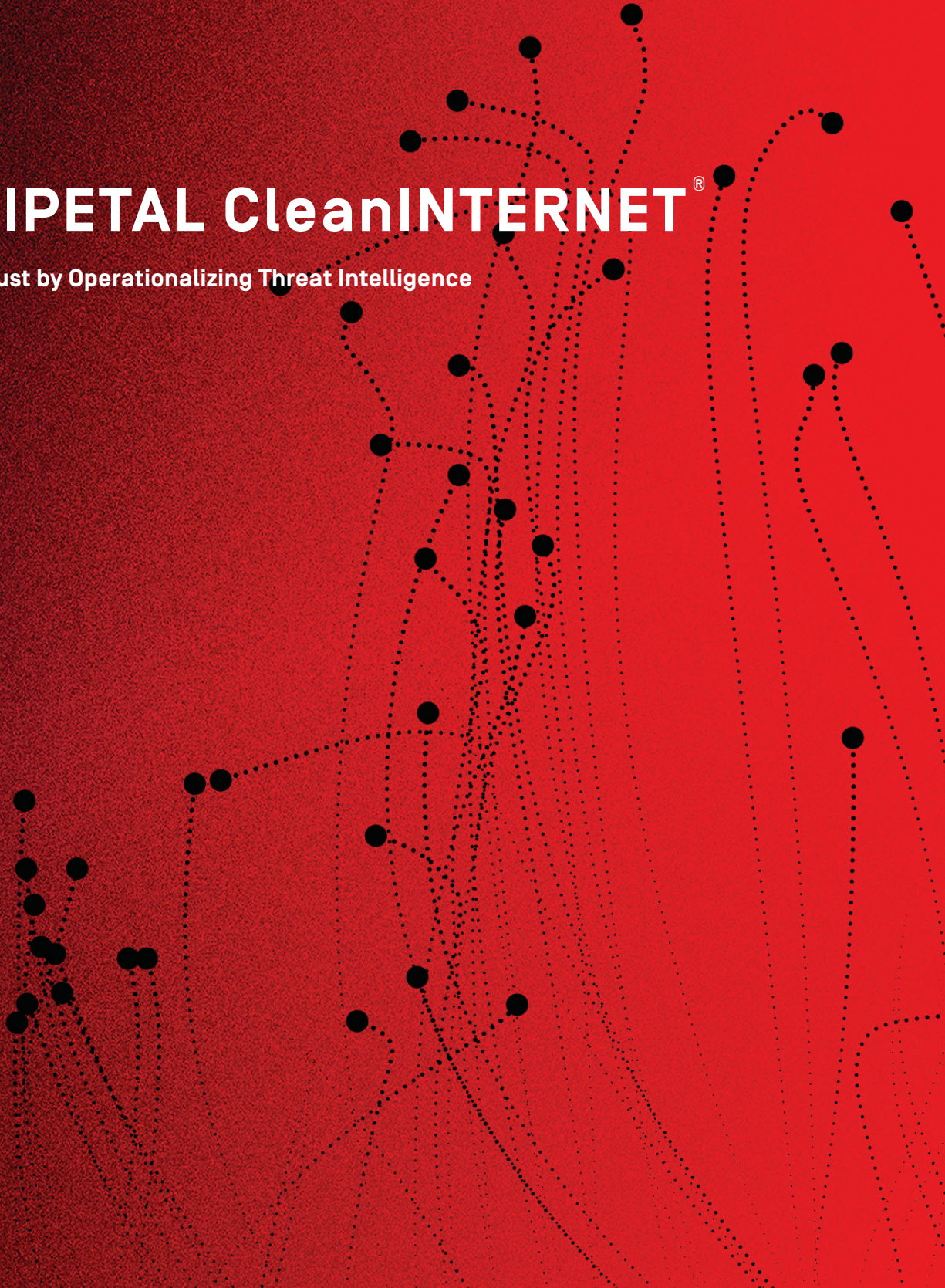




CENTRIPETAL

CENTRIPETAL CleanINTERNET[®]

Providing Zero Trust by Operationalizing Threat Intelligence



ZERO TRUST IS A COMMON BUZZWORD IN THE CYBERSECURITY WORLD, AND THERE IS CERTAINLY NO SHORTAGE OF PRODUCTS IN THE MARKET TODAY.

