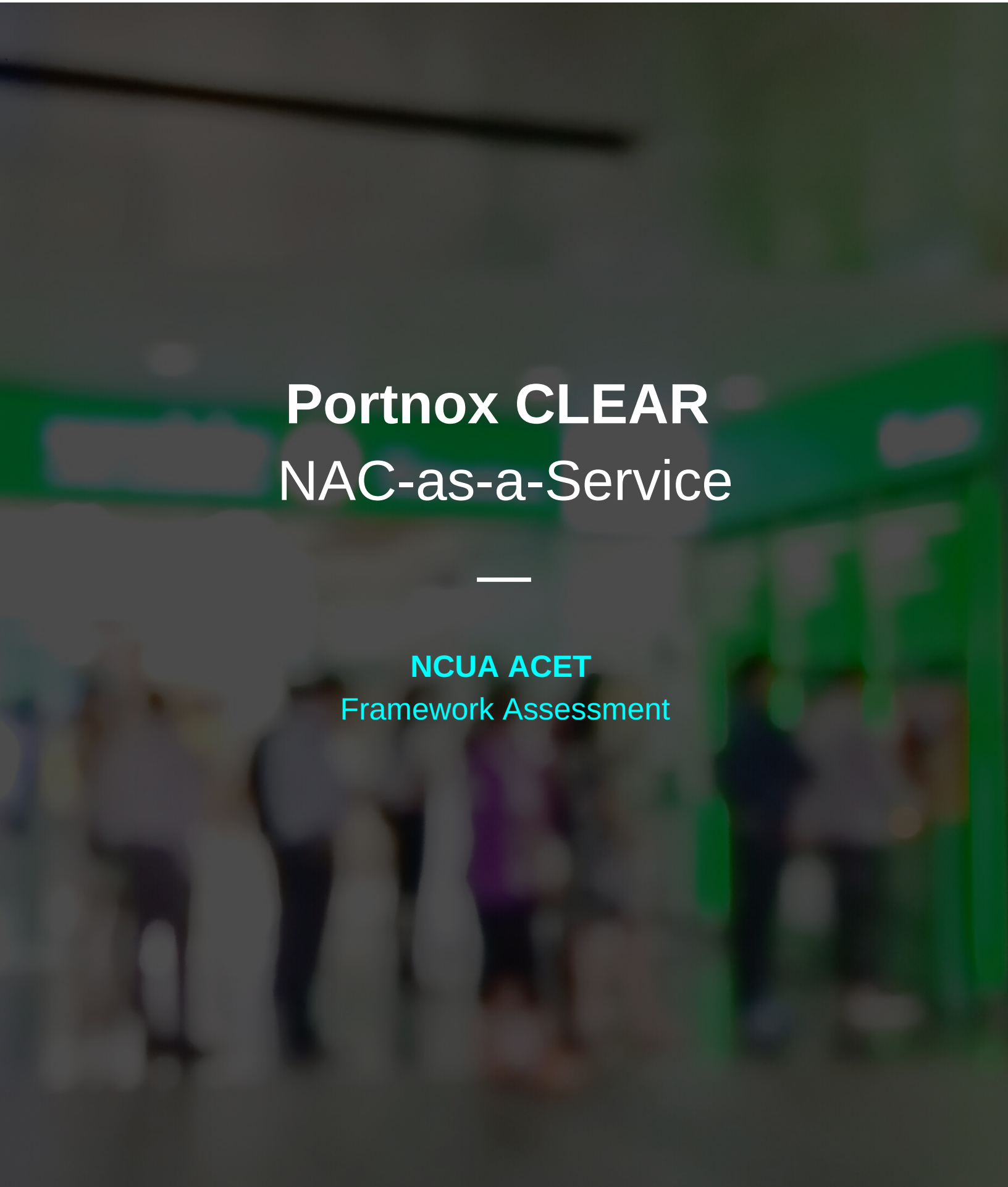

# Portnox CLEAR
## NAC-as-a-Service

—

**NCUA ACET**
Framework Assessment

As the NCUA audits continue to expand, many credit unions struggle with finding an effective solution to meet Domain 3 controls within the ACET framework.

Fortunately, Portnox CLEAR provides the network access control, endpoint awareness, risk and real-time remediation capabilities that either directly meet or highly contribute to many of the most difficult Domain 3 audit areas and requirements.

