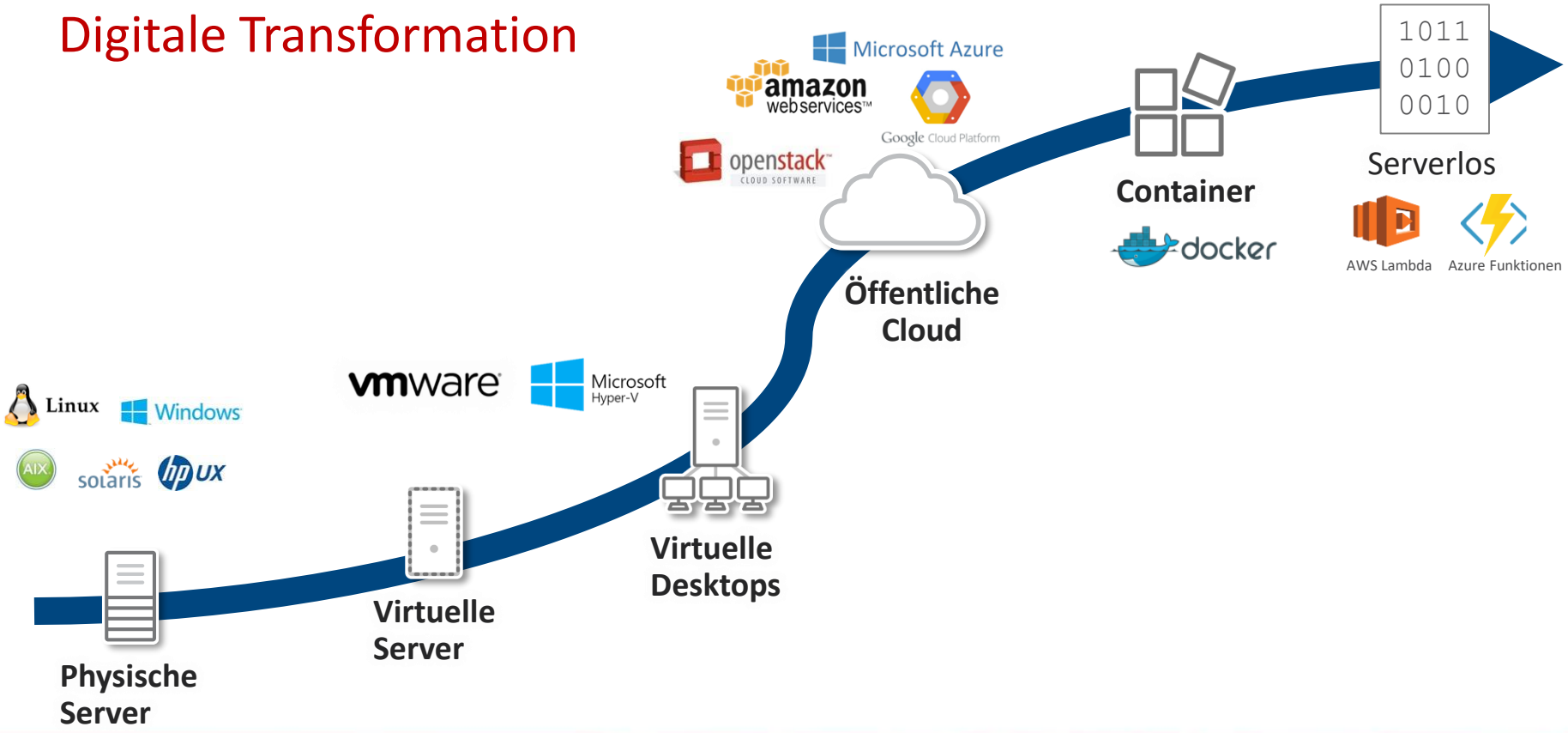
Wirksamer Schutz für virtuelle, physische und cloud-basierte IT-Umgebungen

