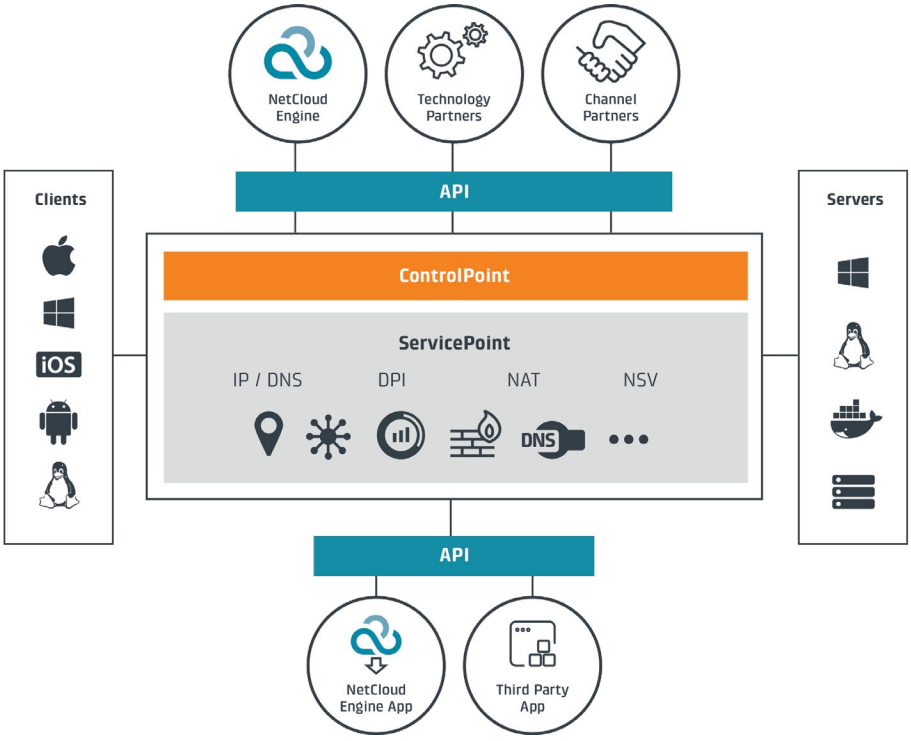
# NetCloud ENGINE

## Next-Generation WAN — Software Defined, Cloud Based

NetCloud Engine provides distributed, cloud-driven enterprises with a next-generation WAN — secure, software-defined, and delivered as a cloud-based service. The NetCloud Engine platform is fueled by SDN and virtualization software to eliminate the hardware, complexity, and operational costs of traditional WANs and extend the simplicity, security, and utility of Layer-3 LANs anywhere across the Internet.

Now IT teams can build and deploy virtual overlay networks in minutes to connect people, places, and things — like remote or distributed workforces, IoT devices, pop-up stores or kiosks, or digital signage — across any private or public cloud, and provide secure access for remote users using Windows, iOS, Android, or Linux devices.

NetCloud Engine works with existing network and security infrastructures. It requires no hardware or configuration, scales instantly, and is subscription-based — so you pay as you grow.




### Key Features:

*Simplicity*

- Deploys in minutes
- No configuration
- No changes to existing network infrastructure

*Security*

- Encrypted data-in-transit (256-bit AES)
- No data stored in cloud
- Private IP address space
- Enables micro-segmentation for zero-trust WANs
- Certificate-based Auto-PKI (X.509 CA)

*High Availability*

- Runs on top-tier cloud providers around the world
- Fully redundant architecture
- Self-healing, self-optimizing
- Seamless failover

*OS Support*

- Windows 7/8, Mac 10.7+
- Windows, Android, and iOS phones and tablets
- Windows 2008R2/2012 and Linux servers
- Docker containers

## Multi-Layer Security: Protects End-to-End, Everywhere

As enterprises continue to embrace workforce mobility, BYOD, and public cloud, protecting network borders and endpoints is no longer sufficient. NetCloud Engine's security foundation is a multi-layer, network-based approach to security that protects users, devices, and workloads wherever they're deployed. Key elements include:

- **Secure overlay:** Abstraction of logical network and address space from the Internet
- **Encryption:** Protects data-in-transit end-to-end with the strength of 256-bit encryption
- **Network virtualization:** Enables zero-trust WANs through micro-segmentation
- **Multi-layer authentication:** Device, virtual network, domain, and certificate level

These security building blocks help protect against a myriad of network-based attacks:

- IP address-related attacks (port scans, spoofing, DNS poisoning, and DDoS)
- Packet sniffing exploits (Firesheep and other nefarious sniffing programs)
- Authentication hacks (unchanged passwords, brute force, and single factor)

## Zero-Trust WANs: Contain Threats When & Where They Happen

As more subnets connect over the WAN, the "attack surface" of a breach or malware infection grows both inside or outside the firewall. To significantly limit the impact of such events, NetCloud Engine's virtual networks can be micro-segmented on a site, departmental, or even user and device level. The result is a zero-trust WAN that automatically isolates threats and quarantines them when and where they happen.

