DISTRIBUTED DECEPTION WITH EASYNAC



TRANSFORMING NAC FROM PASSIVE CONTROL TO ACTIVE CYBER DEFENSE

EasyNAC is a trademark of InfoExpress, Inc. Other product and service names are trademarks and service marks of their respective owners. The products described in this document are protected by U.S. Patent No. 8,117,645, 8,112,788, 8,108,909, 8,051,460 and 7,523,484 and may be protected by other U.S. Patents or pending applications.

www.easynac.com

v3.2.250930

CONTENTS

Executive Summary 3

The Problem with Traditional NAC and Honeypots 3

How EasyNAC's Distributed Deception works 4

Integration with EasyNAC's Zero Trust Framework 5

Key Advantages 5

Use Cases 6

Why It Matters 6

About EasyNAC 6

EXECUTIVE SUMMARY

Modern organizations face sophisticated threats that easily bypass traditional perimeter defenses. Attackers exploit trusted access to move laterally within networks, often going undetected until significant damage occurs. Deception technology changes this paradigm by turning the network itself into an active defense surface.

EasyNAC introduces distributed deception -an integrated honeypot capability built directly into the Network Access Control (NAC) platform. With a single click, EasyNAC deploys virtual honeypots across every protected subnet, enabling real-time detection of malicious activity with near-zero false positives. This innovation delivers agentless, automated, and maintenance-free deception, empowering organizations to detect and contain threats before they escalate.



EasyNAC's deception technology complements its broader Zero-Trust architecture—combining malware lateral spread protection, automated threat response, and device fingerprinting for end-to-end network security.

THE PROBLEM WITH TRADITIONAL NAC AND HONEYPOTS

Legacy NAC solutions were designed for compliance, not active defense. They rely on switch integration, dynamic VLANs, and complex configurations—resulting in long deployment times and inconsistent protection.

Standalone honeypots, while powerful, also pose challenges: Require separate servers and constant updates. Provide limited network coverage. Demand specialized expertise to maintain.

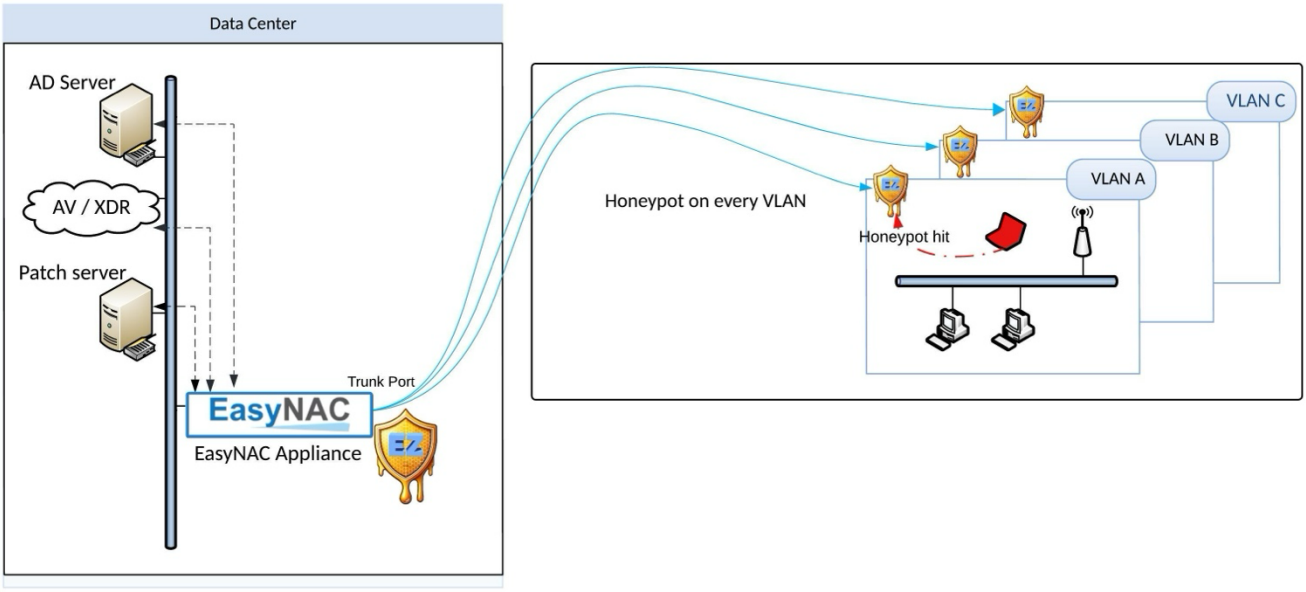
EasyNAC eliminates these barriers. It embeds deception at the access layer, enabling each protected subnet to host honeypot services without any new infrastructure, licenses, or ongoing management overhead.