Benjamin_Greve@Trendmicro.com
Dipl.-Inform., CISSP
Senior Sales Engineer

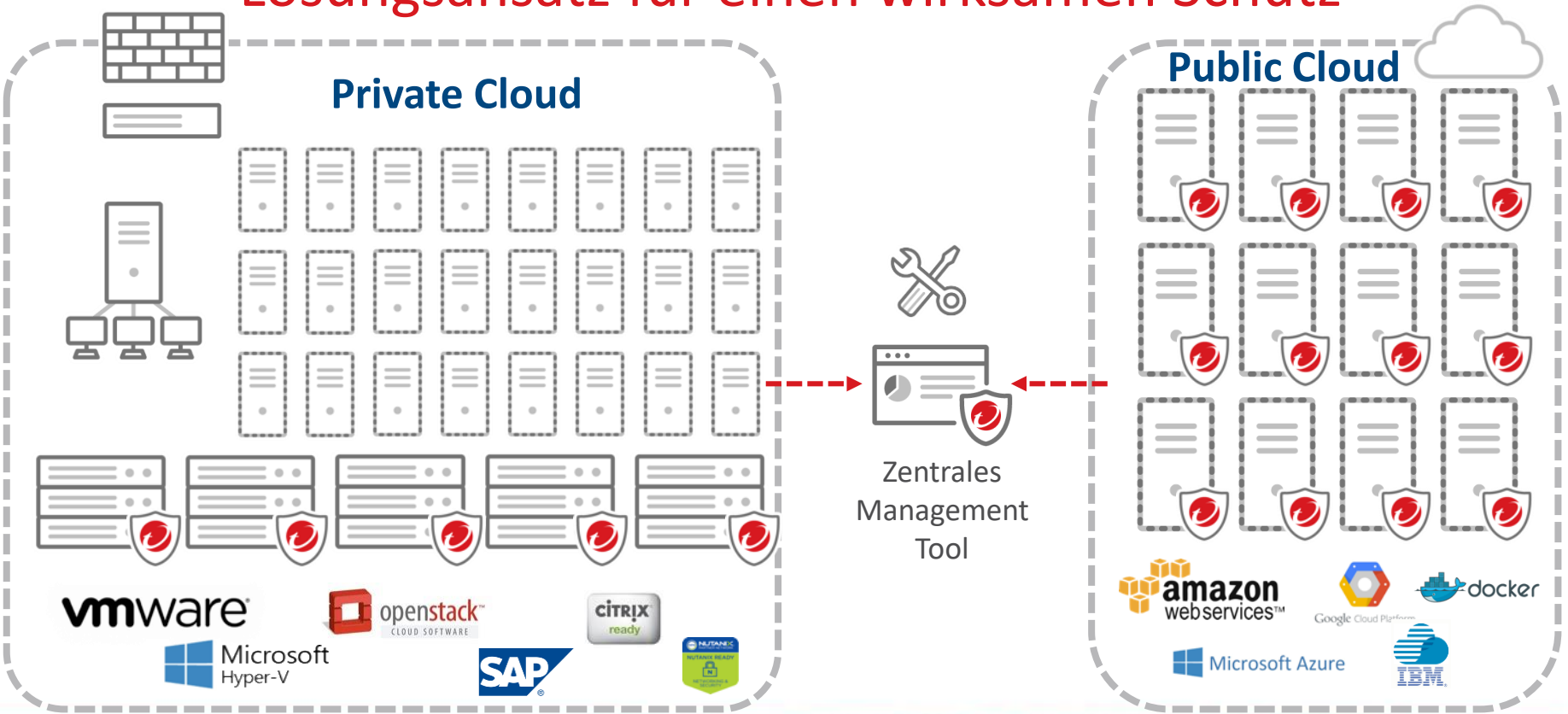
Digitale Transformation



Zusammenfassung der Situation

- Neue Geschäftsprozesse müssen durch Anpassung der IT umgesetzt werden.
- Gesetze und Regularien müssen berücksichtigt werden.
- Risiko durch Schadprogramme bzw. Cyberkriminielle steigt.

