FAR BEYOND
THE FIREWALL

Centripetal CleanINTERNET®

CENTRIPETAL

RISING COMPLEXITY IN NETWORK PROTECTION

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. Increasingly the firewall is ineffective in preventing malware from entering the network, (usually through various phishing mechanisms — email, chat, ads, etc.) creating 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 an 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®

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 in the number of rules they can deploy and the stateful assumptions they make on risk. With an everchanging threat landscape, the firewall cannot process large amounts of 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 threat intelligence powered CleanINTERNET®

Feature	Firewalls	Centripetal CleanINTERNET®
Scalability	Limited amount on average of approximately **7-20,000 blunt**, uni-directional rules. Cannot keep pace with evolving IOCs. Decreasing efficiency as ruleset grows.	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 filters at scale with the highest decision rate in the industry. **Detailed primary and secondary inspection** with full real time logging. Micro-second latency at up to 100Gb/s line speeds.
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.** 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.**	Enhances security with **>95% coverage against known threats.** Employs zero-trust adaptive filtering for every packet, reducing known risks in SIEM for prioritized Advanced Threat Detection

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

COMMON CUSTOMER FINDINGS

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

- Reduced firewall logs and SIEM ingested events requiring human review **by 90%-95%**
- Identified and mitigated **DDoS type scans** and reflection attacks
- **Discovery of previously embedded Advanced Threats** including infected assets (printers, laptops, UPS) and the discovery of unknown IoT, BYOD and other assets
- Identified and blocked **external reconnaissance of IoT assets** (HVAC Smart Panels)
- **Blocked spam**, VoIP fraud, remote access fraud, targeted phishing, malvertising, and intrusion attempts on public-facing services (RDP, eCommerce, web apps, FTP, Telnet/SSH).
- **Shielded** against latest phishing link clicks from internal assets
- After 30 days of deployment, utilizing approximately 95% of available intelligence, **no discernible impact** on business mission and services
- **Identified** shadow IT assets actively under attack

FEATURES AND BENEFITS OF CENTRIPETAL CleanINTERNET®

Centripetal's CleanINTERNET® 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/cloud form. Centripetal's RuleGATE has been independently verified to be the highest performance[3] network filter that exists. The RuleGATE provides network filtering with undetectable latency. 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 systems engineering team or partners.

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.

Advanced Threats

We analyze risks and detect advanced threats using deep packet inspection, payload analysis, ProbableCause™ PCAP collection, decryptionless inspection, and correlation analysis.

Threat Intelligence

Centripetal monitors over 250 threat intelligence providers selecting 3,500 risk-based feeds to provide comprehensive and cost-effective coverage for any type of business. This intelligence updates at a rate of 4 billion IOC changes daily

Shielding

CleanINTERNET's® shielding mode crucially eliminates non-essential traffic, enabling focussed extensive Advanced Threat Detection operations.

Event Reduction

A secondary benefit of our shielding operations is the significant reduction in security events and consequently reduced storage and analysis costs.

[2] ESG Validation Analysis, May 2018

FOR MORE INFORMATION

centripetal.ai