CENTRIPETAL

FAR BEYOND THE FIREWALL

Centripetal CleanINTERNET® Service

Protecting the network has become extremely complex and difficult for any organization.
The legacy firewall has been bypassed by the ever-evolving threat landscape. Many organizations still rely heavily on firewall technology to protect against network infiltration as their main line of defense. This causes a domino effect that creates a lack of direction, a flood of unknown events to the SIEM, and an inability to act on the part of cyber security teams.

As cyberattacks become more sophisticated and frequent, these modern attack methods have reduced firewall effectiveness in many ways. First, in many cases the firewall is ineffective in preventing malware from entering the network, (usually through various phishing mechanisms — email, chat, ads, etc.) that create vulnerabilities to internal hosts and users. The assumption of insider trust, on which the stateful firewall relies, is now clearly invalid. Relying on this stateful trust assumption, firewalls allow malware to open outbound requests, enabling data to be easily exfiltrated by Command and Control infrastructure. Advanced threats often use malware variants capable of disabling the firewall, allowing the threat actor to take full command of the network and access mission-critical data.

Best practice is to layer security, and the most effective network layer approach is a zero-trust intelligence-based defense. You cannot rely on the stateful firewall layer for an intelligence-based defense as this requires zero-trust and adaptive state tracking based on threat. In almost every public breach a legacy network firewall was deployed and bypassed. One would ask "why were these breaches successful with active firewall technology in place, especially in enterprise environments?" In the following sections, we will explain the differences and capabilities, actual use cases and findings between legacy firewalls and the technologies enabling Centripetal's CleanINTERNET® service.

KEY DIFFERENTIATORS

Firewalls inspect traffic using linear search capabilities where the engine mainly relies on a static and constrained IP reputation list. Firewalls are not inherently dynamic, and legacy firewalls cannot scale because they are extremely limited to the number of rules they can deploy and the stateful assumptions they make on risk. With an everchanging threat landscape, the firewall cannot process the large amounts of IOC intelligence to maximize the shielding of known threats, nor can it triage the areas of possible threats. Attackers rapidly set up cloud-based providers to create malicious services on machines that host legitimate websites, further complicating the identification of unwanted traffic.

The following chart compares the capabilities between legacy firewalls and in network intelligence with Centripetal CleanINTERNET Service:

FEATURE	FIREWALLS	CENTRIPETAL CLEANINTERNET SERVICE
Scalability	Limited amount on average of approximately 7-20,000 blunt, uni-directional rules. Cannot keep pace with evolving IOCs. Less than .01% available CTI coverage ratio.	Mass-scale Ingestion of billions of unique IOCs applied bi-directionally with highly granular per rule element inspection. Seamless updates without any disruption to the network.
Dynamics	Updating a conventional firewall requires a service window and a service outage. Millions of IOC elements change daily leaving a legacy firewall consistently out of date.	Patented live update technology enables continuous IOC updates without any drop-in traffic or gap in security inspection. Millions of updates processed daily, billions processed weekly.
Network Performance	High latency and packet dropping when approaching rule capacity, logging, using a multi-field rule, or performing any secondary inspection.	High performance software loosely filters at scale with the highest decision rate in the industry. Detailed primary and secondary inspection with full real time logging. Micro-second latency in excess of 100Gb/s capacity.
Security Performance	Deploys less than .01% of available CTI in operations leaving known TTP exposure of over 99%.[1] Stateful assumptions of trust. Inability to triage CTI events inline places huge burden on the SIEM with mass event triggering. Clouds security operations.	Greatly increases the efficacy of the security stack by Shielding against known malicious threats and TTPs with > 90% coverage ratio.[2] Zero-trust adaptive filtering of every single packet – always. Dramatic decrease of known risk ingested to SIEM prioritizing Advanced Threat Detection.
Analytics & Operations Performance	No ability to triage security operations on the basis of intelligence. No real time analytics.	Full spectrum intelligence defense run by Centripetal SOC with continual access to expert team. Cross customer and cross industry research and analysis delivered with tailored Shielding policies and individual Advanced Threat Detection. Real time event analytics with machine learning. Work directly as an extension of your team bringing extensive expertise.

[1] Based on 20,000 IOCs out of 200 million — Gartner, State of the Threat Environment 2016

[2] Webroot

COMMON CUSTOMER FINDINGS

Centripetal's customers all use enterprise-class firewalls from leading providers including Cisco, Palo Alto Networks, Fortinet, and Checkpoint. Common feedback provided after deploying in operations illustrates the positive effects on their network and the unprecedented visibility they have achieved.

KEY REPEATED CUSTOMER FINDINGS:

- Reduced firewall logs and SIEM ingested events requiring human review by 90%-99%
- Within 30 days of adopting a Shielding posture, utilizing approximately 95% of available intelligence without any observable mission impacts
- Discovery of previously embedded Advanced Threats including infected assets (printers, laptops, UPS) and the discovery of unknown IoT,BYOD and other assets
- Shielded massive waves of spamming from known malicious sources, VoIP fraud, Remote Access fraud, targeted phishing and malvertising,and intrusion attempts on common vulnerable public facing services (RDP, eCommerce Platforms, web applications, FTP, Telnet/SSH, remote access tools)
- Identified and mitigated DDoS type scans and reflection attacks
- Shielded against phishing link clicks from internal assets
- Identification of shadow IT assets actively under attack
- Scanning of IoT assets (HVAC Smart Panels)

FEATURES AND BENEFITS OF CENTRIPETAL CleanINTERNET

Centripetal's CleanINTERNET service uses an advanced intelligence driven gateway — the RuleGATE® that is your secure access point to the internet. The RuleGATE is a software-based system that can be deployed on any speed link and in physical or virtual form. Centripetal's RuleGATE has been independently verified to be the highest-performance, largest scale network filter that exists. The RuleGATE provides network filtering with undetectable latency.[3] An in network RuleGATE greatly increases your overall efficacy and security posture, working seamlessly as the boundary for your existing IT infrastructure. Service features include:

- **INSTALLATION:** Installation, configuration, and support by our implementation team.
- **THREAT INTELLIGENCE:** Over 90 integrated threat intelligence providers and over 3,000+ risk-based feeds to provide comprehensive and cost-effective coverage for any type of business (additional feeds can be easily integrated at no cost by our support team).
- **ENFORCEMENT:** Automated enforcement of billions of unique IOCs to provide effective Shielding and Advanced Threat Detection intelligence policies to prevent network infiltration and data exfiltration.
- **SHIELDING:** The first mode of our intelligence operations provided in CleanINTERNET is Shielding. This is an essential part of our operational model which iteratively eliminates "All risk, no mission" traffic from our Client environments. The operational benefits of Shielding make our extensive Advanced Threat Detection operations possible.
- **ADVANCED THREAT DETECTION:** With precision Shielding deployed the second mode of our service delivery is to implement extensive Advanced Threat Detection. We utilize all available intelligence to identify "possible & probable" risks and triage this event load through an extensive set of secondary inspection processes including deep packet inspection, payload analysis, ProbableCause™ PCAP collection, ProbableCause decryption-less inspection, and correlation analysis across provider, asset, and network status. This extensive and detailed analysis is possible because of our Shielding operations.
- **COMPLIANCE:** An embedded benefit of our Shielding operations is the satisfaction of certain network standard by enforcing criteria such as PCI DSS, ITAR, HIPAA, etc.

[3] ESG Validation Analysis, May 2018