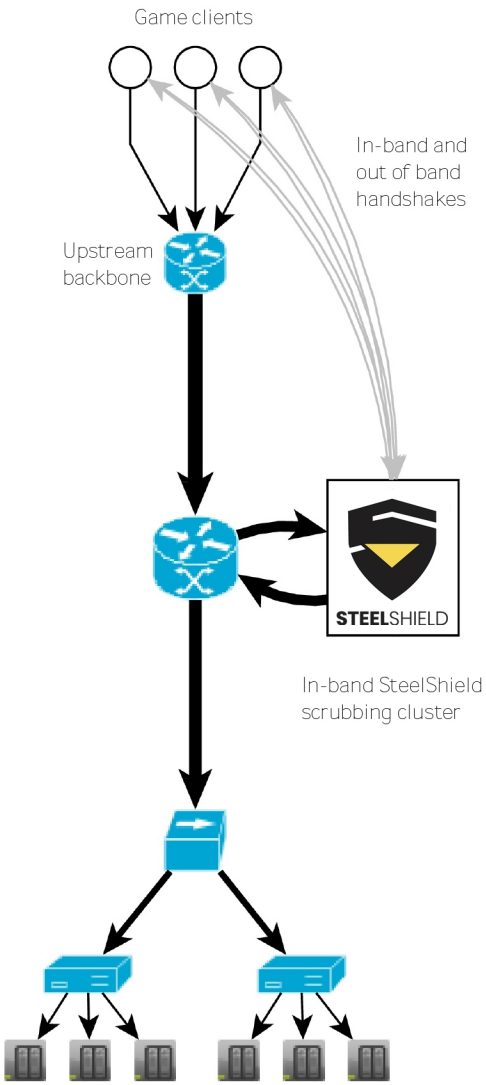
Reinventing DDoS mitigation

Traditional approaches to DDoS mitigation and common heuristics regularly fail when applied to custom UDP-based game traffic. Due to the nature of the underlying network protocols, effectively protecting game servers from DDoS attacks has been an unsolved problem - until now.

Our solution is called "SteelShield" - our in-house DDoS mitigation platform. It replaces fuzzy heuristics by in-depth application-level integration. SteelShield is the culmination of many of years of research and development by our engineers.

SteelShield effectively solved the DDoS problem for ourselves, as well as for our enterprise customers - read on to find out whether we can solve yours, too.

STEELSHIELD



Protocol integration

Our engineers will work directly with you to implement a custom handshake protocol into your products, either by integrating with your proprietary networking protocol or by using a separate out-of-band authentication service. This handshake will be completed by our high-bandwidth scrubbing servers at the edge of our network, handing the session over to your application servers only after the authentication has been completed.

This fully eliminates attacks using spoofed UDP source IP addresses - after implementing SteelShield, not a single spoofed packet will hit your servers.

Handshaking can even be tied to your custom authentication server, offloading ban list enforcement and similar policy decisions to the network layer.

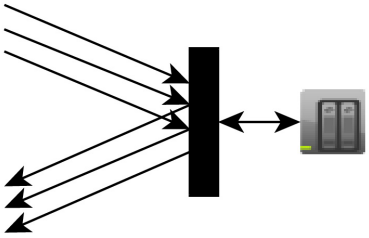
The handshaking protocol also supports an extended version which includes a "client puzzle", a proof-of-work computation the client is required to perform.

marbis GmbH
Griesbachstr. 10
D-76185 Karlsruhe
Germany
m.boessendoerfer@marbis.net

marbis / Nitrado USA, Inc.
4600 Kietzke Lane, H-188
Reno, Nevada 89502
USA
volker.huber@marbis.net

Custom edge caching

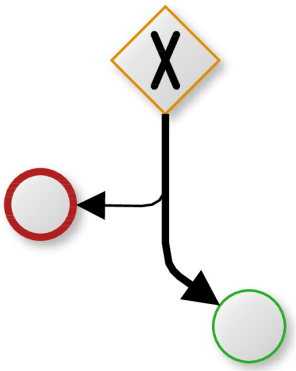
In addition to scrubbing "dirty" traffic, SteelShield in able to cache static content directly at the edge. Common examples of this are "server list" and "server query" protocols, replying to requests in place of the original service. This mode of operation is similar to caching proxies like Varnish, just not for HTTP, but for your protocol.



Our engineers are deeply familiar with usual protocols like the one Steam and Valve's master list are using and implemented support for these. The mechanism is modular and additional protocols can easily be implemented in order to meet your requirements.

