CENTRIPETAL

PRODUCT BRIEF

CleanINTERNET®

With up to 99% of all breaches caused by known threats, traditional security defenses are falling short in stopping even preventable attacks. Centripetal CleanINTERNET can help with a fully managed SecOps as a service that shields enterprises from 99% of cyber threats mapped by the intelligence community.

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

By automatically shielding 99% of globally known threats, CleanINTERNET eliminates the noise and false positives that regularly consume cybersecurity teams using traditional solutions. This enables internal teams to focus on the 1% of zero-day and emerging threats often tailored specifically to an organization or its industry.

Our team of experienced threat hunters can help there, too, by helping overworked IT teams detect and interpret new threats, develop countermeasures, and keep their security policies up to date.

CleanINTERNET uses 57 patented technologies and proprietary algorithms to aggregate, filter, correlate, detect, triage and analyze more than 3,500 threat feeds at massive scale and machine speed.

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.

CleanINTERNET EDGE

CleanINTERNET offers small and midsized locations and organizations a cost-effective, fully managed option to shield their organizations against virtually all known and evolving zero-day cyber threats.

CleanINTERNET 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.

CleanINTERNET 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.

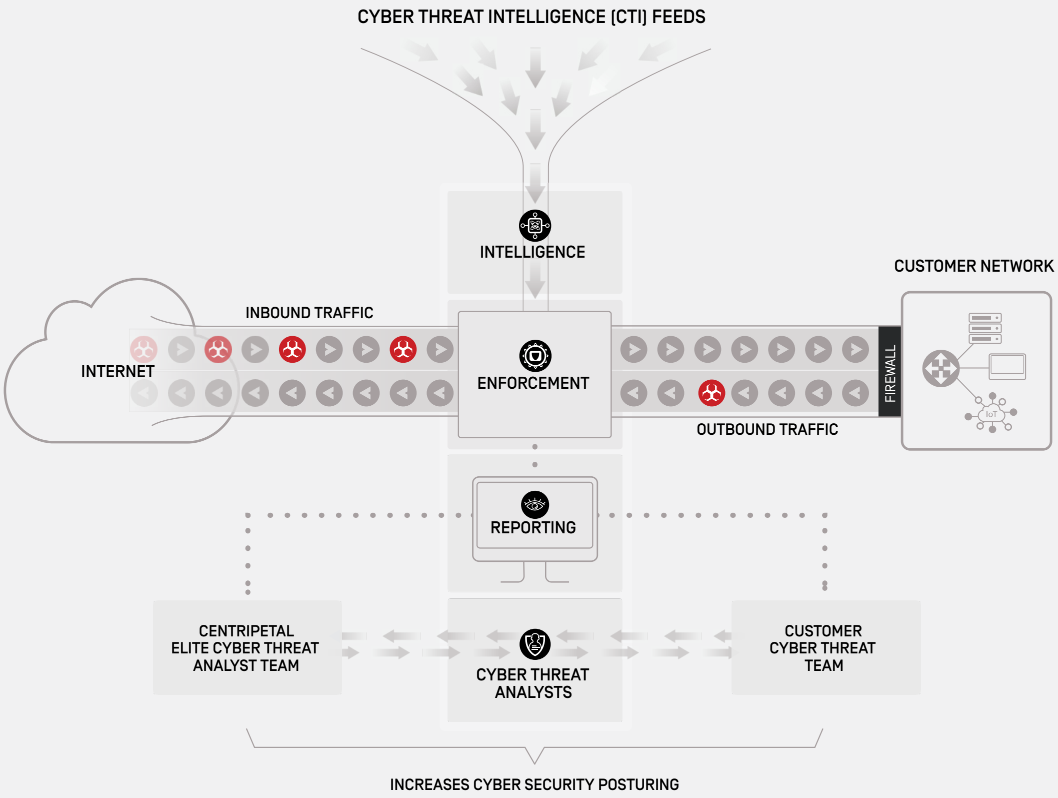
BENEFITS OF CENTRIPETAL CleanINTERNET:

- **All globally mapped threats are shielded automatically and at-scale**
- **Automatic shielding overcomes the reactive nature of traditional threat intelligence**
- **Security teams can spend more time on emerging and zero-day threats**
- **Context-aware protection around the clock**
- **Increases network performance by eliminating volumes of bad traffic**
- **Automatically identifies infected systems that could exfiltrate data**
- **Overcomes the cybersecurity skills gap, team burnout, and IT budget constraints**
- **Maximizes existing defenses (SIEM, IDS/IPS, Firewalls) by reducing event logs by up to 70%**
- **Includes integrated packet capture analysis (PCAP) for IDS/IPS**
- **Aggregates, correlates, and applies 3500 intelligence feeds that would cost millions of dollars**
- **Scalability to support unlimited rules/policies**
- **Fully managed SecOps as a service is ideal for organizations of any size**
- **Helps maintain compliance with PCI DSS, ITAR, HIPAA, and more**

HOW CENTRIPETAL CleanINTERNET WORKS

Unlike existing approaches, CleanINTERNET operationalizes cyber threat intelligence with a combination of automated shielding, advanced threat detection, and an elite team of human threat hunting analysts. 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 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 AI to identify potential new threats as they develop.


CYBER THREAT INTELLIGENCE (CTI) FEEDS
INTELLIGENCE
CUSTOMER NETWORK
INBOUND TRAFFIC
INTERNET
ENFORCEMENT
FIREWALL
IoT
OUTBOUND TRAFFIC
REPORTING
CENTRIPETAL ELITE CYBER THREAT ANALYST TEAM
CYBER THREAT ANALYSTS
CUSTOMER CYBER THREAT TEAM
INCREASES CYBER SECURITY POSTURING

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. It also allows access to a real-time cloud-based SIEM dashboard showing inbound and outbound threat activity.

ANALYSIS

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 in transitioning to a zero-threat environment.

CENTRIPETAL