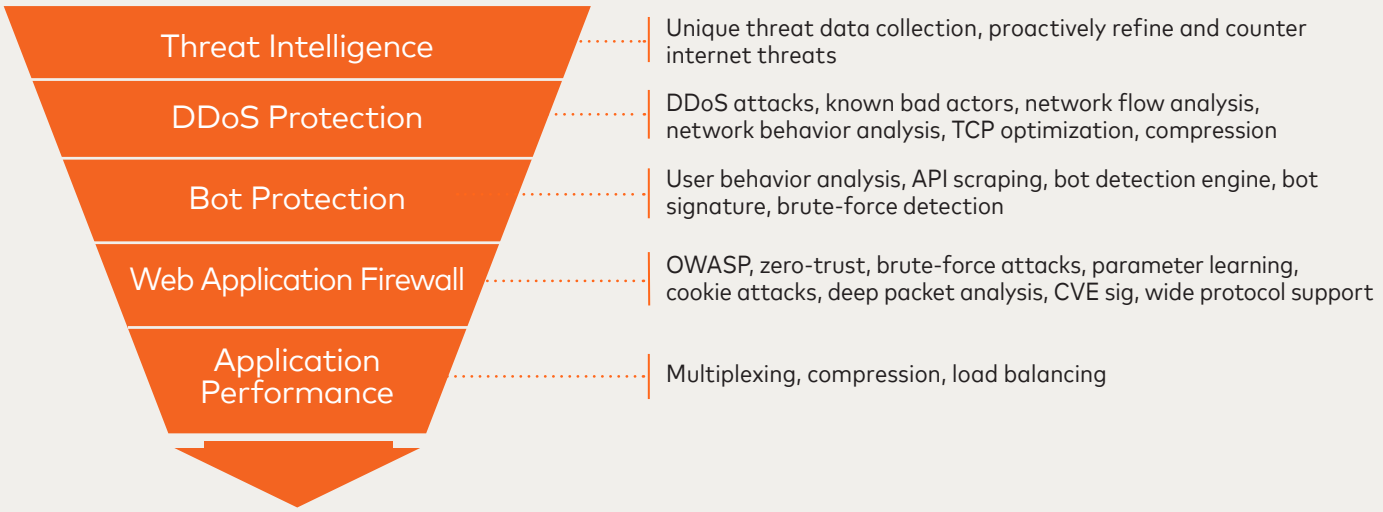
RiskRecon® Threat Protection

TECHNICAL OVERVIEW

Advanced machine learning within RiskRecon Threat Protection swiftly detects and mitigates application and network-level attacks, ensuring continuous and secure online operations.

Our cloud-based service provides multi-layered protection you can trust

Unique full-stack protection, coupled with layered security, safeguards your business against threats at any location, around the clock. Without any hardware, middleware or SDKs needed.



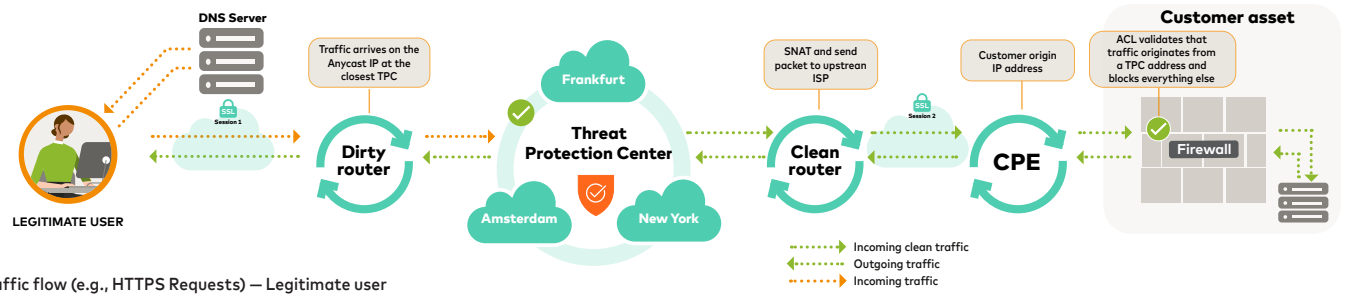
HOW IT WORKS

Two deployment options, same level of protection and security – 24/7

We offer varied deployment methods to suit your needs, allowing for a seamless implementation. The proxy and routed traffic configuration options can also be combined to provide an unmatched level of safety and security.

