enhanced with a central monitoring and reporting system, the solution provides ongoing unified situational awareness of the network and applications using a single Security Event Information Management (SEIM) engine for all components.

During persistent attack campaigns where the system cannot mitigate all attack vectors out of the box, Data Foundry provides real-time support from our service team, helping customers restore operational status under attack. If necessary, further backup is available from the Global Emergency Response Team.


EMERGENCY RESPONSE TEAM
Anti-DoS
IPS
DefenseSSL
SME
DME
OnDemand Switch
WAF
NBA
In the Cloud DDoS Mitigation
Data Foundry Security Team
Security Event Information Management (SEIM) Engine

CONTACT US FOR A 30-DAY FREE TRIAL**

sales@datafoundry.com • 888-839-2794 • datafoundry.com

> Cybercrime is the greatest transfer of wealth in history.

KEITH ALEXANDER

NSA DIRECTOR 2005-2014

Top Industries Targeted by DDoS Attacks

FINANCIAL SERVICES

Financial services companies are frequently victims of ransom-based cyber attacks. These attacks allow hackers to gain access to sensitive user information, which is usually sold on the black market, resulting in reputational damage and money spent managing fraud. Attacks on financial institutions are commonly executed using high-bandwidth UDP/TCP floods and connection floods.

MEDIA AND ENTERTAINMENT

Attacks on media and entertainment organizations are often political in nature, allowing hackers to protest against particular issues via DDoS attacks. Because so many media and entertainment sites now require online subscriptions, attacks are also aimed at stealing user data.

SOFTWARE AND TECHNOLOGY

DDoS attacks are common for cloud-based and SaaS technologies. These attacks don't only cause software companies to lose substantial revenue, but interfere with clients' business operations, damaging software companies' reputations in turn.

GAMING

Online gaming continues to be the most heavily targeted industry for DDoS attacks using SYN floods. The gaming industry is an appealing target to hacktivist groups and overly ambitious gamers because centralized platforms allow for effective attacks with few resources.

E-COMMERCE AND ONLINE SERVICES

Attacks on e-commerce and retail sites are increasingly more common, rivaling attacks on the financial sector. Retail companies lose revenue with each minute the site remains blocked and also lose customer trust when their personal information is stolen in the process.

EDUCATION

DDoS attacks on schools and educational websites target mail servers, online educational tools and platforms for submitting work. Students increasingly put out requests to "DDoS" their schools. Attack vectors for these targets include UDP amplified reflected floods, DNS query flood and web-crawlers.

Why Is Our DDoS Protection Unique?

INLINE, ALWAYS-ON PROTECTION

Unlike other types of DDoS mitigation services, ours is always on and constantly monitoring traffic. It does not need to be switched on in the event of an attack.

SECURE WEB PORTAL

Our attractive and straightforward web portal allows you to view events and traffic patterns and create unlimited reports. View real-time and historical data.

LOCAL SCRUBBING

Traffic is monitored and scrubbed locally at Data Foundry's Texas 1 data center. Because traffic is not diverted to other locations, there is virtually no latency from traffic scrubbing.

PROFILE-BASED OPTIMIZATION

Profile-based DDoS optimization learns your traffic patterns and evolves to meet the specific defense needs of your network. As your profile becomes more fine-tuned over time, your protection is optimized.

ON PREMISES 24X7X365 MONITORING

Data Foundry staff is on the premises 24x7x365, receiving real-time security alerts regarding your network in our Network Operations Center. If your network falls under attack, our service team will be onsite to help you restore operational status.

SCALABLE WITH NO DOWNTIME

As your business grows and the traffic to your website increases, you may require more bandwidth to manage larger volumes of traffic. We can seamlessly increase the volume of clean traffic to your site in the moment you wish to do so with no downtime.

