THE FIREWALL FALLACY

Are Firewalls Giving You a False Sense of Security?

CENTRIPETAL

ADDRESSING THE FAILING FIREWALL

Today's cyberwarfare leaves traditional enterprise firewalls floundering. Vendor attempts to evolve them into "Next Generation" technology can't mask the harsh reality: firewalls are outmatched and blindsided by the ever-growing arsenal of attacks. Today's security revolution is far beyond the legacy firewall. That appliance was never meant to dynamically triage the risk of every single connection using all global knowledge, and to do all of that in thousandths of a second (10^-6). That's what it takes today to close the detection to protection gap.

Despite being hailed as the first line of defense, firewalls consistently fail in the Era of Intelligence. Every major data breach has waltzed right past one, exposing sensitive data. **In 100% of data breaches there was a firewall, often the most modern variant, in place.**

So should I throw mine away? No. The systemic vulnerability stems from a functional crisis. The firewall is designed for network segmentation and for defining an enterprise's specific, static usage policy. That is an important corporate security investment that is custom and should be kept. The impossible burden arises with the idea that the legacy firewall will somehow evolve through bolt on packages to track and discriminate every global connection, by jamming in patches and a pointlessly small set of blunt rules. This is a recipe for disaster.

Most organizations lack the resources to even adequately manage static firewall rules of just several thousand. Policy analysis tools routinely find rule conflict and policy "shadows" which violate policy in even this simple set. Dynamic intelligence tracking is today on the order of tens of billions in aggregate with a daily flux of over one billion valid threat changes. No organization can run an effective intelligence-based security operations in the firewall. No firewall can process that set of data.

Enterprises face a cybersecurity spending conundrum. They must not throw good money after bad, doubling down on a failing firewall to try to drag it into an inevitable slaughter in the intelligence domain. It's time to face that challenge with a specialist. The security challenge has fundamentally changed. While core segmentation and enterprise acceptable use policy remain very important layers of defense the frontline of modern cyber is intelligence powered defense.

FUNDAMENTAL FAILINGS

Advanced threats bypass firewalls with ease, sneaking malware in through phishing attacks or by exploiting internal vulnerabilities. These firewalls often lack the muscle to stop malware from reaching out, phoning home to malicious servers, and stealing data.

Firewalls struggle in today's dynamic threat landscape. They rely on outdated methods like static IP deny lists, essentially checking packets one by one. This linear approach can't keep up with the ever-changing tactics of attackers. Legacy firewalls are also inflexible, limited in the number of rules they can handle and susceptible to misconfigurations. The real solution lies in threat intelligence, but firewalls simply aren't built to take advantage of vast amounts of threat data or make real-time decisions. They lack the ability to distinguish malicious traffic from legitimate, without disrupting network operations.

Modern attackers exploit this rigidity. They can quickly spin up cloud-based infrastructure that appears legitimate, rendering firewalls blindsided.

Firewalls are simply outmatched by the speed and sophistication of today's cyber threats.

Relying solely on firewalls is a recipe for disaster. Instead of acting as a shield, firewalls have become data spewing machines, bombarding SIEM or log management systems with event data in the hope of uncovering threats. Given the lightning-fast attack landscape, where threats can activate within minutes, this approach is delusional. Security teams drown in a never-ending deluge of alerts, unable to keep pace. There must be a better way.

CENTRIPETAL CLEANINTERNET®

Centripetal breaks the mold, disrupting the status quo, with a revolutionary approach to network defenses. We leverage the power of threat intelligence, applied wholesale at the network's edge, to keep you protected.

CleanINTERNET® is your intelligence shield.

This high-powered solution combines cutting-edge algorithms, expert security analysts, and advanced computing power to deliver unmatched protection. The economic benefits are not only realized in the short term - in a matter of weeks - but the investment here is minor considering the levels of protection and threat intelligence delivered.

CleanINTERNET® rewrites the script on cyber defense.

It prioritizes threat intelligence, transforming your defenses. Typically, organizations will wait for something to happen, hedging their bets and only reacting when a security incident occurs. We're different, and can provide adaptive and pre-emptive protection, blocking malicious traffic from entering your network. This empowers your security team to work smarter, not harder.

CleanINTERNET® seamlessly complements your existing firewall, deploying at the network edge.

It acts as a powerful shield, significantly reducing the malicious traffic bombarding your firewall and other security tools. By blocking all known threats at the gate, CleanINTERNET® frees your firewall to focus on their core network functions.

The following chart clearly illustrates the stark contrast between legacy firewalls and the game-changing power of CleanINTERNET® powered by threat intelligence.