Lösungsansatz für einen wirksamen Schutz

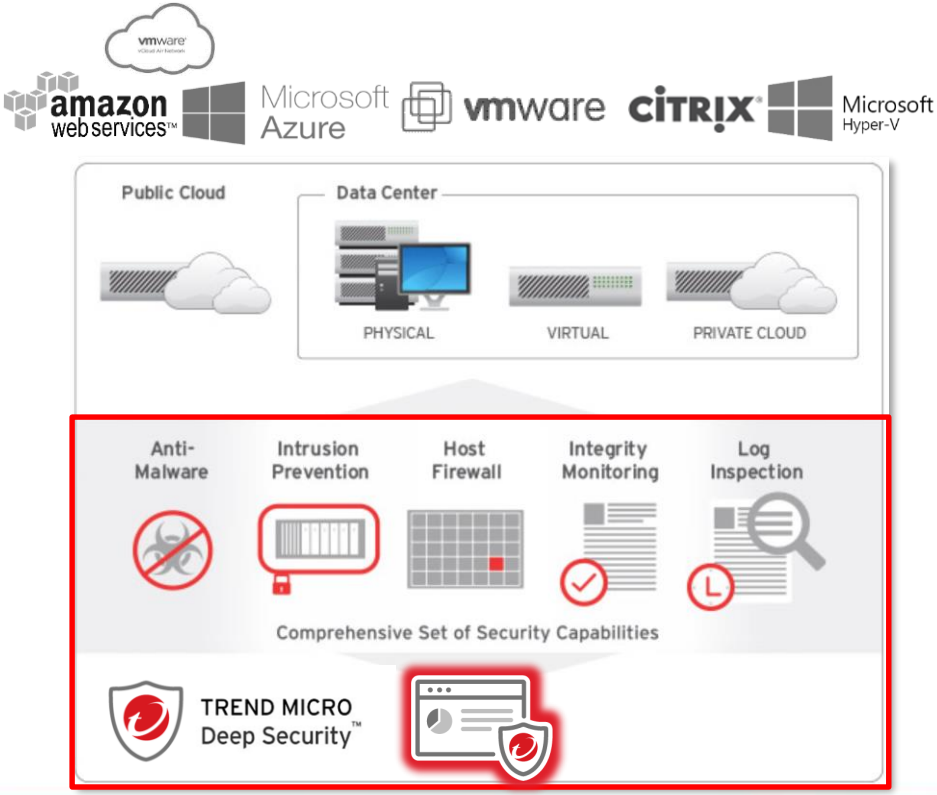


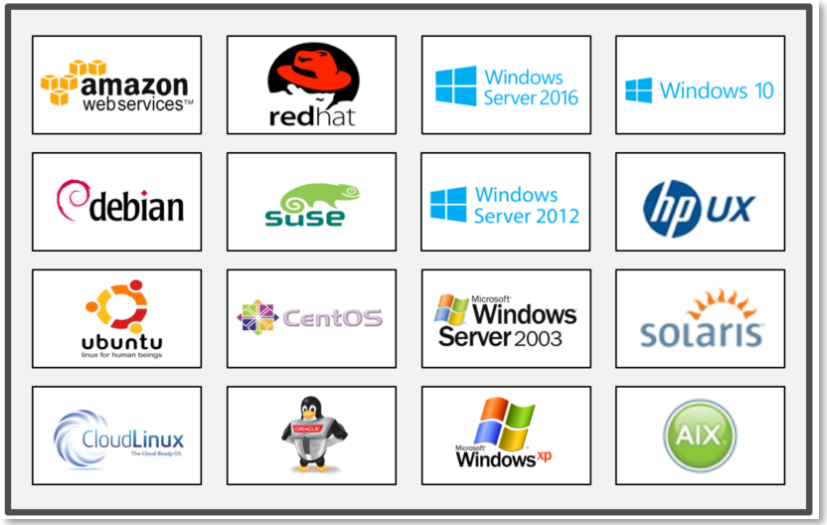
Deep Security

(Wirksamer Schutz für virtuelle, physische und cloud-basierte IT-Umgebungen)

Benjamin_Greve@Trendmicro.com
Dipl.-Inform., CISSP
Senior Sales Engineer

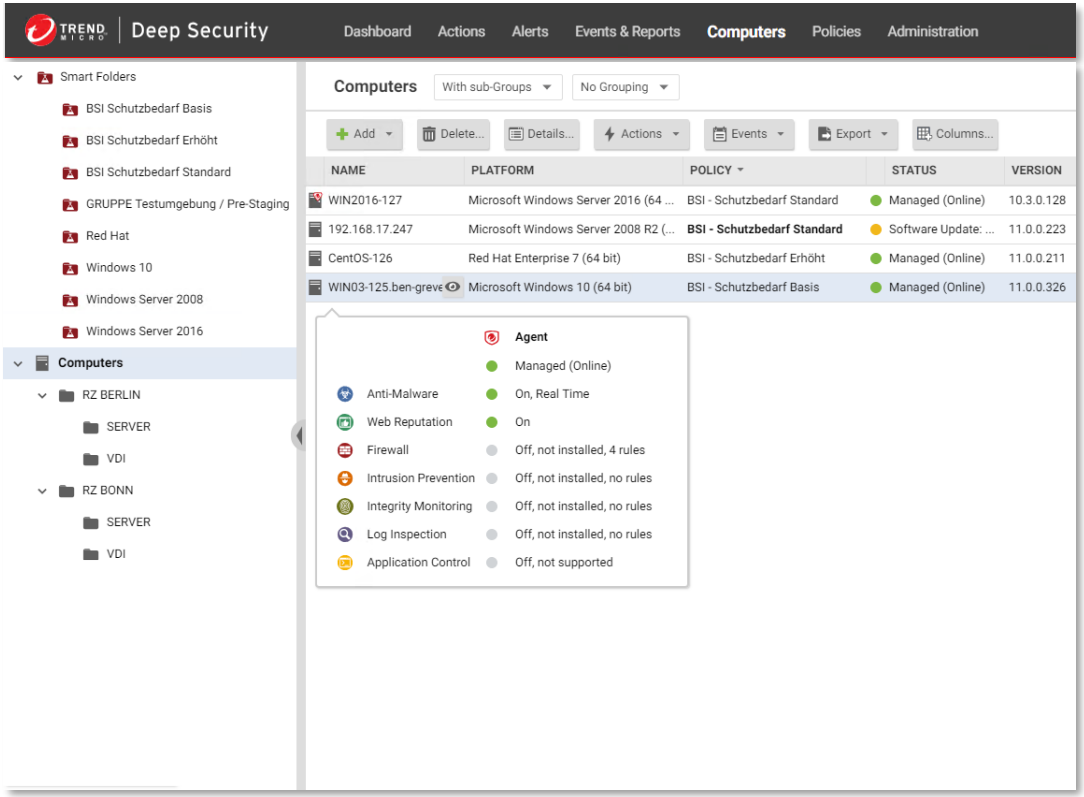
Deep Security: Umfassender Schutz für das moderne Rechenzentrum