Here's how...

| Statement # | Domain | Assessment Factor | Component | Maturity Level | Category Declarative Statement | Portnox Value... |
|---|---|---|---|---|---|---|
| 188 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Baseline | Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices. | Contributes |
| 189 | | | | Baseline | All ports are monitored. | Meets |
| 190 | | | | Baseline | Up to date antivirus and anti-malware tools are used. | Meets |
| 192 | | | | Baseline | Ports, functions, protocols and services are prohibited if no longer needed for business purposes. | Contributes |
| 194 | | | | Baseline | Programs that can override system, object, network, virtual machine, and application controls are restricted. | Meets |
| 196 | | | | Baseline | Wireless network environments require security settings with strong encryption for authentication and transmission. (*N/A if there are no wireless networks.) | Meets |
| 199 | | | | Evolving | Technical controls prevent unauthorized devices, including rogue wireless access devices and removable media, from connecting to the internal network(s). | Meets |

| Statement # | Domain | Assessment Factor | Component | Maturity Level | Category Declarative Statement | Portnox Value... |
|---|---|---|---|---|---|---|
| 201 | 3: Cybersecurity Controls | 1: Preventative Controls | 1: Infrastructure Management | Evolving | Guest wireless networks are fully segregated from the internal network(s). (*N/A if there are no wireless networks.) | Meets |
| 205 | | | | Intermediate | The enterprise network is segmented in multiple, separate trust/security zones with defense-in-depth strategies (e.g., logical network segmentation, hard backups, air-gapping) to mitigate attacks. | Meets |
| 206 | | | | Intermediate | Security controls are used for remote access to all administrative consoles, including restricted virtual systems. | Meets on Some Architectures |
| 207 | | | | Intermediate | Wireless network environments have perimeter firewalls that are implemented and configured to restrict unauthorized traffic. (*N/A if there are no wireless networks.) | Contributes |
| 208 | | | | Intermediate | Wireless networks use strong encryption with encryption keys that are changed frequently. (*N/A if there are no wireless networks.) | Contributes |
| 213 | | | | Advanced | Anti-spoofing measures are in place to detect and block forged source IP addresses from entering the network. | Contributes |
| 214 | | | | Innovative | The institution risk scores all of its infrastructure assets and updates in real time based on threats, vulnerabilities, or operational changes. | Contributes |
| 215 | | | | Innovative | Automated controls are put in place based on risk scores to infrastructure assets, including automatically disconnecting affected assets. | Contributes |

| Statement # | Domain | Assessment Factor | Component | Maturity Level | Category Declarative Statement | Portnox Value... |
|---|---|---|---|---|---|---|
| 218 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. | Contributes |
| 219 | | | | Baseline | Employee access to systems and confidential data provides for separation of duties. | Contributes |
| 220 | | | | Baseline | Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls). | Contributes |
| 223 | | | | Baseline | Identification and authentication are required and managed for access to systems, applications, and hardware. | Contributes |
| 227 | | | | Baseline | Production and non-production environments are segregated to prevent unauthorized access or changes to information assets. (*N/A if no production environment exists at the institution or the institution's third party.) | Contributes |
| 229 | | | | Baseline | All passwords are encrypted in storage and in transit. | Complies |
| 230 | | | | Baseline | Confidential data are encrypted when transmitted across public or untrusted networks (e.g., Internet). | Contributes |
| 231 | | | | Baseline | Mobile devices (e.g., laptops, tablets, and removable media) are encrypted if used to store confidential data. (*N/A if mobile devices are not used.) | Meets |
| 232 | | | | Baseline | Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. | Meets |

| Statement # | Domain | Assessment Factor | Component | Maturity Level | Category Declarative Statement | Portnox Value... |
|---|---|---|---|---|---|---|
| 233 | 3: Cybersecurity Controls | 1: Preventative Controls | 2: Access and Data Management | Baseline | Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorized software. | Meets |
| 241 | | | | Intermediate | The institution has implemented tools to prevent unauthorized access to or exfiltration of confidential data. | Contributes |
| 244 | | | | Intermediate | All physical and logical access is removed immediately upon notification of involuntary termination and within 24 hours of an employee's voluntary departure. | Contributes |
| 245 | | | | Intermediate | Multifactor authentication and/or layered controls have been implemented to secure all third-party access to the institution's network and/or systems and applications. | Meets |
| 248 | | | | Baseline | Controls are in place to prevent unauthorized access to collaborative computing devices and applications (e.g., networked white boards, cameras, microphones, online applications such as instant messaging and document sharing). (* N/A if collaborative computing devices are not used.) | Contributes |
| 251 | | | | Innovative | Adaptive access controls de-provision or isolate an employee, third-party, or customer credentials to minimize potential damage if malicious behavior is suspected. | Meets |
| 254 | | | | Innovative | The institution is leading efforts to create new technologies and processes for managing customer, employee, and third-party authentication and access. | Contributes |