	Firewalls	Centripetal CleanINTERNET®
Scalability	• Limited amount of blunt, unidirectional rules. (Typically, 7K-20K) • Cannot keep pace with evolving threats. • 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 technology enables continuous intel 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 minimal amounts of threat intelligence leaving known TTP exposure of over 99%. • Inability to triage security events inline places a huge burden on the SIEM with mass event storage.	• Greatly increases the efficacy of the security stack by Shielding against known malicious threats and TTPs with >90% coverage ratio. • Adaptive filtering of every single packet – always. • Dramatic decrease of events ingested to SIEM, with a reprioritization Advanced Threat Detection.
Analytics & Operations Performance	• No ability to triage security operations based on intelligence. • No real time analytics.	• Enhances security with >95% coverage against known threats. • Employs adaptive filtering for every packet. • Extensive reporting

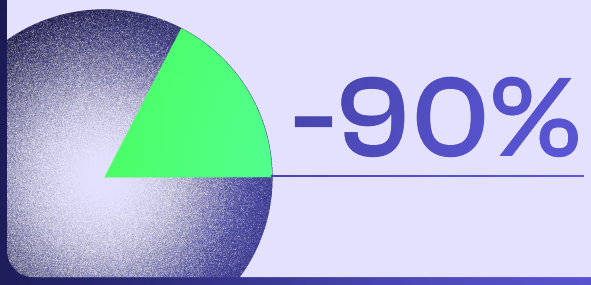
WHAT OUR CUSTOMERS EXPERIENCE

Centripetal's customers consistently report a significant improvement in their overall security posture after deploying CleanINTERNET®.

Here's how CleanINTERNET® helps security teams:

Reduced workload by 90-95%:

CleanINTERNET® significantly reduces the number of security alerts requiring human review, freeing up security teams to focus on strategic initiatives.



Expanded Visibilitying Hidden Threats:

CleanINTERNET® provides unprecedented visibility into the network, allowing for the discovery of shadow IT assets and identification of external reconnaissance attempts targeting IoT devices.

Proactive Threat Prevention:

CleanINTERNET® proactively stops DDoS attacks before they disrupt operations and prevents data breaches by blocking phishing attempts and malicious traffic at the network edge.

Unveiling Hidden Threats:

CleanINTERNET® proactively stops DDoS attacks before they disrupt operations and prevents data breaches by blocking phishing attempts and malicious traffic at the network edge.

Business Continuity:

Throughout this process, CleanINTERNET® seamlessly integrates with existing firewalls, ensuring no impact on critical business functions and services.

BENEFITS OF CENTRIPETAL CLEANINTERNET®

Centripetal's CleanINTERNET® uses an advanced intelligence driven gateway, which we term the RuleGATE®, that is your delivery point to a secure internet. The RuleGATE® is a software-based system that can be deployed on any speed link and in both physical and cloud environments.

Centripetal's RuleGATE® has been independently verified to be the highest performance network filter in existence. It provides network filtering with undetectable latency ensuring no disruption to your critical business operations.

This powerful security gateway seamlessly integrates with your existing IT infrastructure, acting as a robust shield at the network boundary. By harnessing the power of CleanINTERNET® and RuleGATE®, you gain a significant boost to your overall security posture.

SERVICE FEATURES INCLUDE:

Automated Threat Blocking:

Stop network breaches and data leaks with real-time enforcement of billions of threat indicators (IOCs) and advanced threat detection policies.

Advanced Threat Detection:

Uncover hidden threats with deep packet inspection, payload analysis, and PCAP collection. We even handle encrypted traffic for comprehensive protection.

Unmatched Threat Intelligence:

Centripetal monitors a massive network of over 250 threat intelligence providers, curating 3,500 feeds to deliver the most relevant and cost-effective coverage for your business. This intelligence is constantly updated, with 4 billion IOC changes processed daily.

Streamlined Security Operations:

CleanINTERNET®'s shielding mode prioritizes critical traffic, allowing your security team to focus on advanced threat detection with fewer distractions.

Reduced Security Costs:

By eliminating non-essential traffic, CleanINTERNET® significantly reduces security events, lowering your storage and analysis expenses.

EMBRACE INTELLIGENCE

Cyberattacks are a constant threat, putting immense pressure on businesses to fortify their networks. IT managers understand their vulnerabilities, but limited budgets often hold them back. Traditional firewalls have become a costly burden, draining resources with technology, management, event storage, and potential outsourcing fees.

Centripetal offers a smarter solution. By leveraging a powerful global threat intelligence network, we deliver a new layer of defense that saves you money and significantly strengthens your security posture. Don't settle for ineffective defenses. Embrace a new, intelligence-driven approach with Centripetal.

FOR MORE INFORMATION

centripetal.ai