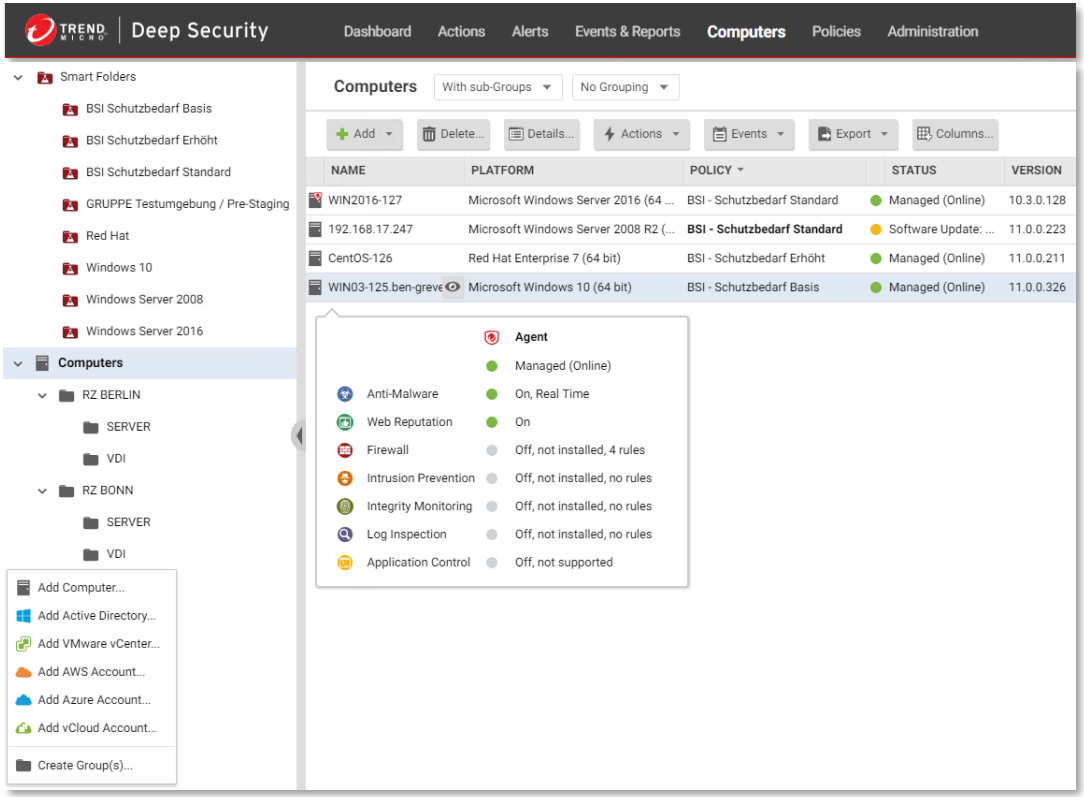
Unterstütze Plattformen

- Windows
- Red Hat Enterprise Linux
- CentOS
- Oracle Linux
- SUSE Linux
- Ubuntu
- Debian
- Cloud Linux
- Amazon
- Azure
- Agentless (VMWare NSX)