However, most cybersecurity offerings today are designed to be reactive, such that they analyze security incidents after the event has occurred. Adopting a zero trust mindset requires a more proactive approach that can help an organization prevent incidents from happening in the first place. This enables cybersecurity teams to stay ahead of potential threats and eliminate the tremendous noise and false positives that regularly consume them and the threat intelligence solutions they might be using.

THE CENTRIPETAL DIFFERENCE

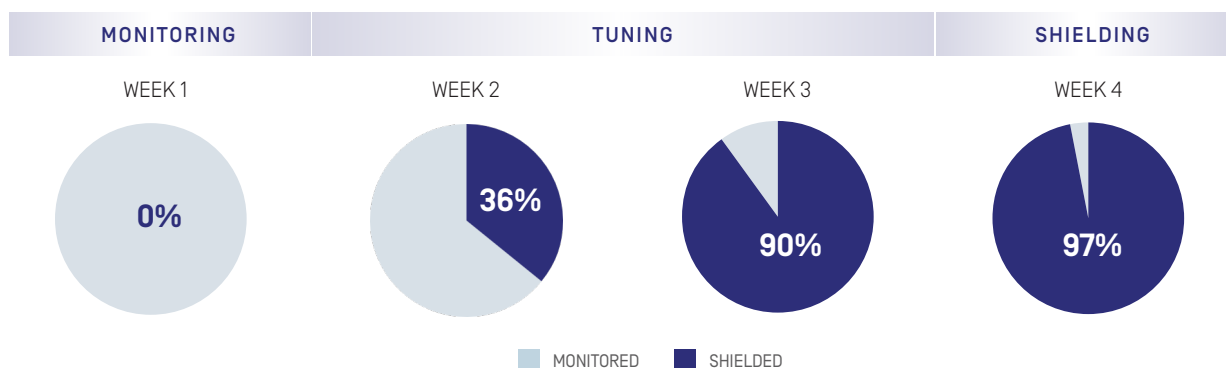
Centripetal CleanINTERNET goes beyond traditional cyber threat intelligence to operationalize intelligence with a combination of automated shielding, advanced threat detection (ATD), and an elite team of human threat analysts.

Unlike traditional threat intelligence solutions that are designed to provide forensic, post-attack analysis, CleanINTERNET is a fully managed SecOps as a service that proactively shields malicious inbound and outbound traffic from an organization's network automatically. Because CleanINTERNET shields known threats before they enter the network, it makes existing network inspection solutions 100x more efficient while also helping overcome the ongoing cybersecurity skills gap.

CleanINTERNET provides:

- Zero trust protection with bi-directional traffic inspection to proactively shield 99% of known attacks by checking every packet against billions of cyber threat indicators in real-time
- Real-time visibility into the threat landscape by aggregating and correlating more than 3,500 global threat feeds in a single, fully managed service
- A solution for the cybersecurity skills gap that helps overworked teams automatically eliminate known threats, interpret new ones, develop countermeasures, and update their security policies
- Higher efficiency and effectiveness of existing security defenses by dramatically reducing the events, alerts, and log data of firewall, IDS/IPS, and SIEM platforms by up to 70%

