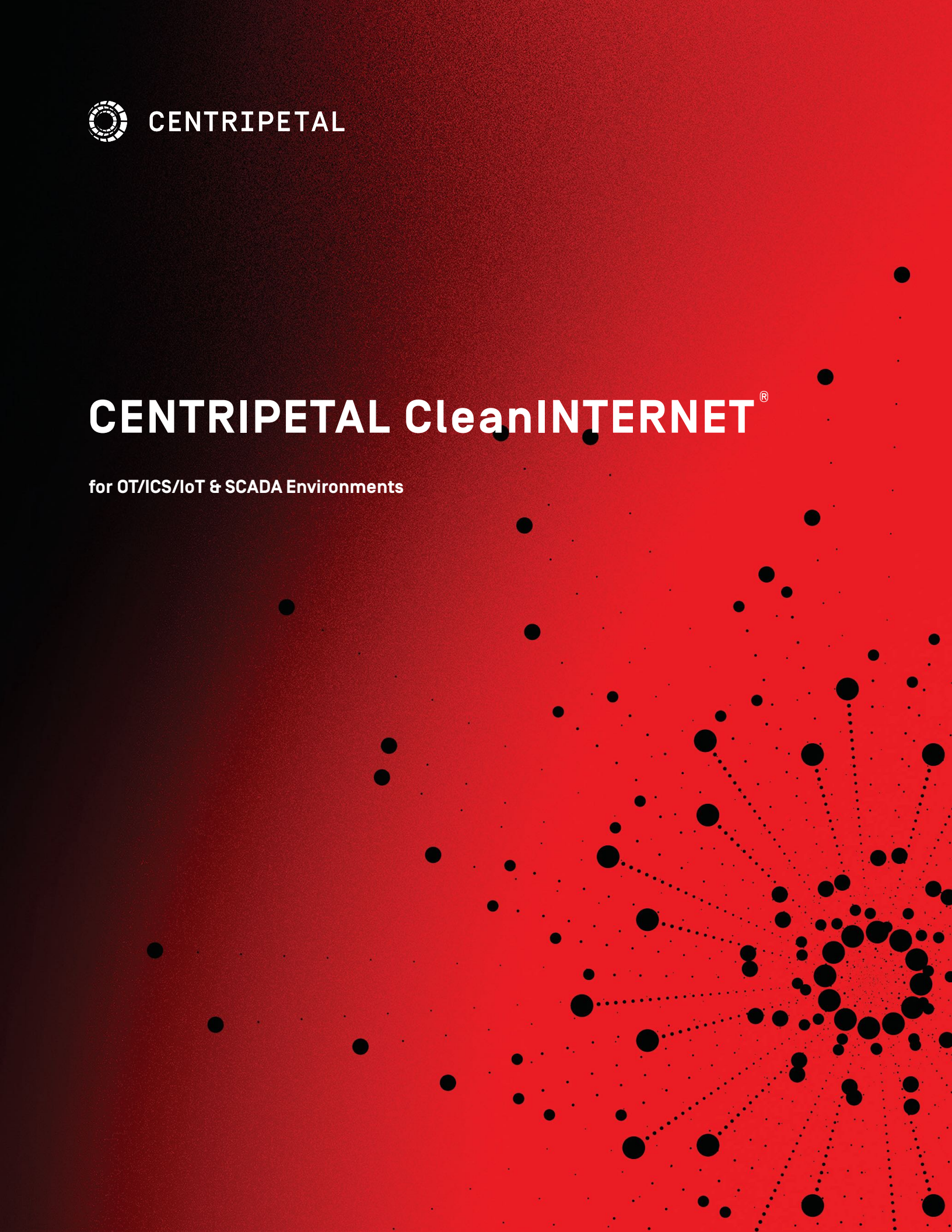
CENTRIPETAL

CENTRIPETAL CleanINTERNET®

for OT/ICS/IoT & SCADA Environments



INTERNET-CONNECTED DEVICES CONTAIN A VARIETY OF VULNERABILITIES AND SECURITY RISKS – especially since they are a targeted entry point into critical infrastructure (OT/ICS) that contains SCADA and IoT systems and other internal networks. IoT devices have physical limitations due to a small footprint which results in a lack of security.