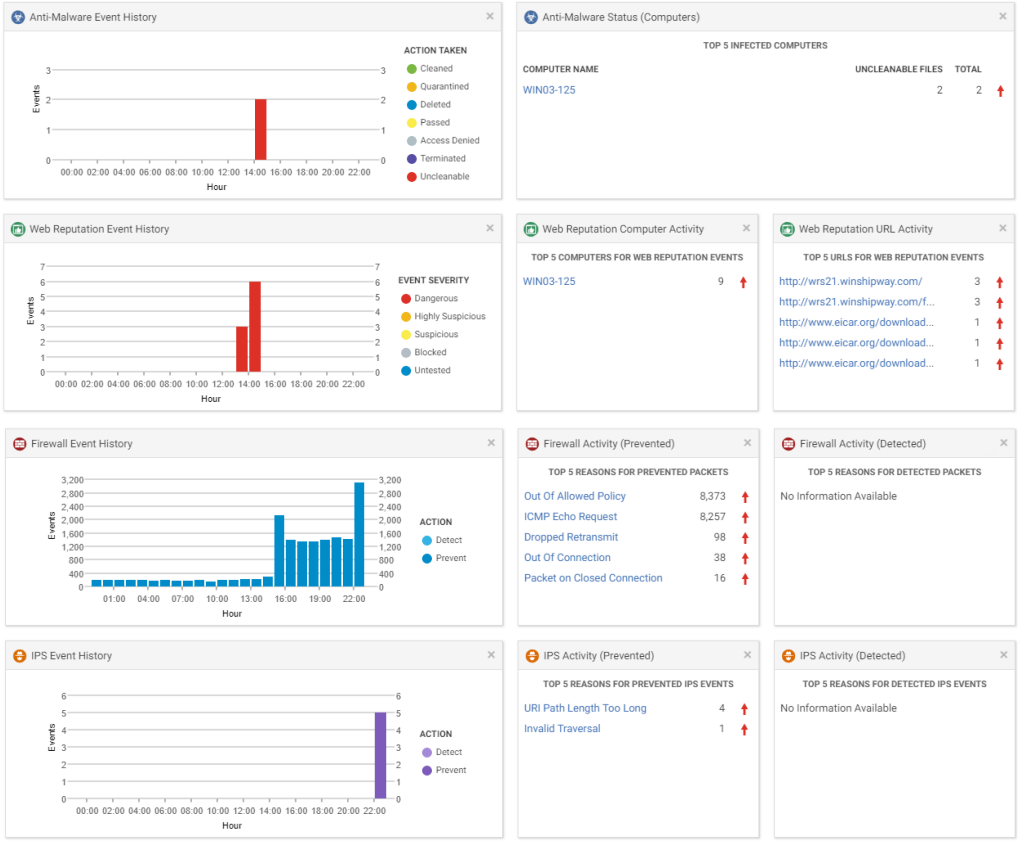
Deep Security Manager

- Eine Zentrale für Alles
  - Systemverwaltung, / Überwachung
  - Richtlinienverwaltung
  - Reporting / Monitoring
  - Hoch-Verfügbar, Ausfallsicher
  - Mandantenfähig
  - Automatisierung
- Kontrolle bei
  - Provisionierung, Softwareverteilung
  - Programmupdates- /upgrades
  - Signaturupdates (Rollback)
  - Monitoring (Status d. Clients)
- Smart Folders
  - Schnelle gefilterte Ansicht auf Systeme



Deep Security Manager

- Integration / Automatisierung
  - ActiveDirectory
  - VMWare / NSX
  - AWS
  - Azure
  - …
- API - Schnittstelle



Ereignisverarbeitung

- Ereignisse
  - Dasboard
  - Berichte
  - Alarmierung
- Einbindungung übergeordneter Sicherheitssysteme (z.B. SIEM)
  - Email, Syslog, SNMP
- Individuell anpassbar

