Centripetal

PRODUCT BRIEF

CleanINTERNET®

Automation and Enforcement Technology

Centripetal is dedicated to protecting organizations of all sizes, from small and medium businesses to large corporate enterprises and datacenters. Centripetal has developed a revolutionary solution that offers cyber teams continuous prevention from attacks through intelligence-led enforcement. We operationalize intelligent-driven security by implementing an advanced patented technology-centric solution.

Our CleanINTERNET cybersecurity service uses applied threat intelligence, rapid network correlation, and automated enforcement of millions of IOCs to prevent over 90% of known threats. CleanINTERNET extrapolates any and every threat intelligence feed, and applies advanced packet filtering at the network edge to prevent unwanted traffic from ever hitting your network. Detailed packet analysis, event monitoring and the collection of critical threat statistics make this turnkey service powerful and effective.

High-Performance Threat Intelligence Gateway

Centripetal's threat intelligence gateway — RuleGATE, is a dense multi-core platform that uses industry leading proprietary and patented algorithms to enable comprehensive enforcement of network traffic on a per-packet basis. This combination of advanced software and hardware enables detection and enforcement of every packet, utilizing over 5 million threat indicators, with latency of less than 10 microseconds, at up to 10Gb/s bi-directional throughout.

Transparent Network Device

The threat intelligence gateway operates on IP traffic as a layer 2, or like a "bump-in-the-wire", device with no IP address, making it transparent to the network. With only microseconds of latency and no network addressable ports, an attacker or malware cannot detect the security enforcement gateway on a CleanINTERNET protected network.

Intelligence Correlation

Centripetal's enforcement of threat intelligence is made possible by sublinear filtering and the correlation of a massive amount of threat data. We have solved the challenge of complex data processing and filtering so that your security analyst team does not have to take it on.

Policy Construction

In order to prevent hundreds of millions of threats, the curation and correlation of bulk threat data has to convert to policies that instruct what is enforced. The policy construct of our CleanINTERNET solution is designed to operate across a risk-based spectrum to optimize and prioritize human analysis and workflow. We build intelligence policies from complex combinations of static and dynamic rules.

Protect Organizations From Advanced Threats by Operationalizing Intelligence

Policy Scope

Rules and policies can filter on any combination of elements, which are typically part of the commercial indicators of compromise, including: malicious IP's, source/destination/IP range (V4 or V6), port or port range, protocol, domain, URL, FQDN, and dynamic multi-dimensional IOCs.

Dynamic Policy Enforcement

CleanINTERNET enables dynamic updates of threat indicators from a customer's internal knowledgebase and industry leading threat intelligence partners, as soon as the information is available, and without packet loss or network interruption. The TCP/IP 5-tuple and Fully Qualified Domain Names (FQDNs) are available to operationalize threat intelligence with high-fidelity enforcement.

Scalable Cybersecurity

Centripetal's core technology scales to the size and speed of today's attackers, malware creators and emerging threats to enable total network awareness of every packet entering, or exiting a network protected with the CleanINTERNET service.

Flexible Integration

Advanced API and SDK allows for third party and internal threat indicator sources to push-or-pull policies as indicators are created, or changed in real-time. The API and SDK are designed to easily expand to any protocol and transport mechanism.

Advanced Shielding and Blocking

The advanced algorithms allow for automatic removal of risk-based threats, including targeted geo-blocking, compliance policies, TOR proxy removal, known malicious IPs, malvertizers, and new domain shielding.

Flow Event Logging

Inspection of every inbound and outbound packet, log-and-flow event delivers real-time analytics. The syslog data is continually sent to standard Security and Event Monitoring (SIEM) platforms for threat analysis and mitigation. Advanced packet filtering that leverages threat intelligence becomes a critical technology in today's SOC.

Full Packet Capture (PCAP)

Centripetal's solution is able to deliver full packet capture for indicator-based hits, which quickly provides a definitive answer on risk. By capturing only threat traffic, this technology is over one hundred times more efficient than other solutions.

> ***"Minimizing the event workload on analysts increases their efficiency, and enables performance optimization of downstream tools, which can reduce infrastructure costs—fewer intrusion detection systems (IDS), intrusion prevention systems (IPS), firewalls, sandboxes, anti-malware appliances, packet capture resources, etc."***
>
> *— Tony Palmer, ESG Senior IT Validation Analyst*

Centripetal

CentripetalNetworks.com