THE PERCENTAGE OF THREATS DETECTED AND SHIELDED OVER A 30-DAY PERIOD DURING A PRE-CUSTOMER TRIAL



WHAT WE DO

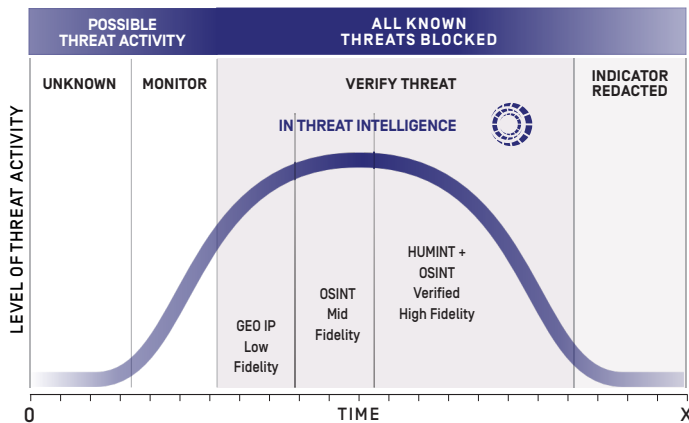
As a fully managed service, CleanINTERNET shields enterprises from 99% of cyber threats globally mapped by the threat intelligence community by using over 5 billion indicators of compromise (IOCs) from more than 3,500 feeds. This ensures a superior level of security by analyzing all inbound and outbound traffic across your organization in real-time.

In addition to its automatic threat shielding, the CleanINTERNET service includes the support of our elite SecOps team every step of the way. This seasoned team of cryptologists, security specialists, and former intelligence officers actively monitors your environment to provide ongoing secondary inspection analysis and full-service implementation, including:

- Planning, deploying, and testing the CleanINTERNET service to ensure it works seamlessly on your network without any disruption to your business
- Delivering ongoing full-service support based on the needs of your organization and specific industry
- Consulting with your team regularly to review the findings and recommend effective tactics to prevent emerging and zero-day threats

BLOCK 99% OF ALL MALICIOUS TRAFFIC WHILE INCREASING OVERALL NETWORK EFFICIENCY

THREAT LEVEL TIMELINE



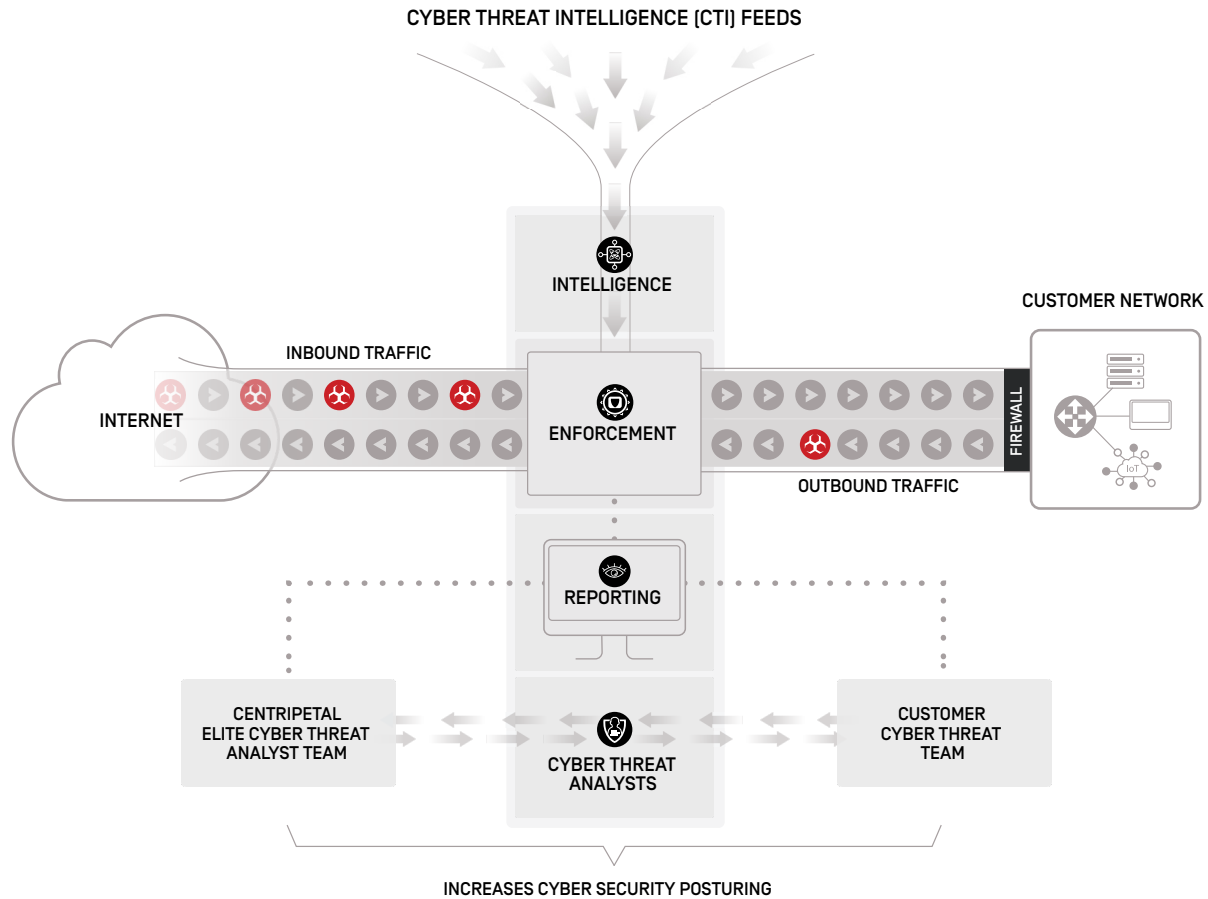
99% of all breaches come from known intelligence. CleanINTERNET allows you to prevent virtually all of these known breaches while increasing overall network efficiency. This is accomplished by the highest performance network filtering technology on the market. Independently tested and verified, Centripetal CleanINTERNET greatly increases the overall efficiency and security posture within the IT infrastructure.

