RedShield.

Protecting web apps with shielding as a service.

CASE STUDY

Key Points

- Private connectivity for improved security
- High-performance peering option for customers using MegaIX
- Dedicated connections to customer data stores through virtual cross connects
- Reliable, cost-effective bandwidth for high-traffic connections

About RedShield

Built from a foundation of penetration testing and security technology expertise, RedShield provides managed web application security that mitigates and remediates vulnerabilities using its proprietary 'shielding' tools, which modify app behaviour without altering a single line of code.

Challenge:

Protecting traffic without relying on Internet Service Providers

RedShield securely publishes and protects web apps and platforms for customers across industries, including national and local government, banking, healthcare, and more. This requires a high-capacity, reliable connection to their customers' data centres, but that's not always possible via a traditional Internet Service Provider (ISP) link – especially when cyberattacks put connectivity at risk.

If a Distributed Denial of Service (DDoS) attack occurs through vectors such as email or web traffic, ISP links can quickly get congested and the data center's network responder can rapidly become overwhelmed. If RedShield is operating through the ISP link too, that means the team is blocked from the customer's server, access to which is crucial for managing risk, mitigating threats, and ensuring dynamic web app content works properly.

RedShield needed a way to operate dedicated connections directly to and from their service and their customers' network infrastructures, whether it's hosted in the cloud, on-premises, or in a hybrid setup.

Solution

Bypassing ISPs through direct connection

RedShield offers a service called Redpipe that allows their customers to bypass internet connectivity using Megaport's platform. Customers can either peer through Megaport's high-speed, low-latency Internet Exchange, MegaIX, or they can use private virtual cross connects (VXCs). The latter can use border gateway protocols or static connections – whatever the customer's infrastructure requires.

Through both methods, RedShield can bypass internet connectivity entirely, accessing the customer's servers directly and securely via Megaport's communications infrastructure. It's a more DDoS-resistant way for customers to expose their web apps to the internet, ensuring high availability even when there's a high load on their links and servers.

> *Megaport's virtual cross connects are a simple, secure, and highly cost effective method of connecting RedShield with our customers' data centers. It's a fantastic option for delivering software-defined connectivity in a multi-cloud environment.*
>
> - Sam Pickles, Chief Operating Officer at RedShield

Benefits

Reliable, protected access through a dedicated link

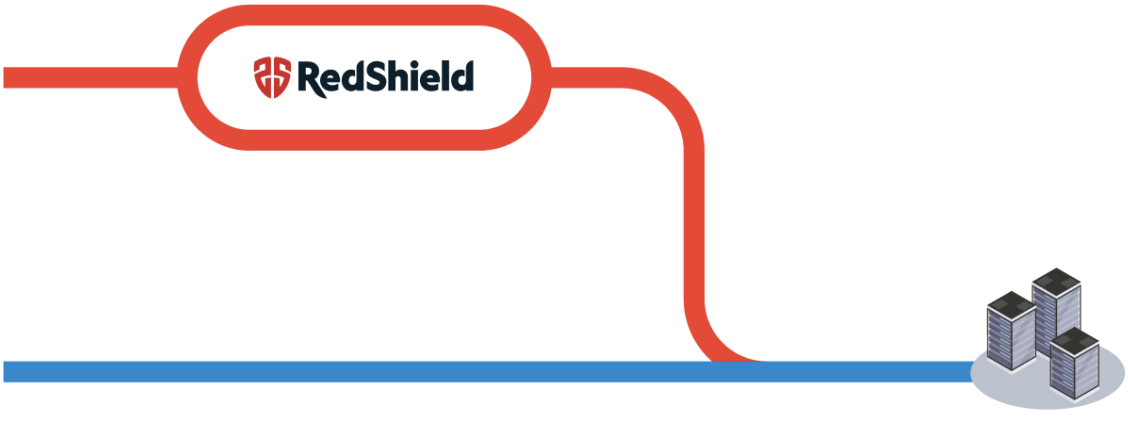
When there's high traffic to a customer's site or apps – whether that's through a targeted attack or something as simple as a product launch or major news event – RedShield's customers can be confident that the direct connection via Megaport helps maintain uptime and performance. All traffic via RedShield is protected and managed by a high-capacity scrubbing center, filtering techniques, usage policies, and other security tools.

Many of RedShield's customers have specific security and compliance regulations to contend with, such as HIPAA in the United States, or GDPR in the EU. RedShield's direct connection via Megaport helps them shore up their security, protect critical and sensitive information, and avoid sanctions or fines, which are getting stricter and costlier by the year.

