CIGENT

Cigent for Networks

Managed cybersecurity for small and medium business

Beat hackers at their own game with C4N.

Managed network detection and response made simple.

Simplify cybersecurity.

Featuring advanced plug-and-protect technology, Cigent for Networks™ (C4N) monitors traffic going into and out of your network—including Dark Web traffic—in real time. When threats, such as ransomware and network trojans, are discovered, C4N blocks them, stopping attacks as they happen. Alerts that require investigation are dispatched to the Cigent Cybersecurity Operations Center (CCOC) automatically. Best of all, C4N is affordable and fully managed by Cigent cybersecurity experts.

Prevent attacks with automated threat blocking.

Cigent for Networks monitors Internet-based traffic going into and out of your network. When threats are discovered, C4N traps and blocks them in real time, preventing attacks before they happen. When further analysis or attention is needed, alerts are dispatched automatically.

Play the game.

Cyberdeception techniques are used internally and externally to provide early, accurate cyberthreat detection. Outside your firewall, C4N provides a real-time view of network reconnaissance and attack attempts, and blocks all communication with threat actors. On your internal network, deception attracts and blocks threats, undetected malware, malicious insiders, and more. Alerts are sent to the CCOC immediately for investigation and remediation.

Deploy with ease.

Cigent for Networks is affordable, easy to deploy, instantly effective, and runs alongside any cybersecurity solutions you already have. It features two components—the Cigent Cyberthreat Sensor,™ an appliance that resides on premises, plugs into your network, deploys in less than 10 minutes, and updates automatically—and the cloud-based CCOC, where worldwide threat intelligence is continually aggregated, analyzed, and deployed. Aggregated alerts are triaged by our team.

Simplify network security monitoring.

Manned by our cybersecurity analysts, the Cigent Cybersecurity Operations Center (CCOC) offers turnkey monitoring and alert-response services. If you have your own security operations center—and prefer to manage alerts internally—we'll send feeds directly to you, in your format of choice.

C4N prevents attacks **before** they happen.

Apply the art of deception to **block threats.**

C4N detects and responds to attacks in real time.

Turn the tables on attackers.

Cigent Network Deception

The more complex a target is, the more effort that's required to compromise it. As a result, a hacker's first line of attack lands on the easiest targets—and Cigent for Networks is standing by with deceptive network traps.

The Cigent Cyberthreat Sensor disguises itself as multiple valuable, vulnerable targets. When a threat actor tries to interact with the sensor, C4N captures its information and blocks all communications between it and your network. Threat information is relayed to the Cigent Cybersecurity Operations Center, for analysis and response.

Gather, analyze, and dispatch intel.

Cigent Threat Intelligence Engine

Threat intelligence from Cigent Cyberthreat Sensors around the world—and from thousands of public, private, and government feeds—is captured and monitored by the Cigent Threat Intelligence Engine and disseminated to all Cigent Cyberthreat Sensors continuously.

Cigent Threat Relevance Engine

Threat intelligence is contextualized and ranked by the Cigent Threat Relevance Engine. Relevant threat indicators are dispatched to your Cigent Cyberthreat Sensors, to ensure network threats are identified and blocked. Results are relayed back to the Threat Relevance Engine, where inactive threats are archived and active threats remain blocked.

Hunt down threats and prevent attacks.

Cigent Network Packet Forensics and Threat Blocking

The Cigent Cyberthreat Sensor monitors traffic flow into and out of your network. Network packets are inspected, classified, analyzed, and logged, ensuring known and unknown indicators of compromise (IOCs) are revealed and blocked in real time.

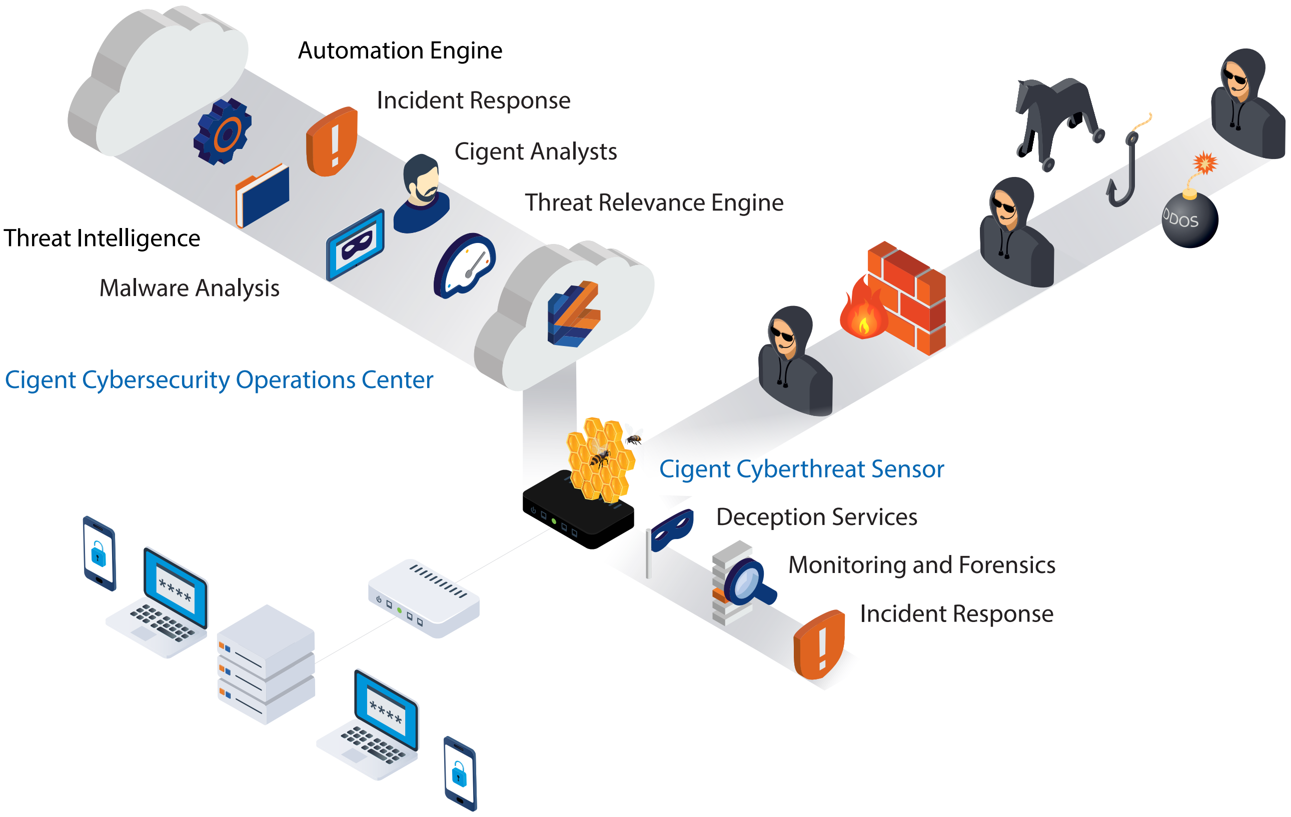
Handle alerts effortlessly.

