# Endpoint Protection

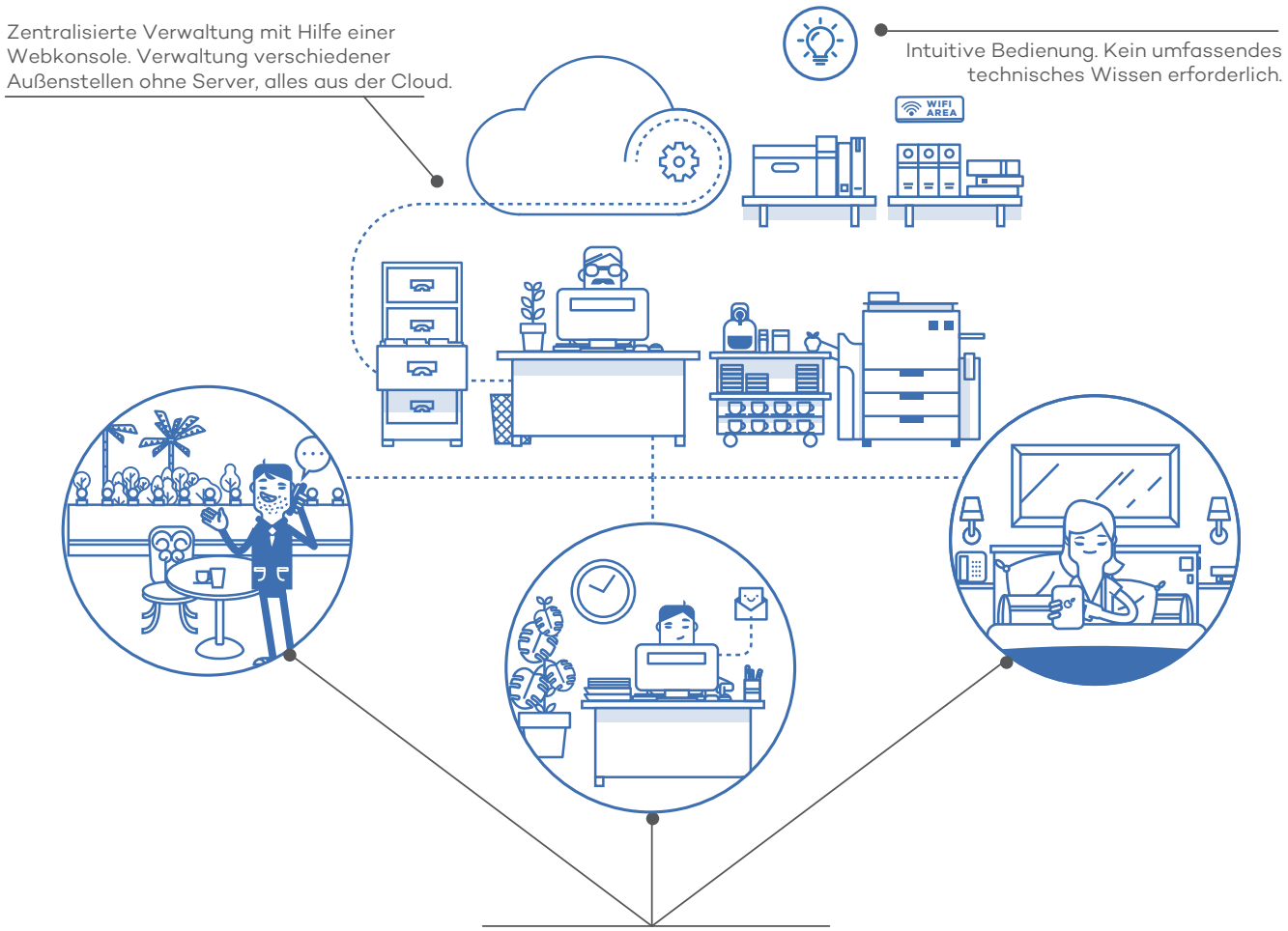
Plattformübergreifender Schutz für alle Endpoints

## SCHUTZ UND VERWALTUNG ALLER NETZWERK-DEVICES

**Panda Securitys Endpoint Protection** ist eine intuitive und ressourcenschonende Endpoint-Sicherheitslösung. Der zentralisierte und unterbrechungsfreie Schutz bietet flächendeckende Sicherheit auf allen Devices. Endpoint Protection schützt Windows-, Mac- und Linux-Workstations, einschließlich Laptops und Server sowie die gängigsten Virtualisierungssysteme.

**Panda Securitys Collective Intelligence** Technologie schützt alle Workstations und Server in Echtzeit vor Malware und Bedrohungen, die unbekannte (Zero-Day) Schwachstellen ausnutzen. Die Installation zusätzlicher Server oder IT-Infrastrukturen ist nicht erforderlich.