HOW EASYNAC'S DISTRIBUTED DECEPTION WORKS

Deception, built in. EasyNAC automatically hosts decoy services (SSH, Telnet, SMB, and FTP) across every VLAN. Any connection attempt to these fake services is treated as a verified attack signal.

When a device interacts with a honeypot: 1. EasyNAC detects the attempt in real time. 2. Credentials used during the attempt are captured and logged. 3. The source device is immediately quarantined using ARP enforcement. 4. Security teams are notified instantly via email, Teams, Slack, WhatsApp, or Syslog.

No complex setup. No specialized hardware. Just proactive protection.



INTEGRATION WITH EASYNAC'S ZERO TRUST FRAMEWORK

Deception technology is part of EasyNAC's holistic approach to Zero Trust security:

- **Malware Lateral Spread Protection (Zero Day):** Detects devices scanning the network or attempting to connect to unused (Dark) IPs.
- **Automated Threat Response:** Integrates with any firewall, SIEM, or XDR via syslog, email, or API to quarantine infected devices.
- **Device Fingerprinting:** Protects against MAC spoofing by uniquely identifying each device based on multiple attributes.
- **Central Visibility Manager (CVM):** Provides unified reporting, license sharing, and policy management across distributed sites.

Together, these capabilities transform EasyNAC into a unified Zero Trust enforcement platform.

KEY ADVANTAGES

Capability	EasyNAC Advantage
Deployment	One-click enablement—no additional servers or configurations
Coverage	Honeypots automatically deployed on every VLAN or subnet
Accuracy	Near-zero false positives; only real attacker activity triggers alerts
Maintenance	Fully integrated—no standalone servers or updates required
Intelligence	Captures attacker credentials and behavior for threat analysis
Response	Real-time quarantine with multi-channel alerts
Cost Efficiency	No additional license fees or dedicated appliances

USE CASES

Financial Services: Detect lateral movement targeting core banking systems before exfiltration occurs.

Manufacturing & OT: Identify compromised IoT devices or unauthorized laptops attempting access to control networks.

Healthcare & Education: Monitor unmanaged medical or lab devices for unauthorized access attempts.

Service Providers: Contain malware propagation across distributed client networks instantly.In essence, the Central Visibility Manager not only ensures that EasyNAC scales effortlessly with the growth of an organization but also simplifies the management process, providing a holistic and integrated approach to network security.

WHY IT MATTERS

Traditional security focuses on prevention. EasyNAC adds **active deception and automated response** at the access layer—where attacks often begin. Its distributed honeypots transform each subnet into an early-warning sensor, detecting real attacks in seconds and isolating threats automatically.

By integrating deception directly into NAC, EasyNAC democratizes advanced cyber defense—making it accessible, affordable, and effortless to manage. Organizations gain continuous visibility, Zero Trust enforcement, and early breach detection in one unified platform.

Simple Control. Strong Security. Real Deception.

ABOUT EASYNAC

InfoExpress, Inc. is a Silicon Valley-based cybersecurity company with over two decades of innovation in network access control. Its flagship solution, **EasyNAC**, delivers agentless Zero Trust control for enterprises across financial, healthcare, education, and industrial sectors. EasyNAC is trusted by organizations worldwide to protect critical networks, prevent lateral attacks, and simplify compliance.

For more information:

www.easynac.com

sales@infoexpress.com