Cigent Alert Automation

Network security is mission critical, but so is the work you do every day. Continuous security alerts disrupt workflow, turning a positive into a negative. Cigent Alert Automation takes the burden off you. Through intelligent automation, standard alerts are handled automatically. Only alerts that comply with specific criteria and behaviors are elevated and sent to the CCOC for evaluation and response.

Combine **relevant threat intelligence** with **threat sensing** to keep your network safe.

Stop cyberattacks before they start.



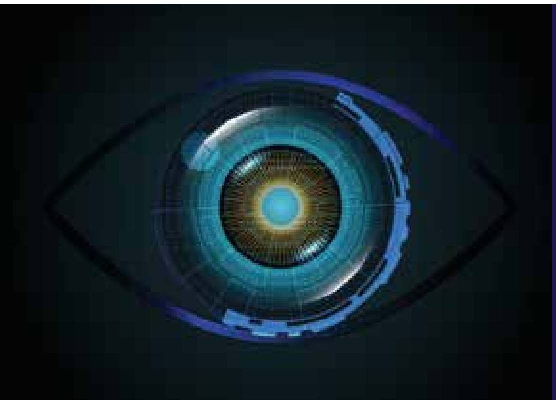
Cigent for Networks

Cigent Cybersecurity Operations Center

Based in the cloud—and monitored by our analysts—the Cigent Cybersecurity Operations Center (CCOC) examines threat intelligence, assesses its relevance, and continually updates Cigent Cyberthreat Sensors accordingly.

Cigent Cyberthreat Sensor

Based on premises, the Cigent Cyberthreat Sensor monitors all traffic running into and out of your network. When a threat is detected, the sensor blocks all communications between the threat and your network and send aggregated alert data is sent to the CCOC for analysis and response.



Cigent for Networks

About Cigent

Cigent Technology keeps the most valuable asset on your network safe—your data. Our cybersecurity solutions are built by an elite team, with backgrounds in NSA-level intelligence, ethical hacking to help public and private entities protect themselves, and data storage, including development, erasure, and recovery. As a result, our solutions beat hackers at their own game, and keep your data safe.

Contact us

Cigent Technology Inc.
2211 Widman Way Suite 150
Fort Myers, Florida 33901

Phone: 669-400-8127
Toll Free: 844-256-1825

Email us

General Inquiries
info@cigent.com

Sales Inquiries
sales@cigent.com

Partner Inquiries
partners@cigent.com

Visit us online

www.cigent.com

C4N Features at a Glance

Cyberthreat Sensor

Based on premises, the Cigent Cyberthreat Sensor monitors all traffic running into and out of your network. When a threat is detected, the sensor entraps it, blocking all communications between it and your network.

Deception Engine

The Deception Engine disguises itself as a valuable, vulnerable target on your network, setting a honeypot-style trap for cyberthreat actors.

Threat Relevance Engine

Threat intelligence from public, private, and government sources is analyzed and ranked by the Cigent Threat Relevance Engine. Relevant threat indicators are dispatched directly to your Cigent Cyberthreat Sensors.

Monitoring and Forensics

As traffic is monitored, data packets are inspected, classified, analyzed, and logged, ensuring known and unknown indicators of compromise (IOCs) are revealed and blocked.

Incident Response

When an incident occurs, the appropriate response is executed automatically. Alerts are dispatched, per your company's notification policies.

Cigent Cybersecurity Operations Center

Based in the cloud—and staffed by our analysts—the Cigent Cybersecurity Operations Center examines threat intelligence, assesses its relevance, and updates Cigent Cyberthreat Sensors continuously.

CIGENT