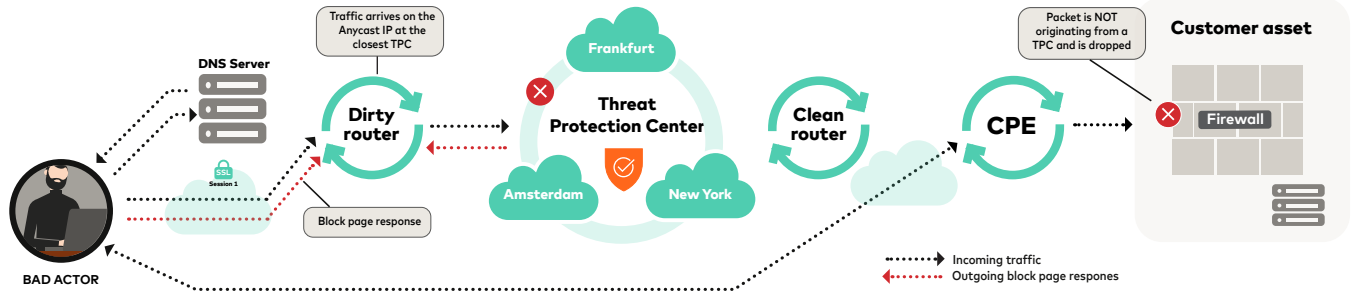
	Proxy Traffic Configuration (L4/L7)	Routed Traffic Configuration (L3/L4)
Mitigation capacity	✓ DNS Redirects – Protection for selected web applications ✓ Detect and mitigate application (L7) DDoS attacks (e.g., HTTP[S]-based, DNS-based)	✓ BGP Routed – Complete network infrastructure protection ✓ Detect and mitigate volumetric (L3/L4) DDoS attacks (e.g., SYN Flood, UDP Flood and ICMP Flood)
Customer criteria	✓ Works for all customers	✓ Requires customer to have their own ASN with at least one public /24 and be in control of their own BGP
Deployment style	✓ Traffic goes in and out via the Threat Protection Center and we will SNAT between the TPC and origin server	✓ Traffic goes in via the Threat Protection Center and a direct service response takes place on the return traffic, using the customer transit link (ISP)

Proxy Traffic Configuration (L4/L7) – DNS Redirect



Traffic flow (e.g., HTTPS Requests) — Legitimate user

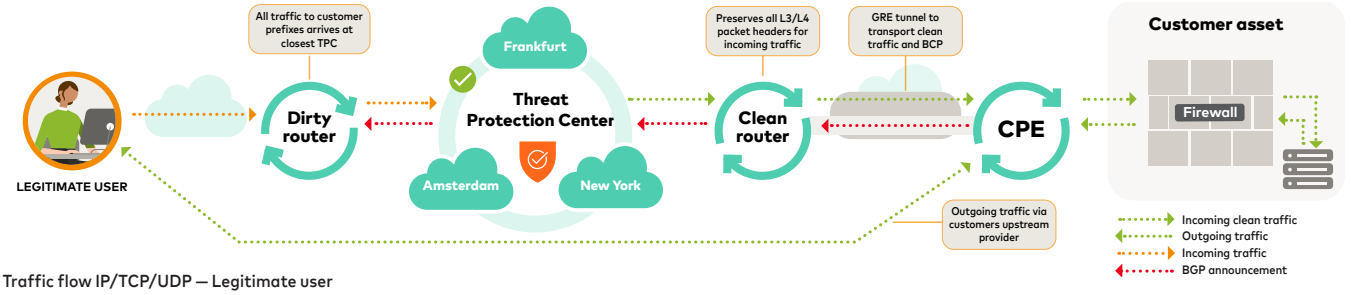
1. A device makes a DNS lookup using your configuration DNS server. For example, baffinbaynetworks.com (A Record).
2. The device receives a DNS response containing IP address 185.195.93.4.
3. HTTPS request is made to 185.195.93.4 GET/ and traffic arrives at the closest Threat Protection Center in Singapore, Frankfurt, Amsterdam, Stockholm 1, Stockholm 2, New York or Los Angeles.
4. Analyzed by the threat protection service and deemed legit.
5. Source Network Address Translation Src IP in IP header gets replaced with the SNAT address of the TPC.
6. Packet arrives at the customer's CPE and is passed on to the asset or a firewall.
7. Firewall or asset extracts the original client IP from the X- Forwarded-For header. Asset processes the packet and replies to the request.
8. HTTP response is sent back the same way it came in.