As the number of connected devices increases, so do the security threats by way of entry points that can include partner/supply chain communication into the network which broadens the attack surface and increases attack vectors. This enables hackers to exploit the vulnerabilities in the system, and in many cases quite easily. There have been several high-profile breaches that have been the result of network infiltration through SCADA and IoT devices.

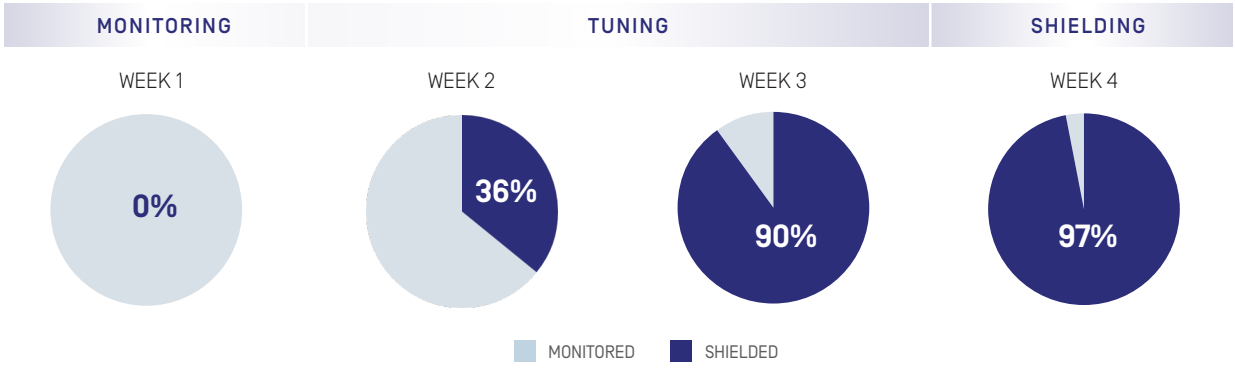
Nation-state hackers and hacktivism actors regard critical infrastructure in government agencies, municipalities, industrial facilities and businesses as high-value targets. Applying shielding against known threats is a highly effective part of the kill chain and prevents network infiltration and data exfiltration.

THE CENTRIPETAL DIFFERENCE

We offer our clients unsurpassed expertise in intelligence, having protected some of the most sensitive assets in the world. We combine a seasoned team of cryptologists, intelligence officers, and security operators from the private sector and the U.S. Intelligence & Defense community. We leverage decades of experience in combination with our highly advanced system technologies to determine, in advance, what would be most effective for our clients. Our team of highly experienced intelligence analysts and security operators remains continuously involved, providing client-specific full-service implementation, including:

- A highly experienced network operations team that will plan, deploy, and test Centripetal CleanINTERNET to ensure that it works seamlessly on your network without any disruption to your business.
- Full-service support from our security operations team. Based on your needs and operational cadence, we will consult directly to review the findings and recommendations from our customized event report.
- Context and recommendations to mitigate identified risks and protect your business-critical networks.
- Ongoing guidance to curate effective Shielding and Advanced Threat Detection Intelligence policies that will preserve your mission.