Mit **Endpoint Protection** wird die Sicherheit einfach und bequem über eine einzige Webkonsole gemanagt, was eine zentralisierte Verwaltung zu jeder Zeit und überall ohne umfangreiches, technisches Wissen ermöglicht.



## EINFACHE UND ZENTRALISIERTE SICHERHEIT FÜR ALLE GERÄTE

Zentralisierte Verwaltung der Sicherheit und Produkt-Upgrades durch einen unkomplizierten Webbrowser für alle Netzwerk-Workstations und Server. Verwaltet Ihren Windows-, Linux- oder Mac OS X- oder Android-Schutz mithilfe einer einzigen Management-Konsole.

## WIEDERHERSTELLUNGSMASSNAHMEN

Dank des Panda Cleaner Monitors desinfizieren Sie aus der Ferne Workstations, die von hochentwickelter, nicht-konventioneller Malware infiziert wurden.

Administrieren und booten Sie Ihre Server und Workstations aus der Ferne neu, um sicherzustellen, dass die neuesten Produkt-Updates installiert sind.

## REAL-TIME MONITORING UND REPORTINGS

Dank der umfassenden und personalisierbaren Dashboards ist eine detaillierte Überwachung Ihrer IT-Infrastruktur in Echtzeit möglich.

Berichte mit Informationen über den aktuellen Schutzstatus, Bedrohungen sowie die missbräuchliche Nutzung von Ressourcen können erstellt und automatisch versendet werden.

## PROFILBASIERTER SCHUTZ

Legen Sie profilbasierte Schutzrichtlinien fest um sicherzustellen, dass für jede Nutzergruppe die am besten geeigneten Richtlinien angewandt werden.

## ZENTRALISIERTE GERÄTEKONTROLLE

Blockieren Sie Geräte (USB-Sticks und Modems, Webcams, DVD/CD-Laufwerke usw.) oder reglementieren Sie deren Nutzung (Zugriff, Sperren, Lesen, Schreiben), um das Eindringen von Malware sowie Datenverluste zu verhindern.

## FLEXIBLE UND SCHNELLE INSTALLATION

Das schlanke Schutzmodul kann auf verschiedene Arten installiert werden: per E-Mail mit einer Download URL oder transparent mit Hilfe des enthaltenen Distribution Tools. Ebenso besteht die Möglichkeit der Erstellung eines MSI Installationspaketes, das mit den Tools von Drittanbietern (Active Directory, Tivoli, SMS usw.) kompatibel ist.

## MALWARE FREEZER

Verbrennen Sie sich nie wieder die Finger an False Positives. Malware Freezer friert entdeckte Malware sicherheitshalber für sieben Tage ein. Sollte es sich um einen Fehlalarm handeln, wird die Datei automatisch für das System wiederhergestellt.

## TECHNISCHE ANFORDERUNGEN:

**Webkonsole**

- Internetverbindung
- Internet Explorer 7.0 und später
- Mozilla Firefox 3.0 und später
- Google Chrome 2.0 und später

**Für Windows Workstations/File Server**

- Internetverbindung
- Betriebssysteme (Workstations): Windows 2000 Professional, Windows XP SP0 und SP1 (32-/64-bit) XP SP2 oder neuere Version (Vista, Windows 7 & Windows 8.1, Windows 10 (32-/64-bit))
- Betriebssysteme (Server): Windows 2000 Server, Windows Home Server, Windows 2003 (32-/64-bit & R2) SP1 und größer, Windows 2008 (32-/64-bit), Windows 2008 R2 (64-bit), Windows Small Business Server 2011, Windows Server 2012 (64-bit & R2)

**Für Mac Workstations/File Server**

- Mac OS X 10.6 Snow Leopard
- Mac OS X 10.7 Lion
- Mac OS X 10.8 Mountain Lion
- Mac OS X 10.9 Mavericks
- Mac OS X 10.10 Yosemite
- Mac OS X 10.11 El Capitan

**Für Linux Workstations/File Server**

- Ubuntu 12 (32-/64-bit) und später
- Red Hat Enterprise Linux 6.0 (64-bit) und später
- CentOS 6.0 (64-bit) und später
- Debian 6.9 Squeeze und später
- OpenSuse 12 (32-/64-bit) und später
- Suse Enterprise Server 11 SP2 (64-bit) und später

**Für Android Geräte**

- Android 2.3 und später

**Für Zertifizierte virtuelle Umgebungen**

- VMWare ESX 3.x, 4.x, 5.x
- VMWare Workstation 6.0, 6.5, 7.x, 8.x und 9.x
- Virtual PC 6.x
- Microsoft Hyper-V Server 2008 R2 und 2012 3.0
- Citrix XenDesktop 5.x, XenClient 4.x, XenServer und XenApp 5.x und 6.x

**Kompatibel mit:**