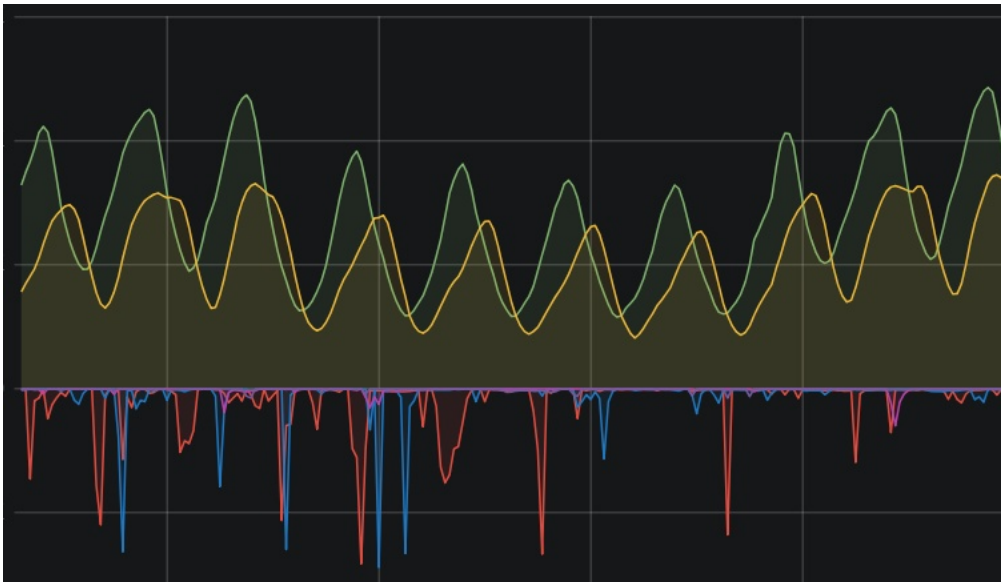
Intelligent whitelisting

Traditional DDoS mitigation solutions require you to statically whitelist remote hosts you're communicating with, with little to no recourse if an attacker finds out and starts spoofing traffic purporting to originate there. In the past, we've even seen attacks impersonating Valve's Steam master servers, trying to trick the DDoS filter into blocking the master servers.



Thanks to our handshaking and caching mechanism, you rarely need to whitelist such traffic. However, in some cases it cannot be avoided if the remote party can't or won't complete a handshake, like with the Steam Relay service.

SteelShield mitigates this by introspecting the traffic, only whitelists it after validating it.

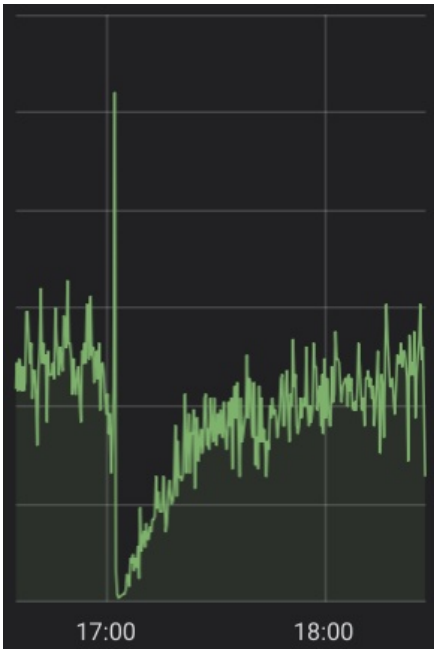


This graph is showing example production traffic for two of our points of presence, with "clean" traffic at the top and "dirty" traffic at the bottom.

As you can see, SteelShield has very high specificity - no attacks are making it through, and no clean traffic is mistakenly marked as dirty.

marbis GmbH
Griesbachstr. 10
D-76185 Karlsruhe
Germany
m.boessendoerfer@marbis.net

marbis / Nitrado USA, Inc.
4600 Kietzke Lane, H-188
Reno, Nevada 89502
USA
volker.huber@marbis.net



Full visibility

We collect detailed in-depth telemetry from our scrubbing servers. Telemetry includes proportional samples of all network traffic and which mitigation action, if any, has been taken.

All telemetry is stored in a high-performance "big data" analytics database. This gives our engineers and customers full and unsurpassed visibility into all network traffic. In addition to viewing data on a graphical dashboard, you can run arbitrary queries on the raw data instead of having to rely on pre-aggregated time series.

This is particularly helpful for post-mortem debugging - even a week after-the-fact, we can tell with certainty whether a given IP address, port or even traffic matching certain patterns has been filtered or rate limited at a given time.

Top AS for tcpFlag |= tcp.SYN

packets	asName
446.36 Mil	ZIGGO Ziggo B.V., NL
112.14 Mil	WOW-INTERNET - WideOpenWest Finance LLC, US
250.48 Mil	WINDSTREAM - Windstream Communications LLC, US
543.92 Mil	VODANET International IP-Backbone of Vodafone, DE
368.86 Mil	VODAFONE_ES, ES
85.46 Mil	VODAFONE-IT-ASN, IT
212.70 Mil	VIDEOTRON - Videotron Telecom Ltee, CA
303.50 Mil	VERSATEL, DE

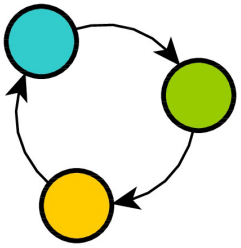
Sample aggregation query that shows the top autonomous systems for packets not matching a particular TCP flag, showcasing our backend's capability to aggregate on arbitrary data points. We can generate the same view for any of the many data points in our telemetry streams.

marbis GmbH
Griesbachstr. 10
D-76185 Karlsruhe
Germany
m.boessendoerfer@marbis.net

marbis / Nitrado USA, Inc.
4600 Kietzke Lane, H-188
Reno, Nevada 89502
USA
volker.huber@marbis.net

Proven in production

SteelShield is backed by a mature software development life cycle, including separate staging clusters, testing and release engineering as parts of our development process.