## Rapid Deployment: Define in Minutes, Deploy With Your Tools

Define and deploy virtual networks, connect local and remote users, small offices, IoT devices and sensors, kiosks, digital signage, and even VMs, containers, and servers in minutes rather than days. NetCloud Engine works with popular automation, orchestration, and client software distribution tools, including Puppet, Chef, and Microsoft SCCM.

*Business Benefits*

- Reduce WAN-related OPEX
- Eliminate hardware costs and complexity; pay as you grow
- Rapidly connect people, places, and things securely no matter their location
- Enhance security & compliance
- Enable BYOD

### Use Cases:

*IoT Devices, Sensors*

- Connect IP-enabled devices to secure network
- Enable remote control and management
- Leverage LTE and WiFi connections to eliminate costly cabling
- Reduce time to deploy from days or hours to minutes

*Enable Access to Resources Anywhere*

- Micro-segment networks with policy engine to enable appropriate access
- Connects any private and public cloud
- Provide application access across providers
- Extend existing networks without additional infrastructure
- Scales up/down instantly

*Remote/Mobile Access*

- Global availability
- Windows, Android and iOS mobile device support
- Persistent, always-on
- LAN experience
- Zero-trust—isolate access to select servers

*Extend Active Directory Domains*

- Maintain domain security
- Keep remote users always connected to AD domain from anywhere
- No user action required
- Eliminate cached passwords
- Instantly push policy and security patches
- Enforce AD DNS use

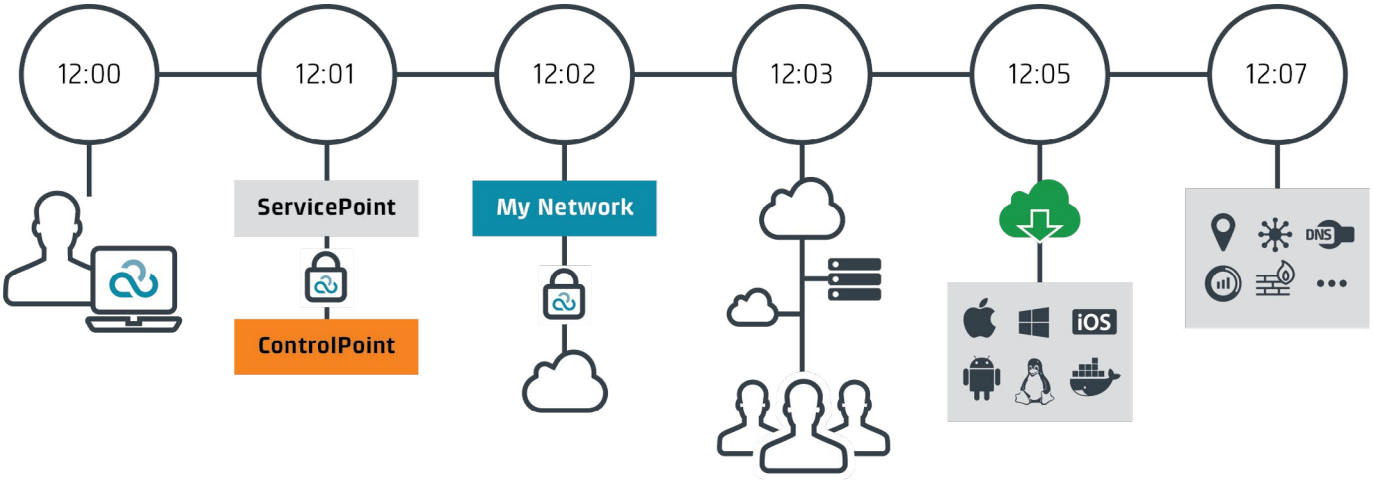
## Network Service Virtualization: Add Services without Appliances

Extend the visibility, security and control of cloud networks with NetCloud Engine Services and Network Service Virtualization. In a few clicks you can add services such as Active Directory integration, security policy deployment for microsegmentation, and network bandwidth monitoring.

## Power of the Cloud: Global Reach, Enterprise Scale, Full Resiliency

The NetCloud Engine platform overlays top-tier cloud data centers around the world, including Amazon AWS, Rackspace and Digital Ocean. This enables massive scale to accommodate large networks and traffic loads, and local points of presence to 80% of the world's computing population. When a disruption occurs, the platform's SDN and multi-cloud architecture enables affected networks to be automatically migrated to another data center—often within the TCP protocol connection timeout—so users' sessions are maintained and users themselves are often unaware of any issue.

GO TO **CRADLEPOINT.COM/NETCLOUD** TO LEARN MORE.




*12:00: Administrator names network. NetCloud Engine spins up L3 switch in cloud.*
*12:01: NetCloud Engine's ServicePoint securely calls ControlPoint to allocate network.*
*12:02: NetCloud Engine secures network with PKI & 256-bit AES encryption. Network is allocated.*
*12:03: Administrator adds devices to network, invites users, adds devices, servers, VMs, and even containers.*
*12:05: Users download on preferred OS enabling them to communicate securely, be located anywhere and be more productive!*
*12:07: Administrator layers on services—ADConnect, GeoView, Application Monitor, Firewall, IDS, etc.*