Wirksame Schutzmodule

Netzwerksicherheit


Intrusion Prevention


Firewall


Scannen von Schwachstellen

Stoppen von Netzwerkangriffen, Schützen angreifbarer Anwendungen und Server

Systemsicherheit


Anwendungs-kontrolle


Integritäts-überwachung


Protokoll-inspektion

Abriegelung von Systemen und Erkennen einer verdächtigen Aktivität

Malware-Schutz

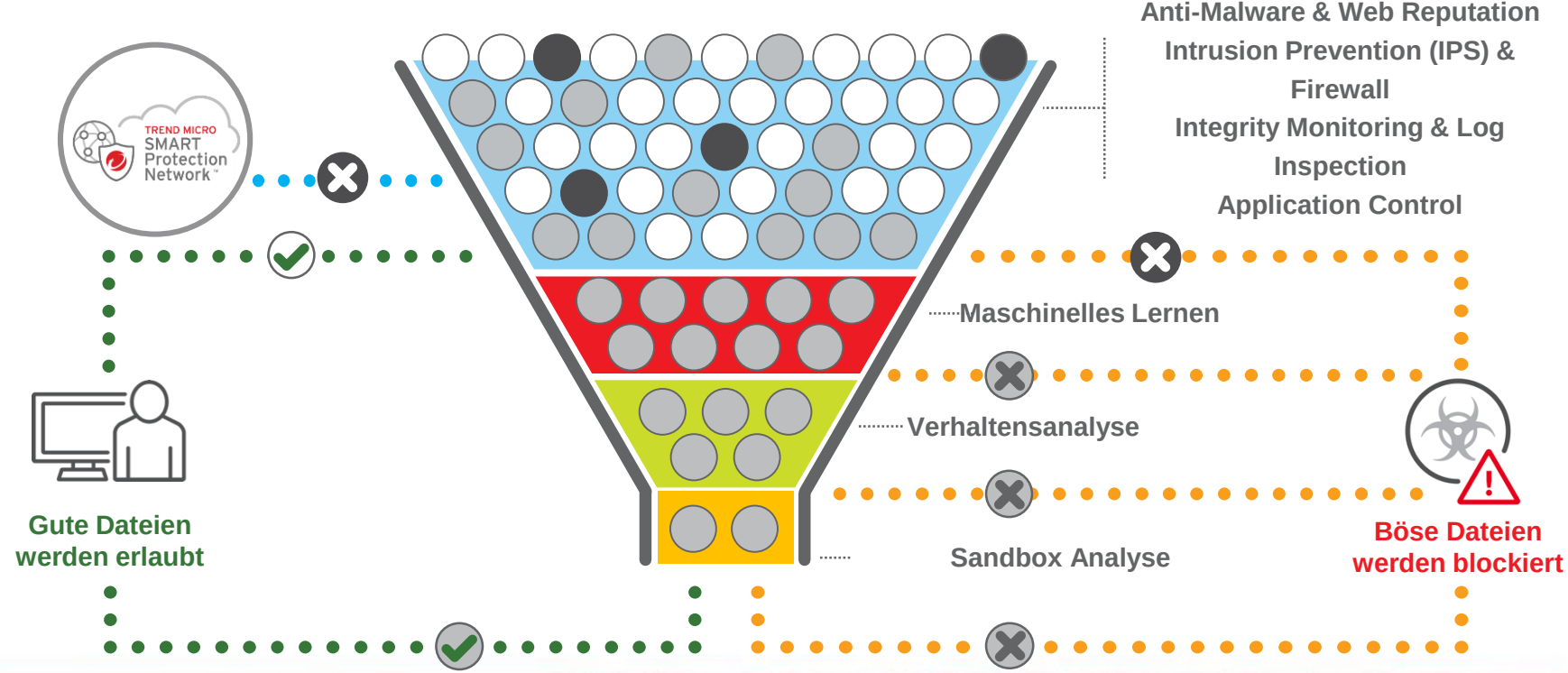

Anti-malware


Verhaltensanalyse und Machine Learning

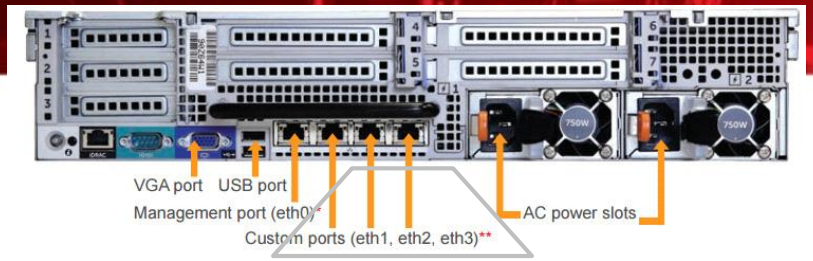

Sandbox-Analyse

Stoppen von Malware und zielgerichteten Angriffen

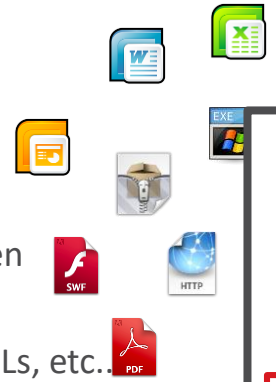
Anti-Malware



Was ist eine Sandbox?



- Eine smarte Sandbox
  - Kunden Image
  - Ausführungsbeschleunigung
  - Erkennung von Tarnmechanismen
  - 32 & 64 bit VMs
  - Analyse von EXE, Office, PDF, URLs, etc..
- Live Überwachung
  - Kernel Integration *(hook, dll injection..)*
  - Netzwerk Analyse
  - Ereigniskorrelation

