SOLUTION BRIEF

CLEARPASS SECURE NETWORK ACCESS FOR HIGHLY SECURE ENVIRONMENTS

INTRODUCTION

Cyberattacks have become increasingly more intelligent, more targeted and more damaging. With a rapidly expanding attack surface that features mobile, BYOD, cloud and IoT, the likelihood of successful attacks continues to grow. Whether it's a government agency protecting vital infrastructure or a healthcare provider concerned about patient information – no organization is immune from the stress of preventing these attacks.

While government agencies have taken the lead in defining the criteria and processes by which products are certified, security teams need to know that the products they deploy to protect their organizations conform to a validated set of security standards.

Since 1999, governments around the world have participated in an ISO Standard Common Criteria testing and validation program. This program evaluates and ensures that Information Technology products perform to high and consistent standards, and contributes significantly to confidence in the security of these products. Today, 28 countries participate in the Common Criteria consortium through initiatives such as NIAP in the US, Agence nationale de la sécurité des systèmes d'information (ANSSI) in France and the Australian Signals Directorate. And as a result, Common Criteria certification is listed as a requirement on many government procurement RFP lists.

Aruba has been at the forefront of Common Criteria certification across its product portfolio, including wireless access points, controllers and remote (VPN) connection software. As a key element in Aruba's 360 Secure Fabric of leading-edge security solutions, ClearPass Policy Manager carries both FIPS and Common Criteria certifications.

CLEARPASS OVERVIEW

The ClearPass family of secure network access control products provide uniform, comprehensive and precision profiling, authentication and authorization for users, systems and devices seeking access to IT resources. ClearPass is designed to address key security challenges associated with an organization without IT boundaries including:

- **Complete visibility.** When network access can be granted from almost anywhere, at any time, with any device, knowing what is on the network is the first challenge. ClearPass provides extensive discovery and profiling to enable not just the security team, but all of IT to see who and what is connected. This is particularly important as IoT-type devices connect to the network.
- **Proactive control.** With ClearPass Policy Manager, every user, system and device on the network is given access to only those resources that their role requires. ClearPass authenticates every entity and assigns access privileges through policies that adjust permissions based on location, device used, time of day, type of user and other factors.
- **Closed-loop response.** Think of ClearPass as the gatekeeper of the network. The same policy engine that enables network access can be used to respond to a cyberattack. When an alert from the security ecosystem (firewalls, sandboxes, endpoint detection and response, SIEM, UEBA, etc.) is received, ClearPass can take a variety of policy-based actions from a re-authentication, bandwidth throttle, quarantine or block.

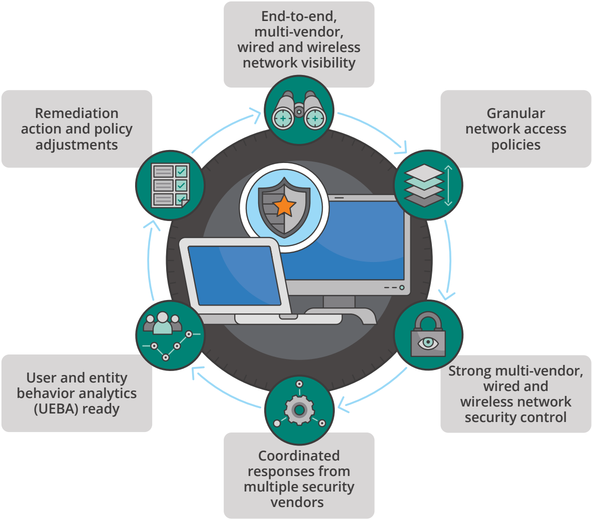
End-to-end, multi-vendor, wired and wireless network visibility
Granular network access policies
Strong multi-vendor, wired and wireless network security control
Coordinated responses from multiple security vendors
User and entity behavior analytics (UEBA) ready
Remediation action and policy adjustments

Figure 1: Aruba ClearPass provides a closed-loop approach to network access control and response.

THE CLEARPASS ADVANTAGE

- **Providing security assurance through Common Criteria certifications.** ClearPass is Common Criteria certified for the Network Device collaborative Protection Profile (NDcPP), covering all aspects of access control including encryption, physical security, certificate validation and processing and TSL/SSL processing, representing a security baseline for any network-connected device or system. In addition, ClearPass received Common Criteria certification for the Extended Package for Authentication Servers, which tests functionality and security specific to RADIUS authentication servers. This level of certification enables customers with extremely security sensitive environments, such as government classified networks, to use ClearPass to securely authenticate wired, wireless, and remote access users and devices.
- **Open and seamless integration.** Unlike other access control solutions that require a commitment to a single vendor's infrastructure, ClearPass is optimized to operate in any network. In addition, ClearPass integrates with over 120 security and general IT solutions to enable them to leverage the profiles and device context that ClearPass generates. Security teams are also utilizing ClearPass to either manually or automatically take action in response to a cyberattack.
- **One network, one view, one policy.** The ability for ClearPass to control the access to IT resources is not only independent from the vendor supplying the equipment, but also whether access is wired, wireless or remote. Organizations design and implement one policy per user or device and ClearPass seamlessly enforces this policy across the entire network topology. This provides time and cost savings that can be applied to other IT and security projects.
- **Optimized networks.** An ROI benefit of ClearPass is it's a policy-based enforcement of port access and utilization. Instead of designating ports for specific use cases (for connecting printers, servers, etc.), organizations can utilize a "colorless port" strategy where any port can connect to any device while ClearPass enforces the appropriate role-based access controls. This simplifies switch set-up and configuration and optimizes port utilization.
- **Ironclad access.** Verify, then trust. Some access control solutions allow any user or device onto the network and then take action if something goes wrong. This "laid back NAC" approach invites lightening quick cyberattacks where it only takes a second for malware to break into the network and launch a prolonged, highly damaging attack. ClearPass takes the approach where no user or device can gain network access without positive authentication and the appropriate policy authorization. When seconds matter, access control must start at T-zero.
- **Attack intercept.** The axiom is: "you cannot protect what you cannot see." One of the benefits of ClearPass discovery and profiling is total visibility. But in a world where every second counts in attack response, you also cannot remediate what you cannot see. By utilizing ClearPass to set up pre-determined responses to cyberattack signals from the security ecosystem, security teams can interrupt attacks before they do damage, while they continue to investigate and determine the extent of the breach.

SUMMARY

Common Criteria certification is a challenging process that requires security protection to be an integral part of a product's architecture and implementation. At one time, Common Criteria was something that only government agencies required, given the high value of the assets and information they were protecting. Today, every organization faces similar risks and consequences if a cyberattack is successful. With enhanced Common Criteria certifications, ClearPass not only delivers a secure foundation, but also a critical element of assurance to support the overall IT security strategy.