Symantec
A Division of Broadcom

Product Brief

Secure Access Cloud

Applying Zero-Trust Access to Applications Deployed in Cloud or On-Premises Environments

At A Glance

Software Defined Perimeter (SDP) architecture eliminates applications exposure:

- Securing access to corporate applications in cloud environments or on-premises datacenters.
- Enabling zero-trust application-level connectivity between authenticated users and applications
- Eliminating inbound connections to your network, making applications invisible to attackers

Flexible any-device, any-location, any-cloud deployment:

- Effortless deployment through a completely agentless solution which deploys in minutes
- Single platform to secure and manage access to any application in AWS, Azure, Google Cloud Platform (GCP), or on-premises data centers
- Supports any user and device including BYOD and third party devices

Granular application visibility and control:

- Fine-grained policies based on the users' identity, location device state, as well as sensitivity of the application or resource accessed.
- Continuously verified application access and govern user actions
- Full audit trail of user activities within an application—including URLs accessed, SSH commands executed, and RDP activities performed

The Need for Zero-Trust Secure Access for Cloud and On-Premises Applications

Providing access to corporate applications and services for authorized audiences was straightforward when everything was located in large corporate data centers and users all resided in predictable locations, using corporate-issued devices. When inside the enterprise's network perimeter, users had full visibility to see applications and services. When they were *outside* the perimeter firewall, they used tools like virtual private networks (VPNs) to get access to the corporate network and then accessed the applications required to do their work.

But the Cloud Generation has forever changed the way employees access information, and IT has worked hard to keep pace. The majority of organizations have begun moving applications to the cloud, and both mobility and access from anywhere are paramount. This transformation has created significant complexities for enterprises and has exposed the security vulnerabilities that exist in traditional network access technologies like VPNs. Today's dynamic business environment, sophisticated threats, and cyber-attacks present unique challenges that require a new mindset, one that moves past a perimeter-based approach reliant on traditional solutions which were not built for the cloud era and expose corporate networks and applications.

Secure Any-Device, Any-Location, Anytime Access to Applications and Resources in Cloud Environments or On-Premises Data Centers

The Secure Access Cloud is a cloud-delivered service providing highly secure granular access management for enterprise applications deployed in IaaS clouds or on-premises data center environments. This SaaS platform eliminates the inbound connections to your network and creates a software defined perimeter between users and corporate application and establishes application level access. This zero-trust access service avoids the management complexity and security limitations of traditional remote access tools, ensuring that all corporate applications and services are completely cloaked—invisible to attackers, targeting Applications, Firewalls, and VPNs.

When an authenticated user requests remote access to a corporate resource, the Secure Access Cloud creates a secure temporary connection between the user and the requested resource. A bi-directional https connection is established at the application layer and avoids the need to allow users onto the corporate networks. The connection is transient and automatically terminates once the user completes their task. With Secure Access Cloud, users gain access only to the specific applications and resources for which they are authorized. The solution takes the zero-

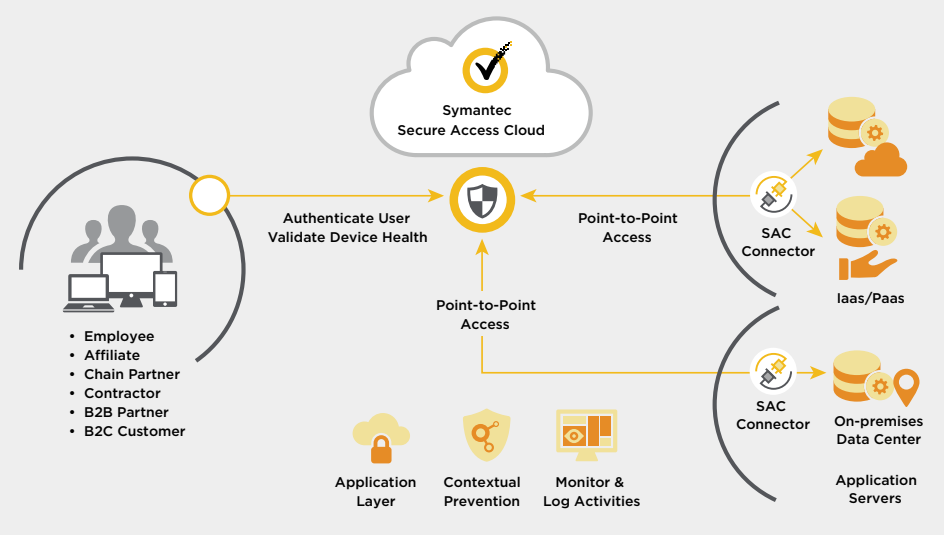
trust access approach further by providing full visibility, governance, and contextual enforcement for user actions—monitoring and logging every operation for simplified auditing and reporting.

Secure Access Cloud reduces complexity through a simple, agentless deployment, does not require deployment or maintenance of any security gateways or changes to existing security configurations, and easily integrates with existing identity and access management solutions. Authorized users can connect from anywhere in the world, using any device, and securely access any hosted application on distributed data centers of any type, either in a private or public cloud or on-premises data center.

Securing Access to Corporate Applications Migrating to IaaS

As enterprises migrate applications to cloud environments, IT teams seek to provide users with a simple and frictionless way of securely accessing enterprise applications while reducing the setup and maintenance complexity of existing tools that were not designed to address the security and compliance challenges of a perimeter-less world.

The Secure Access Cloud is a cloud-native solution that provides fast, agentless, secure access to corporate applications and resources, whether they are located in IaaS environments or on-premises data centers. Granular polices can define access controls based on user identity and device posture, as well as the sensitivity of the application being accessed and operations performed. This zero-trust access service never permits broad network-level access and instead offers narrow connections to specific applications based on the trust profile of the user.



Securing Access for BYOD and Third Parties

In today's modern workforce environment, mobility and BYOD have become the new norm. Employees must be able to access corporate applications easily and quickly regardless of their location or device used. In addition, the current dynamic business ecosystem often requires providing third parties such as partners and suppliers, or entities acquired via merger and acquisition activity, with access to corporate resources or systems. This access needs to be provided while avoiding exposing the corporate network to the security risks associated with unmanaged device connectivity. Symantec Secure Access Cloud is a cloud-native solution providing authenticated, zero-trust access to corporate resources without providing any network access. Your remote users and partner's employees can access specific applications based on their identity and device posture while the enterprise can take real-time actions to block undesired and suspicious activities.

Securing Access for DevOps Environments

DevOps teams require access to both production and development environments. Securing these environments from unwanted parties and unauthorized users is crucial to keeping business running safely. The Secure Access Cloud automatically provisions and deprovisions access to VMs, PaaS workloads, and applications in seconds, using a cloud-native, API-driven, agent-less solution to ensure all DevOps environment access is authenticated, provided just-in-time, based on the Principle of Least Privilege (PoLP), and fully audited and recorded.

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-SAC-PB100 March 30, 2020