

# GRÜNDE FÜR DEN EINSATZ VON SECULUTION

WHITEPAPER

Jeden Tag kommen rund 35.000 neue Viren und andere Schädlinge in Umlauf. Professionell organisierte, kriminelle Banden legen mit Ransomware Ihr Unternehmen bis zur Handlungsunfähigkeit lahm, was in einer handfesten Existenzbedrohung gipfeln kann. Eine Antivirus-Software kann nur vor der Schadsoftware schützen, die sie kennt. Neu entwickelte oder bis zur Unkenntlichkeit modifizierte Schadsoftware hat allein in Deutschland laut IT-Branchenverband Bitkom im letzten Jahr einen Schaden von rund 55 Milliarden Euro verursacht.



**seculution**  
application whitelisting

# WIE ARBEITET SECULUTION IN IHREM NETZWERK?

SecuLution arbeitet nach dem „Whitelisting“-Prinzip und schützt dadurch wirksam und verlässlich vor Schadsoftware, indem es nur bekannte und für die Arbeit benötigte Software zulässt. Nach dem Prinzip eines Türstehers: Was nicht reinkommt, kann auch keinen Schaden anrichten. Sie entscheiden, welcher Software Sie vertrauen. So wird sämtliche Schadsoftware automatisch als „unbekannt“ eingestuft und kann nicht ausgeführt werden.

Dabei hilft Ihnen SecuLution, einen Überblick über Ihr Netzwerk zu behalten, kostspielige Lizenzstrafen zu vermeiden, Ihr Patchmanagement zu erleichtern und durch Data-Leakage-Prevention in Bezug auf USB-Wechselmedien, Datendiebstahl und Cybersabotage zu verhindern. Ohne zusätzlichen Administrationsaufwand. Dies führt bereits innerhalb weniger Monate zu einem positivem Return on Investment.

## ZENTRALE DATENBANK

- \_ Sicherheit auf Basis einer Datenbank erlaubter Anwendungen (Application-Whitelist)
- \_ Application Control, z.B. über Active Directory Objekte. Bestimmen Sie, welcher User welche Software ausführen darf
- \_ Abwehr unerwünschter Programme (Ransomware, Viren, Trojaner, Spiele, unsichere oder fehlerhafte Programme) und automatische Alarmierung bei jedem Versuch, Software auszuführen, die nicht per Whitelist erlaubt wurde
- \_ Schutz vor allen unbekanntem Anwendungen, DLLs und Java Code
- \_ Proaktiv: Null-Sekunden Reaktionszeit
- \_ Keine kontinuierlichen Updates von Signatur- oder Definitionsfiles notwendig
- \_ Automatische Versionskontrolle aller Anwendungen auf Basis von Hashes (elektronischer Fingerabdruck)
- \_ USB-Whitelisting bietet Schutz vor Datendiebstahl oder eingeschleuster Schadsoftware, inklusive aktivierbarer AES256 Verschlüsselung

## EINFACHE ADMINISTRATION

- \_ Vollinstallation und Integration in 5 Stunden möglich
- \_ Automatisches Patchmanagement
- \_ Regelverletzungen bei Bedarf direkt aus den Logs mit einem Mausklick in einen Whitelist-Eintrag wandelbar
- \_ Lern-Modus erlaubt vollautomatische Konfiguration
- \_ Lokales Caching der Whitelist für mobile Nutzer und Schutz vor Netzwerk- und Serverausfällen

## MAXIMALE SICHERHEIT

- \_ Geringer Konfigurations- und Administrationsaufwand bei größtmöglicher Sicherheit auch gegen modernste Angriffsformen

## AUSFÜHRLICHE LOGS

- \_ Exporte der Logs, Reporting in Netzwerkmanagement-Systeme möglich (SysLog)

## → POSITIVER ROI IN WENIGEN MONATEN

### SecuLution GmbH

Alter Hellweg 6b  
59457 Werl  
Deutschland

+49 (0)2922 9589-210  
info@seculution.com  
www.seculution.de



**seculution**  
application whitelisting