Centripetal CleanINTERNET uses dozens of threat intelligence feeds to provide extensive coverage for any type of enterprise. If you are currently subscribed to a threat intelligence feed, it can be easily integrated at no cost by our support team. Supplemental industry and threat-specific subscription feeds are also available by request.

HOW WE DO IT

Unlike existing approaches, CleanINTERNET operationalizes cyber threat intelligence with a combination of automated shielding, advanced threat detection (ATD), and an elite team of human threat hunting specialists. CleanINTERNET's automated shielding applies 57 patents and proprietary algorithms to aggregate, filter, correlate, detect, triage and analyze more than 3,500 global feeds at massive scale and machine speed.

This provides the unique ability to shield an organization from 99% of globally mapped threats identified by the threat intelligence community in real time. CleanINTERNET not only filters virtually all globally known threats, but also uses artificial intelligence to identify potential new threats as they develop.



INTELLIGENCE

CleanINTERNET operationalizes threat intelligence by leveraging over 5 billion global indicators of compromise (IOCs) from more than 3,500 intelligence feeds in real-time. A host of patents and sophisticated machine learning allows the Intelligence component to aggregate and normalize all of this into one service that delivers comprehensive cyber threat coverage with the economics to support even smaller organizations.

ENFORCEMENT

The Enforcement component delivers automated enforcement based on policies made up of millions of complex rules, using billions of threat Indicators of Compromise (IOCs) compiled through the Intelligence component that are applied to the live network at machine speed. This is the first step toward transitioning to a zero-threat environment.

REPORTING

Our CleanINTERNET service includes executive- and analyst-level reporting on key findings of threats, suspicious activity, and historical reinforcement data. The cloud-based SIEM dashboard shows all inbound and outbound threat activity in real-time.

