Security and Convenience — Simple with Gatekeeper

Remote access software can be invaluable for small businesses. Yet every time a port opens to connect with a machine outside of the network, an attacker gets to work trying to probe that access point, escalate credentials and compromise assets and/or infrastructure. **The threat of network exposure is very real.**

Remote access software is widely adopted for its ease, reliability, and affordability. However, remote desktop protocol (RDP) suffers from poor configuration practices, critical vulnerabilities, and increasing attacks. The FBI, NSA and DHS have all issued warnings about the risks to organizations that use RDP without adequate safeguards. **The industry needed a convenient, affordable, and reliable solution to secure remote access.**

Gatekeeper shields systems from the public Internet, unauthorized users, stolen credentials, probes, scans, botnets, brute force, targeted attacks and more.

**Businesses no longer have to weigh convenience against security — enjoy both with Gatekeeper.**

## Gatekeeper Benefits

* Secure
* Convenient
* Client-less
* No VPN overhead
* Auditor-friendly
* Single page listing of hosts user can access
* Works with multiple mobile devices

p.2

## Understanding Gatekeeper

Gatekeeper provides authenticated remote access without having to expose the RDP or Secure Shell (SSH) port to the public Internet.

Unlike traditional port forwarding, Gatekeeper requires end users to authenticate themselves via their AD credentials and a Two-Factor Authentication (2FA) verification code before they are allowed to access the destination host.

The secure and convenient Gatekeeper feature works with multiple mobile devices to offer:

* Multi-factor authentication (MFA) — only users that have been authenticated   
  using their name and password as well as an account-specific Gatekeeper One-Time Verification Code can gain access to the business’s RDP or SSH end point
* Administrator defined rules to grant users, or sets of users, controlled access to specified internal resources
* Secure, one time, source-specific transient firewall rules minimizing exposure to the outside world as the Gatekeeper portal creates a specialized connection to the end user’s IP address that isn’t visible to bad actors scanning for RDP targets

Unlike a VPN, Gatekeeper does not require a client software installation.

Gatekeeper addresses compliance requirements and facilitates adoption of best practices, including many outlined by NIST 800-53 and NIST 800-171.

Gatekeeper, a feature of Calyptix’s AccessEnforcer v5.0 and later, can be used with all types of devices (Windows, iOS, Android & more).

Leave space for our partner clients to add their own logo, CTA

* Questions about Gatekeeper? Contact us: 704.900.0422 | www.calyptix.com