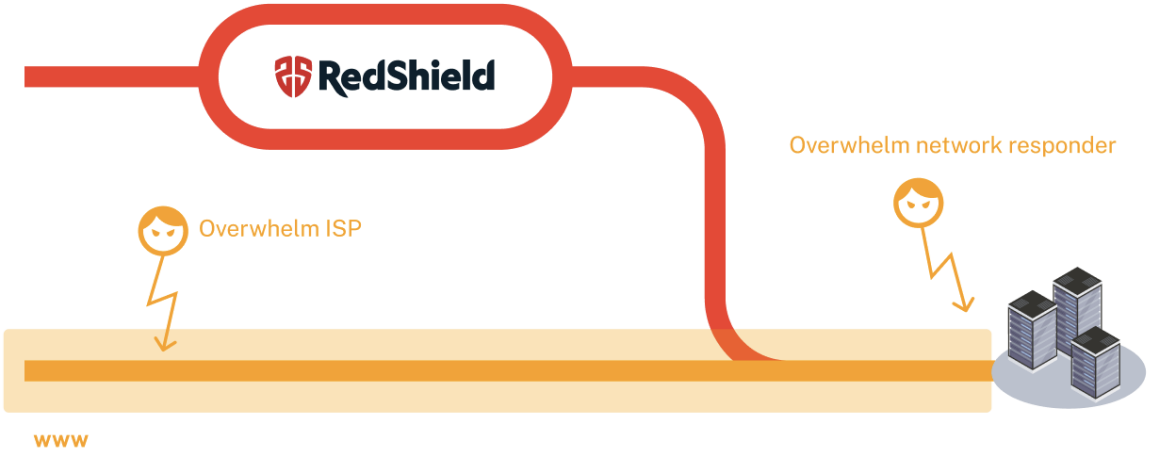
Future plans for RedShield

As their partnership with Megaport grows, RedShield can now focus on optimizing how it uses its VXCs. The team is exploring how to use Megaport's scalable bandwidth to flex capacity up and down as their traffic volume changes.

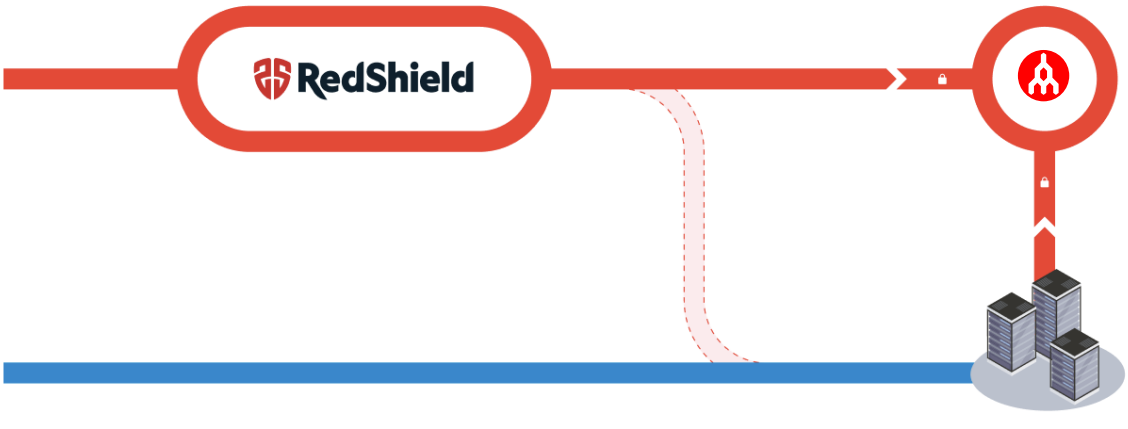
RedShield already works within AWS and IBM Cloud across New Zealand, Australia, North America, and Europe. Megaport's unrivalled worldwide presence will support the team as they continue their expansion into new regions and cloud infrastructures.



Ordinarily, protected traffic flowing through RedShield
still accesses the application servers via the internet



If the ISP gets attacked, even though RedShield is still working,
access to the application servers can be affected



Megaport provides a secure, private, direct connection between RedShield and the
application servers, so the customer is no longer at the mercy of internet outages.

More information

- Megaport Enabled Locations
- Access our Doc Portal
- Access Megaport Portal
- Megaport Videos
- Megaport Cost Estimator
- Contact Us

With thanks to

RedShield

Reimagine connectivity.

Megaport is a leading provider of Network as a Service (NaaS) solutions. The company's global Software Defined Network (SDN) helps businesses rapidly connect their network to other services via an easy-to-use portal or our open API. Megaport's network offers greater agility, reduced operating costs, and increased speed to market compared to traditional networking solutions. Megaport partners with the world's top cloud service providers, including AWS, Microsoft Azure, and Google Cloud, as well as the largest data centre operators, systems integrators and managed service providers in the world. Megaport is an ISO/IEC 27001-certified company.

Megaport

megaport.com
info@megaport.com
Phone: +61 7 3088 5999
Fax: +61 7 3088 5998
Level 3, 825 Ann St,
Fortitude Valley, 4006, AU.
ABN: 46 607 301 959
megaportnetworks
@megaport
@megaportnetwork