Traffic flow (e.g., HTTPS Request) — Bad actor

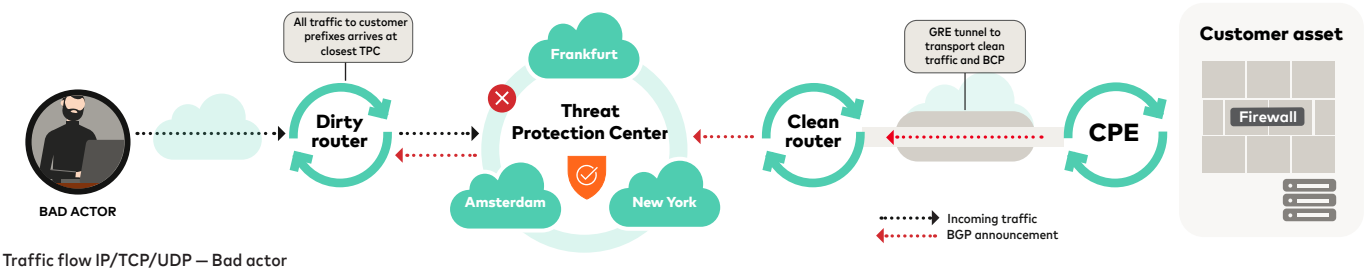
1. The bad actor resolves the DNS name or finds the IP through other methods.
2. The bad actor crafts a malicious request and sends it to the anycast IP and gets routed to the closest TPC.
3. Request is detected as malicious and mitigation takes place. DDoS and Threat Intelligence system drops packets, WAF/ Bot system responds with a block page.
4. The bad actor tries to bypass the TPC and sends a request directly to the origin IP.
5. A firewall rule or router ACL drops all incoming packets that are not originating from a TPC.

Routed Traffic Configuration (L3/L4) – Routed BGP - DSR



Traffic flow IP/TCP/UDP — Legitimate user

1. It all starts with a customer setting up a GRE tunnel or a dedicated PNI into two of our TPC locations.
2. A BGP session is established between the customer's router and the TPC's.
3. The customer announces the prefixes they want to have protected over the GRE tunnel; once a Traffic Configuration for the prefix is created, all TPCs will announce the prefix to the internet.
4. The customer prepends their own ASN at least three times to the announcement of the prefix to their upstream provider.
5. A device makes a connection towards the customer's IP address and arrives at the closest TPC.
6. It is analyzed by the Threat Protection service and deemed legit.
7. The traffic passed on over the GRE tunnel without modifying any IP/TCP/UDP packet headers.
8. Responses and internally initiated traffic go out over the customer upstream provider and do not pass the TPC.



Traffic flow IP/TCP/UDP — Bad actor

1. Bad actor crafts a malicious request and sends it to the customer's IP and arrives at the closest TPC.
2. Request is detected as malicious and mitigation takes place. DDoS and the Threat Intelligence system drops packets, no response is returned.

Trust is at the core of everything we do

For more information about RiskRecon Threat Protection, contact your Mastercard representative.