ANALYST

Centripetal's elite team of cyber threat analysts acts as an extension of your internal cybersecurity team to help monitor and analyze emerging and zero-day threats in the context of your business. This also helps overcome any skills gap your organization may have. With Enforcement being the first, the Analyst component is the second step in transitioning to a zero-threat environment.

OPTIONS TO FIT ANY SIZE ORGANIZATION

Regardless of your industry or the size of your organization, Centripetal offers a CleanINTERNET option perfect for your business.

Clean INTERNET EDGE

CleanINTERNET offers small and mid-sized organizations a cost-effective, fully managed option to shield their organization against virtually all known and evolving zero-day cyberthreats

Clean INTERNET ENTERPRISE

CleanINTERNET operationalizes threat intelligence to increase the effectiveness of an enterprise's existing security stack and enables internal networking and security teams to focus on other critical activities that are often ignored due to time constraints

Clean INTERNET LARGE ENTERPRISE/GOVERNMENT

CleanINTERNET is designed to support the most demanding, high performance environments, including those of global cloud service providers, critical infrastructure enterprises, and government agencies

IOT/OT/SCADA ENVIRONMENTS

Internet of Things (IoT) and Industrial IoT have grown exponentially and are vulnerable entry points into corporate networks and the critical infrastructure we rely on everyday. Because of their physical limitations, these connected devices often lack the security controls to keep them secure in a constantly changing threat landscape.

What's more, an integrated supply chain connecting IoT and operational technology (OT) devices from multiple business partners broadens the attack surface even further. Weak security enables hackers to exploit a single vulnerability and put all partners at risk.

Nation-state hackers and hacktivists consider critical infrastructure to be high-value targets because of the widespread implications to the general public. Shielding known threats from these networks is a highly effective strategy for preventing malicious attacks that can disable critical infrastructure and disrupt the lives of millions of people.

THE BUSINESS CASE FOR CleanINTERNET

The volume and velocity of cyber threats can overwhelm even the most skilled security teams. With billions of known attack indicators and a relentless stream of new ones, it's extremely difficult to distinguish the noise from the legitimate signals that might lead to a debilitating attack.

The traditional defense of signature-based threat detection and manual post-event analysis has proven to be highly ineffective at stopping breaches. However, by delivering zero trust through proactive intelligence, Centripetal CleanINTERNET can create tangible business value by:

- Delivering automated threat analysis and shielding that would otherwise cost millions of dollars in threat intelligence subscriptions and human analysts
- Solving the cybersecurity skills gap with an elite team of cyber threat analysts that provides continuous threat hunting on your behalf
- Increasing the efficiency of existing security defenses by dramatically reducing the events, alerts, and log data of firewall, IDS/IPS, and SIEM platforms by up to 70%
- Enabling industry and regulatory compliance for HIPAA, PCI DSS, GDPR, and others by providing superior protection against threats that can infiltrate networks and exfiltrate data
- Working with your cyber security team to ensure everyone understands the threats specific to your organization to boost your cyber security posture

WHY CENTRIPETAL

A cyber security service provider should be driven by revolutionary technology that is created by passionate people. At Centripetal, we are just that. We are experts in intelligence, with a team comprised of cryptologists, intelligence officers, and security operators from throughout the U.S. Intelligence & Defense community who have protected the most sensitive assets in the world. We are a cyber security provider that leverages our expertise to work directly with you to understand your cyber security needs and help meet your business objectives. For over a decade, we have developed state-of-the-art technology that sets us apart from competitors in performance, security coverage, and exceptional service and support.

For more information, visit www.centripetal.ai, or email us at sales@centripetal.ai



CENTRIPETAL

© 2022 Centripetal Networks Incorporated. All rights reserved. Centripetal, all Centripetal logos, CleanINTERNET, QuickTHREAT, RuleGATE, and ACT are trademarks or registered trademarks of Centripetal Networks in the United States and/or other countries. All other brands, products, or trademarks are property of their respective owners. This product/solution is subject to one or more U.S. or non-U.S. patents.

centripetal.ai