STAY OFF THEIR RADAR.
AND KEEP THEM IN YOUR SIGHTS.

Affordable Managed Defense, Detection, and Response, designed to support lean IT teams and get them back to their other projects.

Autonomous Threat Defense

Shield the network edge by disrupting attacker reconnaissance, blocking in-bound exploitation attempts, and stopping outbound beaconing malware and ransomware in its tracks.

- The Outpost hides your network from would-be bad actors with our Network Cloaking technology.

- Shut down communication with known mailicious networks before it starts with CINS Active Threat Intelligence.

- Reduce the firewall's workload by up to 70% and enhance visibility into exploits, scans, and other malicious traffic.

- Protect and identify weaknesses and misconfigurations on the firewall and public-facing network.

Managed Network Detection & Response

Nomic's Insight provides an independent, SIEM-less, and Agent-less visibility tool to thwart today's insider threats and IoT exploits, monitored and backed by a 24/7 team of security pros.

- A team of experts monitors your network for critical security events and is available 24/7 for support, troubleshooting, and research.

- Automated real-time notifications for high-priority alerts, including C&C communications from malware and ransomware.

- Enriched threat intelligence data including ASN and geo-location, and a comprehensive customizable list of threat intelligence feeds.

- Passive logging of DNS, HTTPS/TLS, and other protocols for deeper analysis and threat hunting.

Nomic's HQ

- Review and correlate critical events across all of your device installations, using powerful filters to find the important alerts quickly.

- Search and filter network Flows in real-time

- Update configuration and threat feeds globally, and monitor the status of each Nomic device at a glance.

- Manage all your support tickets in one place, easily organized by ticket status, with quick links to our Support Center.

"Truly Great."

"The Nomic Networks products are an invaluable addition to our layered security model. They provide a solid product with great value and amazing support. The fully managed system provides exceptional protection and minimal "noise" allowing us to focus resources on other layers. Nomic has far exceeded not only our previous vendor, but our own expectations as well."

- *Network Administrator, a regional bank in Michigan*

WHAT SETS US APART?

A unique yet affordable take on the industry's most effective enterprise network security strategies, distilled down to a simple solution, and backed by real security experts, 24/7.

OUTPOST: MAKE YOUR NETWORK INVISIBLE TO THE BAD GUYS.
NETWORK CLOAKING™

Traditional inline security tools spot malicious packets and send an alert. They might drop a few malicious packets, but these bad actors remain free to scan your network, probing for additional attack vectors. We take a different approach with a proprietary methodology we call Network Cloaking. Instead of blocking a few packets, we drop all communication to and from malicious networks. Your network becomes completely invisible to the bad guys, as if you never existed at all. You stay safe, and they move on to other targets. One less bad guy to worry about.

INSIGHT: MUCH MORE THAN JUST A BLACK BOX.
MANAGED NETWORK DETECTION AND RESPONSE

Our MNDR solution ensures your network is actively monitored by autonomous systems, backed by real human beings 24/7. If there's a problem, you get an alert. If there's a network issue, we're troubleshooting. If there's a new threat brewing, we're already on it. And whether there are actionable events or false positives to work through, we're there to assess the situation, offer our 20+ years of expertise, and point you in the right direction. That saves you time and lets you get back to work.

THE COLLECTIVE BRAIN POWER TO STAY AHEAD OF THE LATEST THREATS.
CINS ACTIVE THREAT INTELLIGENCE GATEWAY

Stay out in front of threats before they come knocking at your network door with Collective Intelligence Network Security (CINS). Our managed Threat Intelligence Gateway continuously gathers attack data from Sentinel devices around the world, as well as reputable InfoSec sources. Each Sentinel device is continuously updated with this new CINS threat intelligence and dynamically blocks this malicious traffic before it reaches your critical infrastructure.

THE INTERNET

NOMIC-PROTECTED NETWORK

Web, VPNs, and valid traffic

Hackers, scans, and malicious traffic

INSIGHT

Servers, IoT Devices, and infrastructure

Firewall

ISP Router

OUTPOST

Workstations

NOMIC HQ

NOMIC MANAGED SECURITY OPERATIONS

DMZ

Ransomware, Malware, and Spyware