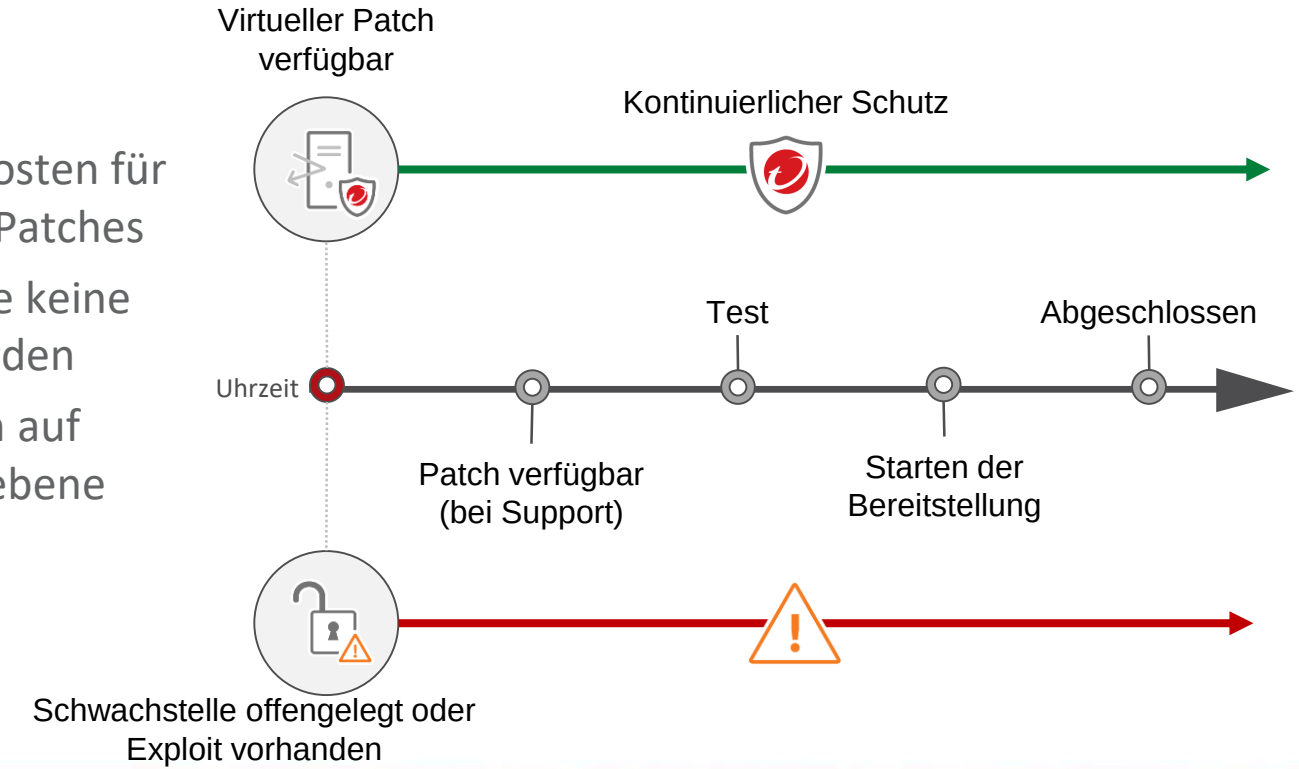



```
LoadLibraryA ARGs: ( NETAPI32.dll ) Return value: 73e50000
LoadLibraryA ARGs: ( OLEAUT32.dll ) Return value: 75de0000
LoadLibraryA ARGs: ( WININET.dll ) Return value: 777a0000
key: HKEY_CURRENT_USER\Local Settings\MuiCache\48\52C64B7E\LanguageList
value:
key: HKEY_CURRENT_USER\Software\Microsoft\Onheem\20bi1d4f
Write: path: %APPDATA%\Ewada\eqawoc.exe type: VSDT_EXE_W32
Injecting process ID: 2604 Inject API: CreateRemoteThread Target process ID:
1540 Target image path: taskhost.exe
socket ARGs: ( 2, 2, 0 ) Return value: 28bfe
socket ARGs: ( 23, 1, 6 ) Return value: 28c02
window API Name: CreateWindowExW ARGs: ( 200, 4b2f7c, , 50300104, 0, 0,
250, fe, 301b8, f, 4b0000, 0 ) Return value: 401b2
internet_helper API Name: InternetConnectA ARGs: ( cc0004,
mmlzntponzkfuik.biz, 10050, , , 3, 0, 0 ) Return value: cc0008
.....
```

