**Cyxtera**™

# Common Criteria (CC) Certification and Protecting Critical Infrastructure



## Secure Critical Infrastructure with CC Certified AppGate SDP

Today's modern organizations, both public sector and private, large or small, need to ensure secure access to critical infrastructure. It is imperative for organizations that are protecting security-sensitive or critical resources, to select solutions that undergo continuous and rigorous independent third-party validation. Any validation needs to be based on strict, established, and agreed-upon standards. Brigadier General Gregory J. Touhill (ret.), President of Cyxtera Federal Group stated that Common Criteria (CC) is the international "gold standard" for information technology security product certification.

### OVERVIEW

AppGate SDP, the leading network-enforced, identity-centric solution for accelerating the journey to Zero Trust, is Common Criteria Certified. The certification assures that AppGate SDP meets the most stringent security requirements of government entities for operating in security-sensitive or critical systems.

Originally a government-driven certification, its importance is also recognized by non-government businesses and organizations looking to acquire trusted security software solutions that are designed with compliance and performance in mind. Products evaluated against a Common Criteria standard exhibit a clear chain of evidence that the process of specification, implementation, and evaluation has been conducted in a rigorous and consistent manner.

1. Source: https://www.commoncriteriaportal.org/iccc/ICCC_arc/history.htm

### BENEFITS OF APPGATE SDP:

Grants access to enterprise resources based on contextual data including user profile, environment, and enterprise.

Provides complete visibility of network activity, including detailed information on resources accessed, users, and context.

Leverage native integration with cloud-specific security features to secure public cloud workloads and provide consistent access controls across hybrid environments.

Enables transparent remote and third-party access to network resources while eliminating the burden and vulnerabilities of VPNs.

Reduces the network attack surface and ensures a robust defense against DDoS, Man-in-the-Middle, and other attacks.

Leverages patented multi-tunnel capabilities to seamlessly connect users to applications wherever they run simultaneously.

## WHAT IS COMMON CRITERIA

The Common Criteria for Information Technology Security Evaluation, referred to as Common Criteria or CC, is an international standard (ISO/IEC 15408[1]) for computer security certification.

Common Criteria is recognized by 30 nations and was developed by the U.S., United Kingdom, Canada, France, Germany, and the Netherlands. It originated from three standards: ITSEC, CTCPEC, and TCSEC.  These standards were unified so that the government sector could select products that were all evaluated against one set of standards.

The CC standards cover processes for, evaluating and approving on an on-going basis, software and tools that are considered "trusted". Those labled "trusted" are therefore usable by the member countries leveraging and contributing to these standards or common criteria.

CC evaluations are performed by approved third-parties to establish and ensure the level of confidence that may be placed in the product's security features, through quality assurance processes.

Some definitions:

- Security Assurance Requirements (SAR) are descriptions of the measures taken to assure product compliance and are typically included in the CC.

- Evaluation Assurance Level (EAL) is a statement of the numerical value to show whether the standard completed meets the needs for the use by that agency or group.

- Protection Profile (PP) is a newer standard for IT evaluation.

- Security Functional Requirements (SFRs) specify individual security functions which may be provided by a product.

At this time, PPs are still relatively new and slowly replacing the EAL statements. It is most commonly used for evaluating IT components such as firewalls, operating systems, smart cards, etc.  When using a PP in an evaluation of a product, the PP will also include appropriate cryptographic requirements for CC evaluations that would typically be covered by FIPS 140-2 evaluation.

Although Common Criteria certification does not guarantee security, it can ensure that claims about the security attributes of the evaluated product were independently verified.

## APPGATE SDP AND CC CERTIFICATION

AppGate SDP was submitted for CC (ELA 2+) approval as part of Cyxtera's rigorous compliance program.  This third-party evaluation process leveraged both the EAL and PP. While there is currently no PP specifically for Software-Defined Perimeters, the evaluation did include several PP standards that are applicable to a Software-Defined Perimeter.

Among the specific security functional requirements (SFRs) that were evaluated as part of the CC process were: cryptographic support, life-cycle support, security management, identification and authentication, and user data protection.

"Deploying a Zero Trust strategy in today's dynamic cyber environment is essential, and AppGate SDP is the first-of-its-kind solution to achieve Common Criteria certification," said Brigadier General Gregory J. Touhill (ret.), President of Cyxtera Federal Group and former first Federal CISO during the Obama administration. "Achieving this certification demonstrates that Cyxtera is committed to providing the most secure solutions to combat modern threats that threaten the government, private companies, everyday citizens, and our way of life."

AppGate SDP achieved the following certification: Evaluation Assurance Level (EAL) 2+, which includes many of the Protection Profiles for secure network access. By receiving a certification of AppGate SDP based on these independently verified standards, it allows for entities looking to leverage AppGate SDP in their enterprise, to be comfortable that the technology is both sound and secure.

AppGate SDP is the first and only layer three Software-Defined Perimeter to be certified under the Common Criteria certification program. It can help secure your organization, public or private.

# THREE REASONS TO SELECT A SOFTWARE DEFINED PERIMETER THAT IS COMMON CRITERIA CERTIFIED:

## Standards-based third party validation

- AppGate SDP passed the rigorous independent third-party validation mandated by 30 countries, delivering both credibility and trust through the independent CC testing and attestation process.

## Improved Enterprise Risk Management

- Organizations managing risk rely on high and consistent standards as they implement their enterprise risk management programs. Those organizations leveraging products certified by CC, demonstrate cybersecurity due care and due diligence

## Ongoing Commitment to Excellence in Security

- When you invest in a product that is CC certified, you receive more than a secure product, you also gain a partner that demonstrates their commitment to the highest standards of information technology security

**IDENTITY-CENTRIC**

Designed around user and device identity. SDP builds a multi-dimensional profile of a user or device and authorizes users before granting access.

**ZERO-TRUST MODEL**

Enforces the Zero Trust model by applying the principle of least privilege to the network. It completely reduces the attack surface.

**BUILT LIKE CLOUD, FOR CLOUD**

Built for the cloud, and like the cloud. Engineered to operate natively in cloud networks, it's completely distributed and as scalable as the internet itself.