Der SEC-Stick Server schützt Ihren Terminal-server – Einfach sicher!

Der team2work SEC-Stick Server: maximale Benutzerfreundlichkeit bei 100% Rundumschutz

Sechs schlagkräftige Argumente für den SEC-Stick Server

❶ Der RDP Server ist für Dritte unsichtbar

Damit ein Server über das Internet erreicht werden kann, muss auch der Serverdienst erreichbar sein. Dadurch können aber auch Angreifer sehen, welche Dienste bereitstehen und auf diese zugreifen.
Der SEC-Stick Server verhindert einen direkten Zugriff auf den Terminalserver **zuverlässig zu 100 %!** Der SEC-Stick Server steht „vor" dem Terminalserver und macht den Terminalserver für Angreifer unsichtbar: **Was ich nicht sehe, kann ich auch nicht angreifen!**

❷ Zusätzliche sichere Autorisierung

Damit der vorgelagerte SEC-Stick Server die Benutzer autorisieren kann, benötigen Sie Ihren privaten digitalen Schlüssel auf dem SEC-Stick. **Die Verwaltung der Schlüssel ist zentralisiert über das Management gelöst.** Es ist keine eigne Windows CA erforderlich. Der SEC-Stick Server verwendet das bewährte und robuste SSH V2 Protokoll. **Schützen Sie ihre Infrastruktur mit diesem zusätzlichen leistungsstarken Schloss.**

❸ Der Benutzer sieht nur seine persönliche Umgebung

Nach der Anmeldung sehen die Benutzer nur die für sie persönlich freigegebenen Ressourcen und können sich auch nur auf diese Verbinden. Der Zugriff auf Serverdienste wird vom Administrator zentral verwaltet.

❹ Kinderleichte Bedienung

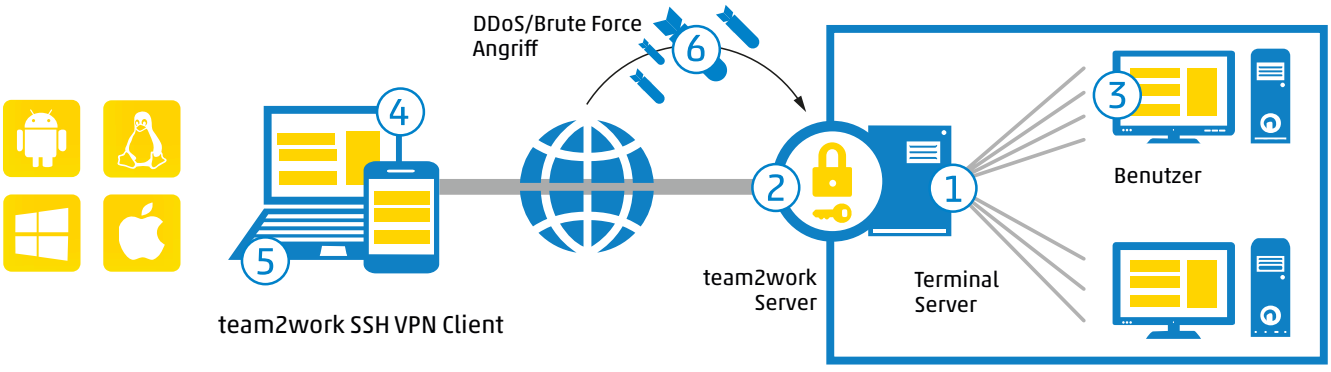
Die Benutzung des SEC-Stick ist kinderleicht und seit vielen Jahren erprobt. Im Bereich der sensiblen Medizin-IT wird unser SEC Stick seit vielen Jahren erfolgreich verwendet.

❺ Keine Installation von Clientsoftware nötig

Den SEC-Stick verbinden Sie mit einem Windows, Mac oder Linux PC per USB und Sie können direkt die Verbindung aufbauen. **Es ist keine Installation notwendig!**
Vergessen Sie virtuelle Adapter und komplexe Konfigurationen von IP-Sec Clients!

❻ Denial-of-Service und Bruteforce Schutz

Der SEC-Stick Server schützt das Netzwerk effizient gegen „Denial Of Service" Attacken und gegen „Bruteforce" Angriffe auf die Benutzerkonten.



Vorteil für den Benutzer:	Unterstützte Systeme:	Kerneigenschaften:
+ Made in Germany	+ Windows	+ SSH V2 Protokoll
+ 100% Zuverlässigkeit	+ Apple	+ Zentrale Schlüsselverwaltung
+ Kinderleichte Bedienung	+ Linux	+ Keine Client-Installation notwendig
+ Bundesweiter vor Ort Service	+ Android	+ Unterstützt TS-Broker
+ Top-Support		+ 2048 Bit RSA Keys
+ Über 10 Jahre Erfahrung		+ zentrales Management