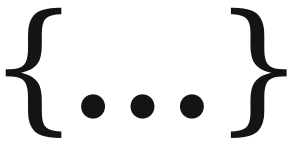
Deployments are done without incurring downtime.

These efforts have paid off: since its inception, SteelShield has not caused a single production incident, even at traffic levels that exceeded its initial specifications.

Multiple watchdog mechanisms ensure that even in the unlikely event of a system crash, routes will immediately be withdrawn, minimizing production impact.

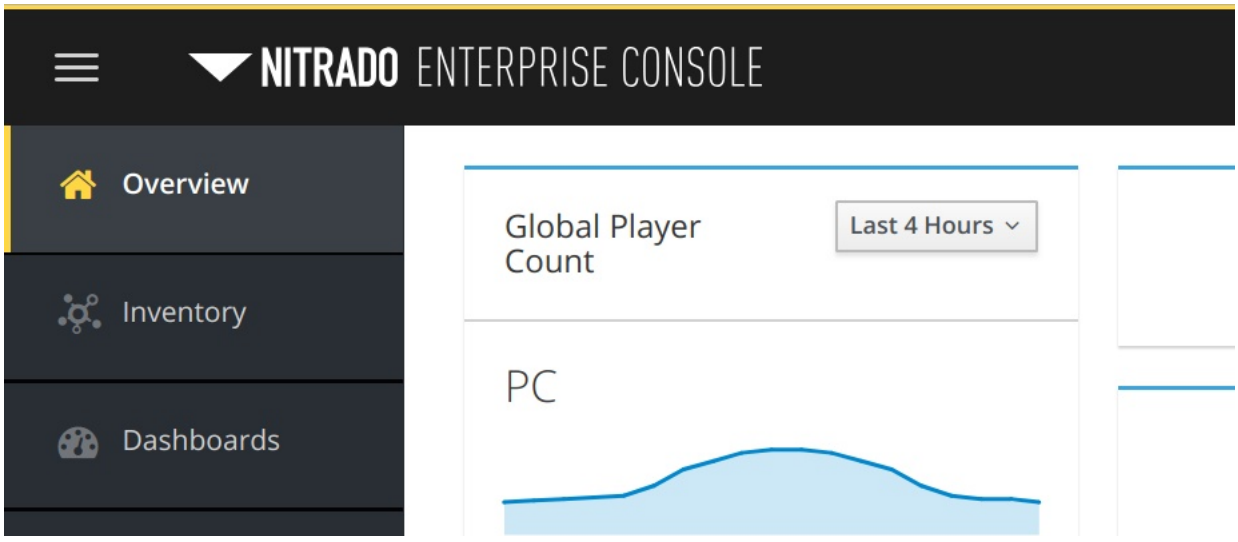
API interface

You can use our REST API to programmatically interact with the SteelShield control plane. For instance, customers can dynamically adjust whitelists or reroute traffic for a particular host. It integrates with deployment orchestration tools like Ansible.



Customer panel

In addition to the API, you can soon use our web-based dashboard to interact with SteelShield, as well as a hosted monitoring and deployment service. Stay tuned!



marbis GmbH
Griesbachstr. 10
D-76185 Karlsruhe
Germany
m.boessendoerfer@marbis.net

marbis / Nitrado USA, Inc.
4600 Kietzke Lane, H-188
Reno, Nevada 89502
USA
volker.huber@marbis.net

Strong partners

Our network is protected by Link11's award-winning filtering technology. Link11 is one of the world's leading DDoS mitigation companies. All inbound traffic is permanently routed through their scrubbing centers, the highest tier of protection they offer.

This ensures that large volumetric amplification attacks that exceed our backbone bandwidth are rate-limited before they reach our network. As opposed to the Layer 7 attacks that SteelShield protects against, volumetric attacks are easy to detect and filter. However, they require large amounts of external bandwidth to absorb. Link11's more than >1 Tbps of aggregate transit and peering capacity ensures that our network survives even the largest attacks.

We were targeted by the same memcached amplification attack that took down GitHub and made it out unscathed.

In addition to this, Link11's global presence, augmented by our internal inbound route optimization technology and peering agreements, ensures very low latencies worldwide. Instead of relying on single Tier 1 providers like Cogent and Level 3 whose peering ports with Tier 2/3 providers are regularly congested in the evenings, we maintain paid peering relationships with important "eyeball networks" like Deutsche Telekom and Unitymedia.

marbis GmbH
Griesbachstr. 10
D-76185 Karlsruhe
Germany
m.boessendoerfer@marbis.net

marbis / Nitrado USA, Inc.
4600 Kietzke Lane, H-188
Reno, Nevada 89502
USA
volker.huber@marbis.net