| Statement # | Domain | Assessment Factor | Component | Maturity Level | Category Declarative Statement | Portnox Value... |
|---|---|---|---|---|---|---|
| 256 | 3: Cybersecurity Controls | 1: Preventative Controls | 3: Device / End-Point Security | Baseline | Controls are in place to restrict the use of removable media to authorized personnel. | Meets |
| 257 | | | | Evolving | Tools automatically block attempted access from unpatched employee and third-party devices. | Meets |
| 258 | | | | Evolving | Tools automatically block attempted access by unregistered devices to internal networks. | Meets |
| 259 | | | | Evolving | The institution has controls to prevent the unauthorized addition of new connections. | Meets |
| 260 | | | | Evolving | Controls are in place to prevent unauthorized individuals from copying confidential data to removable media. | Meets |
| 261 | | | | Evolving | Antivirus and anti-malware tools are deployed on end-point devices (e.g., workstations, laptops, and mobile devices). | Contributes |
| 263 | | | | Evolving | The institution wipes data remotely on mobile devices when a device is missing or stolen. (*N/A if mobile devices are not used.) | Meets |
| 265 | | | | Intermediate | Mobile device management includes integrity scanning (e.g., jailbreak/rooted detection). (*N/A if mobile devices are not used.) | Meets |
| 267 | | | | Advanced | Employees' and third parties' devices (including mobile) without the latest security patches are quarantined and patched before the device is granted access to the network. | Contributes |

| Statement # | Domain | Assessment Factor | Component | Maturity Level | Category Declarative Statement | Portnox Value... |
|---|---|---|---|---|---|---|
| 284 | 3: Cybersecurity Controls | 2: Detective Controls | 1: Threat and Vulnerability Detection | Baseline | Antivirus and anti-malware tools are updated automatically. | Contributes |
| 289 | | | | Evolving | Antivirus and anti-malware tools are updated automatically. | Meets |
| 307 | | | 2: Anomalous Activity Detection | Evolving | Logs provide traceability for all system access by individual users. | Contributes |
| 317 | | | | Advanced | A system is in place to monitor and analyze employee behavior (network use patterns, work hours, and known devices) to alert on anomalous activities. | Contributes |
| 320 | | | | Innovative | The institution has a mechanism for real-time automated risk scoring of threats. | Contributes |
| 321 | | | | Innovative | The institution is developing new technologies that will detect potential insider threats and block activity in real time. | Contributes |
| 323 | | | 3: Event Detection | Baseline | Mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert management to potential attacks. | Contributes |
| 324 | | | | Baseline | Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software. | Meets |
| 326 | | | | Baseline | The physical environment is monitored to detect potential unauthorized access. | Meets |
| 327 | | | | Evolving | A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall). | Contributes |

| Statement # | Domain | Assessment Factor | Component | Maturity Level | Category Declarative Statement | Portnox Value... |
|---|---|---|---|---|---|---|
| 329 | 3: Cybersecurity Controls | 2: Detective Controls | 3: Event Detection | Intermediate | Event detection processes are proven reliable. | Contributes |
| 330 | | | | Intermediate | Specialized security monitoring is used for critical assets throughout the infrastructure. | Contributes |
| 331 | | | | Advanced | Automated tools detect unauthorized changes to critical system files, firewalls, IPS, IDS, or other security devices. | Contributes |
| 332 | | | | Advanced | Real-time network monitoring and detection is implemented and incorporates sector-wide event information. | Meets |
| 333 | | | | Advanced | Real-time alerts are automatically sent when unauthorized software, hardware, or changes occur. | Contributes |
| 335 | | | | Innovative | The institution is leading efforts to develop event detection systems that will correlate in real time when events are about to occur. | Contributes |
| 336 | | | | Innovative | The institution is leading the development effort to design new technologies that will detect potential insider threats and block activity in real time. | Contributes |
| 341 | | 3: Corrective Controls | 1: Patch Mgmt. | Evolving | Systems are configured to retrieve patches automatically. | Meets |

For more in-depth information on how Portnox CLEAR specifically fits into the above areas of the NCUA ACET framework, please visit: **www.portnox.com/ncu-acet**

portnox™

# About Portnox

Portnox provides simple to deploy, operate and maintain network security, visibility and access control solutions. Portnox software can be deployed on-premises, as a SaaS/cloud-delivered service, or in hybrid mode. It is agentless and is vendor agnostic, allowing organizations to maximize their existing network and cybersecurity investments. Hundreds of enterprises around the world rely on Portnox for network visibility, cybersecurity policy enforcement and regulatory compliance. The company has been recognized for its innovations by Info Security Products Guide, Cyber Security Excellence Awards, IoT Innovator Awards, Computing Security Awards, Best of Interop ITX, Cyber Defense Magazine and more. Portnox has offices in the U.S., Europe and Asia.

www.portnox.com // sales-us@portnox.com