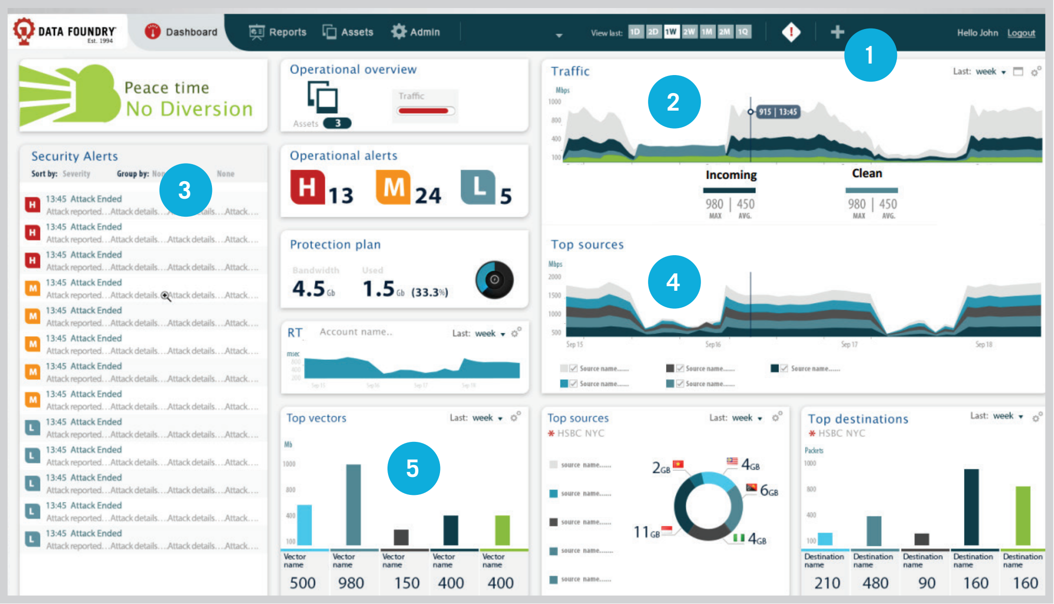
OFFSITE CLOUD-BASED SCRUBBING AVAILABLE

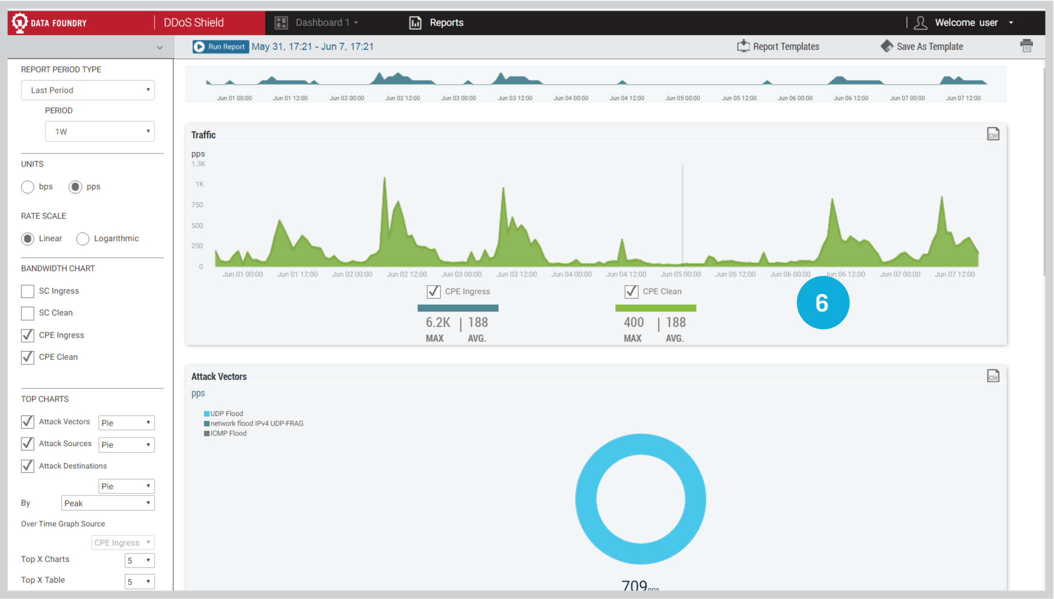
In the event that your organization requires mitigation for large-scale, volumetric attacks, we have the ability to quickly transfer your optimized DDoS profile to high-capacity cloud-based scrubbing centers that can manage attacks of unlimited size.

USABLE FORMAT FOR INVESTIGATIONS

Data is captured and organized in a way that is accepted by law enforcement and admissible in court in the event that an investigation is opened.

Access Our Secure DDoS Web Portal





REPORT PERIOD TYPE: Last Period

PERIOD: 1W

UNITS: ○ bps ● pps

RATE SCALE: ● Linear ○ Logarithmic

BANDWIDTH CHART

□ SC Ingress

□ SC Clean

☑ CPE Ingress

☑ CPE Clean

TOP CHARTS

☑ Attack Vectors: Pie

☑ Attack Sources: Pie

☑ Attack Destinations: Pie

By: Peak

Over Time Graph Source: CPE Ingress

Top X Charts: 5

Top X Table: 5

1. Add, subtract, rearrange and resize widgets
2. Monitor bandwidth being used
3. Get real-time alerts
4. See where attacks are coming from and the size of each attack
5. View the types of attack vectors being used
6. Review historical data from any time frame

CONTACT US FOR A 30-DAY FREE TRIAL** sales@datafoundry.com • 888-839-2794 • datafoundry.com

Let Data Foundry build confidence in your network security.

CONTACT US FOR A 30-DAY FREE TRIAL**

sales@datafoundry.com • 888.839.2794 • www.datafoundry.com

*Restrictions apply.

*Free trial offer cannot be initiated while under attack.