CIGENT

Cigent for Networks

Always on patrol

Beat hackers at their own game.

Choose advanced, affordable cybersecurity.

Cybersecurity is an ongoing battle for entrepreneurs and enterprises alike. Here's the good news—cyberthreats can be detected and blocked using advanced network traffic monitoring. Unfortunately, many companies don't have the expertise, technology, or resources to deploy and manage an effective solution. Cigent can help.

Prevent attacks by blocking threats.

Cigent for Networks™ monitors Internet-based traffic going into and out of your network. When threats are discovered, Cigent 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.

To foil hackers, Cigent for Networks uses deception tactics. Outside your firewall, Cigent provides a real-time view of network reconnaissance and attack attempts, and blocks all communication with threat actors. Used inside, network deception attracts and traps threats and undetected malware, blocks all communication, thwarting their attempts to gather information.

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 and plugs into your router, and the cloud-based Cigent Cybersecurity Operations Center, where worldwide threat intelligence is continually aggregated, analyzed, and deployed.

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.

Prevent attacks **before** they happen.

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

Cigent for Networks is always on the job.

Turn the tables on attackers.

Cigent Network Deception

The more complex a target is, the more effort that's required to hack it. As a result, a hacker's first line of attack lands on the easiest targets—and Cigent for Networks is standing by with a honeypot-style trap.

The Cigent Cyberthreat Sensor disguises itself as valuable, vulnerable target. When a cyberthreat appears, the sensor attracts the threat actor, 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 dispersal.

Gather, analyze, and dispatch intel.

Cigent Threat Intelligence Engine

Intelligence from Cigent Cyberthreat Sensors around the world—and from thousands of public, private, and government feeds—is captured by the Cigent Threat Intelligence Engine.

Cigent Threat Relevance Engine

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 Threat Relevance Engine, where inactive threats are archived and active threats remain blocked.

Hunt down threats and prevent attacks.

Cigent Data Packet Forensics and Threat Blocking

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

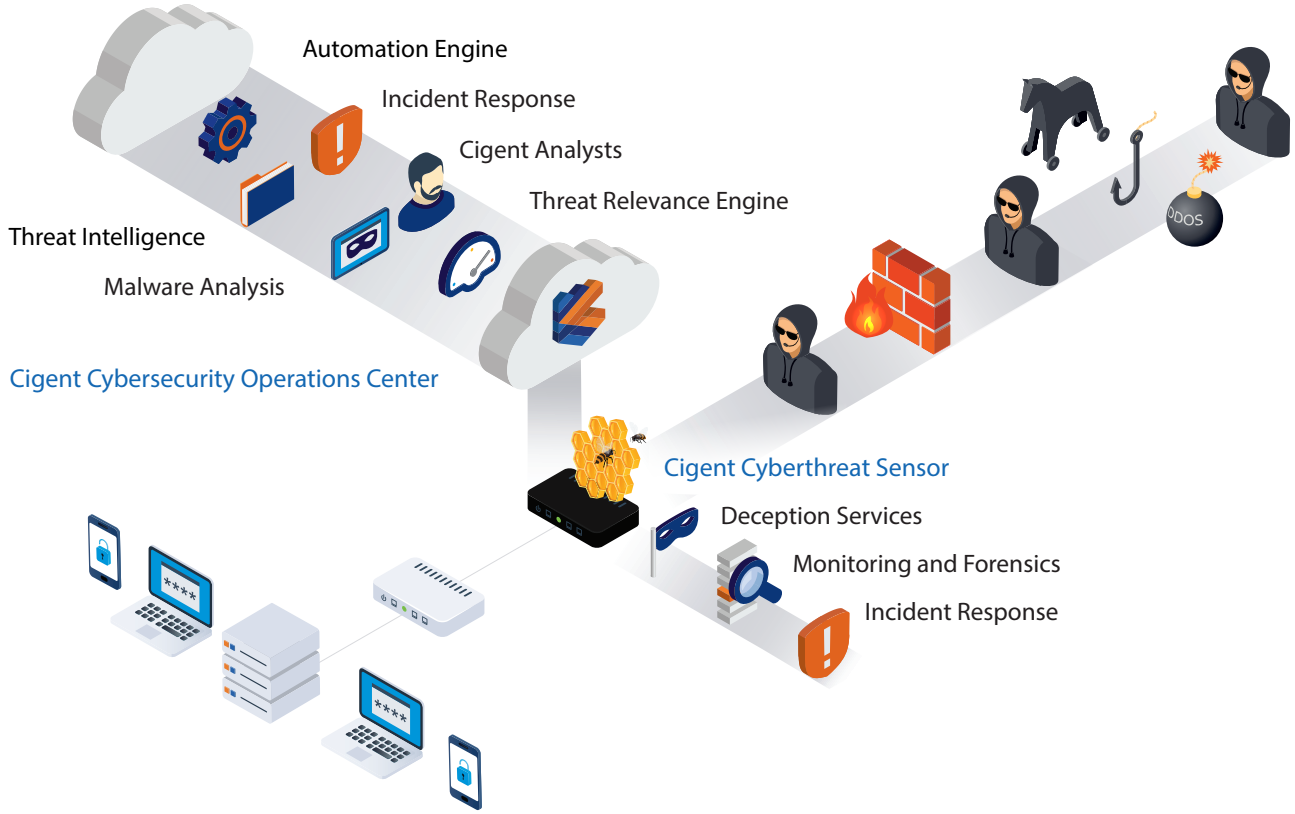
Handle alerts effortlessly.

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.

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 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 entraps it, blocking all communications between it and your network.

Cigent for Networks

Licensing Plans

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

Features	Silver	Gold	Platinum
Core Technologies			
Cigent Deception Engine	✓	✓	✓
Cigent Threat Intelligence	✓	✓	✓
Cigent Threat Relevance Engine	✓	✓	✓
Cigent Intrusion Detection and Prevention	✓	✓	✓
Cigent Security Monitoring	✓	✓	✓
One year of packet metadata log storage		✓	✓
Cigent Security Forensics		✓	✓
Deployment			
Managed installation	✓	✓	✓
Dashboard			
Real-time network threat and attack information	✓	✓	✓
Monitoring and Management			
Cigent Cybersecurity Operations Center	✓	✓	✓
Cigent Malware Analysis		✓	✓
Incident response planning			✓
Event and incident response services			✓
Real-Time Threat and Attack Response			
Threat hunting, detection, and blocking	✓	✓	✓
Attack tracking and response	✓	✓	✓
Endpoint intrusion detection			✓
Endpoint malware and incident response			✓
Escalation			
Report potentially compromised devices to appropriate personnel		✓	✓
Monthly Reports			
Detected and blocked threats	✓	✓	✓