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



WHAT WE DO

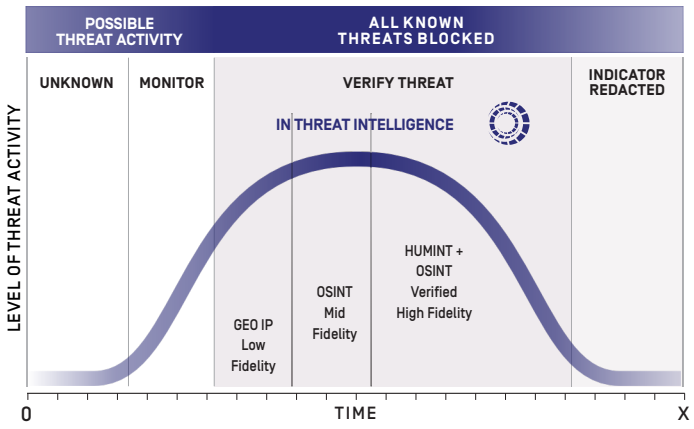
Centripetal's CleanINTERNET service offers personalized, client-centric services to help your organization's cyber security initiatives. CleanINTERNET is a cost-effective, industry agnostic solution for Shielding & Advanced Threat Detection that uses dynamic intelligence on a mass-scale. We leverage over 100 sources that contain more than 3,500 cyber threat intelligence feeds using Centripetal's Advanced Cyber Threat ACT® service, alleviating the burden of implementing complex cyber threat intelligence systems. CleanINTERNET monitors and analyzes mass-scale inbound and outbound traffic via an appliance gateway. Once malicious traffic is identified, the SIEM will deliver real-time analysis enabling monitoring or blocking according to your policy.

Centripetal CleanINTERNET offers you:

- **Zero Trust —** upfront mass-scale bi-directional shielding prevents network infiltration and data exfiltration to protect your organization's assets from known threats
- **Greater visibility into the threat landscape —** our elite team of cyber threat analysts easily customizes policies and enables trusted business-critical communication while performing constant threat hunting on your behalf
- **Greater efficiency for internal cyber security teams —** dramatically decreases the number of alerts and logs by up to 70%, enabling cyber teams to concentrate on mission-critical activities
- **Alleviates the burden placed on the security stack —** delivers greater efficiency to the cyber security infrastructure by helping to protect from DDoS and other attacks

BLOCK 90% OF ALL MALICIOUS TRAFFIC WHILE INCREASING OVERALL NETWORK EFFICIENCY

THREAT LEVEL TIMELINE



90% of all breaches come from known intelligence. CleanINTERNET allows you to prevent 99% 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 is delivered with core threat intelligence feeds that 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.

USE CASES AND DISCOVERY

Centripetal CleanINTERNET is used by several customers to protect their valuable IT, OT/ICS and SCADA assets. Centripetal's elite cyber threat analyst team has identified the following vulnerabilities within critical infrastructure:

- Verified and delivered contextual threat data and nation-state attribution.
- Delivered attribution information to LEAs relating to nation-state activity that resulted in network infiltration within government agencies and critical infrastructure facilities.
- Identified hosts that have established C&C communications in targeted networks that resulted in sensitive data exfiltration.
- Provided timelines and data of malicious activities.

Cyber security professionals need a solution that:

- **Protects their valuable IT assets and applications**
- **Safeguards employees, partners, and stakeholders**
- **Mitigates risk to deliver exceptional business value to the most complex organizations**
- **Provides personalized support and services to fit an organization's exacting needs**

THE BUSINESS CASE FOR CleanINTERNET

Cyber security has a conditional consequence associated with it, making it hard to assess value and the appropriate investment. However, by delivering Zero Trust through proactive intelligence, Centripetal CleanINTERNET can create tangible business value by:

- Delivering cost-effective mass-scale threat analysis that would require millions of dollars in manpower
- Helping to bridge the skills gap with an elite, intelligence-driven cyber threat analyst team that continuously provides threat hunting on your behalf
- Easing the burden on internal cyber security resources by increasing security stack performance and allowing your team to focus on mission-critical activities
- Enabling compliance (HIPAA, PCI DSS, GDPR, etc.) by thwarting off incoming threat traffic that can infiltrate your network and exfiltrate data
- Greatly reducing the risk of a damaging breach that would result in compliance fines and damaged reputation
- Working with your cyber security team to ensure your entire team understands the threats to your organization and dramatically increase 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