NetCyte is a next-generation NAC solution that provides dynamic and adaptive access control with unparalleled threat discovery.

Digital transformation and technology adoption is disrupting the way we live and work. In a hyper-connected world, businesses are challenged to provide access and robust security at the same time. Exponential growth in number and range of connected devices due to IoT and increased mobility is expected to be 29 billion devices by 2022. Such unprecedented growth and today's evolving landscape requires new methods for controlling access to the network.

Parallel to this growth, threats are evolving at an exponential rate with new methods for distribution, infection, infiltration and evasion. These new techniques are continually overcoming traditional cyber defences.

Business demands of BYOD and partner/guest access can result in devices accessing corporate networks which are not verified against corporate compliance and security posture.

NetCyte creates a holistic view of IT infrastructure by enabling 100% accurate discovery, classification and profiling of any device. NetCyte reduces the attack surface and minimises the impact of cyber threats originating from devices in the corporate networks.

Discover
Any device in the network is discovered in real-time and managed centrally.

Enforce
Enforce dynamic and adaptive policies across your entire infrastructure regardless of technology, user and device.

Enable
BYOD and security controls for guests and unknown devices.

Automate
Dynamic orchestration and automation of real-time security tasks such as network segmentation, remediation and compliance.

Product Benefits

- **Total Control of Infrastructure.**
- **Detection of Threats to Critical Systems.**
- **Total Visibility of Every Device in the Network.**
- **Lower Operational Costs.**
- **Manageable and Secure BYOD** (Bring Your Own Device).
- **Easy to Implement, Easy to Manage.**

NetCyte at a Glance

- **VISIBILITY**
  Real-time inventory and continuous profiling of users, devices and networks.
- **PROTECTION**
  Policy enforcement and baselining with in-depth threat discovery for users, guests and devices.
- **AUTOMATION**
  Automate guest access and remediation actions for uncompliant devices.
- **AUDIT & COMPLIANCE**
  Enabler for corporate compliance and regulations like PCI, HIPAA and GDPR.
- **RETURN ON INVESTMENT**
  Reduce administrative overhead, risks, and improve infrastructure management.

Technical Highlights

- Easy discovery without depending on network devices or traffic sniffing.
- Discover weak Windows and SNMP passwords on any device.
- Detect port scans and password breach attempts.
- Full functionality support with or without an agent.
- Flexible deployment options, no appliance needed in remote networks.
- Audit log tracking for detection of security events such as password changes, account lockouts, event log deletion and group membership changes.
- Advanced process analysis for discovering traffic flow.
- Discover hubs and stacked devices in the infrastructure.
- In-Depth threat discovery.
- Dynamic inventory analysis for all devices in the estate.
- Ability to integrate with any network device supporting a remote connection.
- Multiple methods for discovering and managing devices across all network topologies.
- Automate network segmentation by IP, device, user and Active Directory group.
- Orchestrate the quarantine and remediation of compromised devices.
- Full Active Directory integration down to organisational units and groups.

NetCyte Threat Discovery

- Processes Utilizing Network Ports
- Processes Creating Network Traffic
- Bandwidth Utilisation Analysis
- Network Connection Analytics
- Port Scan Detection
- Password Breach Attempt Detection
- Weak SNMP Credential Discovery
- Weak Windows Credential Discovery
- Malware Discovery
  - Malicious Driver Discovery
  - Malicious Service Discovery
  - Malicious Start-up Object Discovery
  - Malicious Scheduled Task Discovery

NetCyte Posture Analysis

- Any Supported Information Using WMI & Remote Registry.
- Endpoint Security Software Health Check.
- Critical Security Event Analysis (e.g. ClearAudit Log, Change Group Membership)
- Detection of Network Address.
- Translation Through Virtualization Platforms.
- File Existence & Version Analysis.
- Process & Service Analysis.
- Installed Software Analysis.
- Operating System Version Analysis.
- Real IP Address & Rogue DHCP & Static IP Usage Detection.

Hardware Requirements

Scale	Server
0-1000 Normalised Users*	1x 6 Core CPU, 16 GB RAM, 250 GB HDD Windows Server (Any Release), MS-SQL Standard (Any Release)
1001-5000 Normalised Users	1x 6 Core CPU, 16 GB RAM, 500 GB HDD Windows Server (Any Release), MS-SQL Standard (Any Release)
5001-10000 Normalised Users	2x 6 Core CPU, 32 GB RAM, 500 GB HDD Windows Server (Any Release), MS-SQL Standard (Any Release)
10000+ Normalized Users	For every 10000 Users using one NAC Server is recommended.

Features

Advanced threat analytics without needing an agent and/or appliance on networks.

Guest Networking with customisable captive portal.

Discover compromised guest devices without admin rights.

Ability to detect port scans and password breach attempts.

Agentless security log tracking.

Advanced scripting interface for executing commands on network devices.

Detection Methods

- ARP Sniffing
- DHCP Sniffing
- MAC & ARP Table Tracking DHCP Logs
- Port Mirroring

Prevention Methods

- ARP Redirection
- Disabling Switch Ports Changing VLAN on Switch Ports
- 802.1X
- ACL Management
- TCP Reset

About CyberCyte

CyberCyte is a UK based cybersecurity company that provides a framework of solutions based on the Circle of Zero Trust for identity management, network access control, and DNS security. Our integrated security solutions enable enterprises, governments and service providers to protect their users and digital assets seamlessly with minimum operational overhead..

Davidson House, Kings Road Reading UK RG1 4EU

+44 118 900 1422

www.cybercyte.com