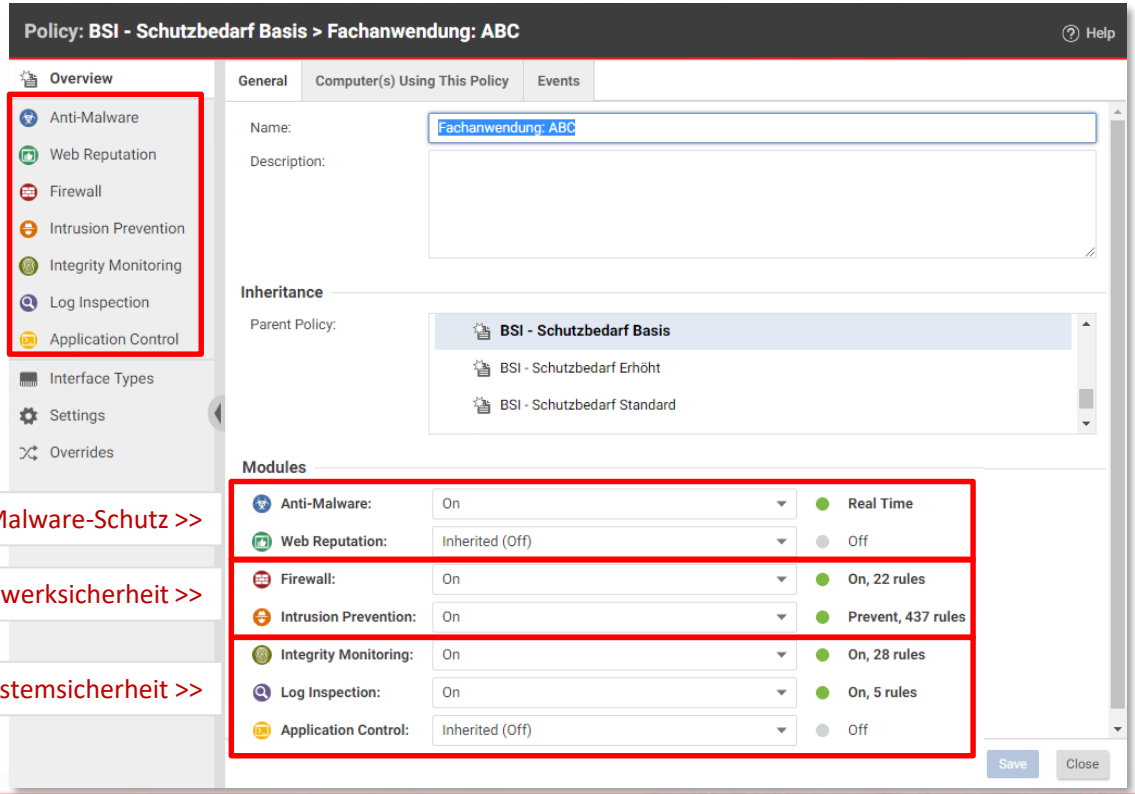
Modifies file with infectible type : eqawoc.exe
Inject processus : 2604 taskhost.exe
Access suspicious host : mmlzntponzkfuik.biz

Intrusion Prevention

- Reduzieren von Betriebskosten für Notfall- und fortlaufende Patches
- Schutz für Systeme, für die keine Patches bereitgestellt werden
- Schutz vor Schwachstellen auf Server- und Anwendungsebene

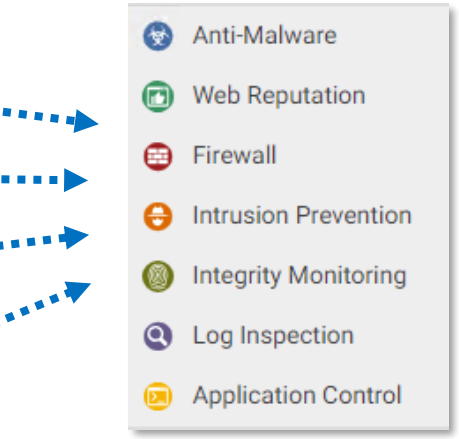


Wirksame Schutzmodule

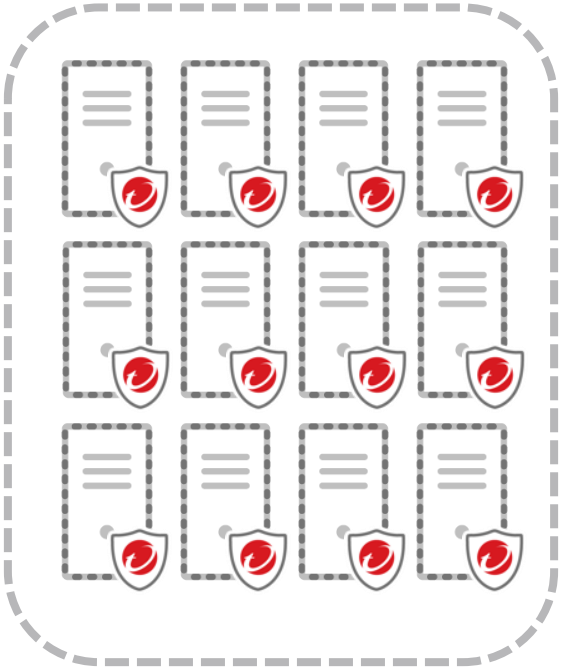


- Absicherung von Servern mit verschiedenen Fachanwendungen und unterschiedlichen:
  - Einstellungen
  - Anforderungen
  - Schutzbedarfen
- Erfüllung der Anforderungen durch Nutzung der Module

Umgang mit Richtlinien

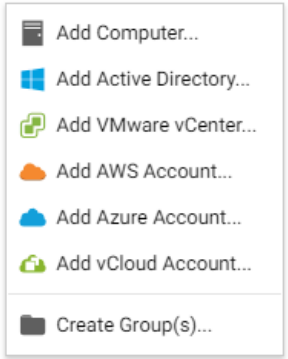


- BSI - Schutzbedarf Basis
  - Windows Server 2000
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2012
  - Windows Server 2016
- BSI - Schutzbedarf Erhöht
  - Fachanwendung: ABC
  - Fachanwendung: XYZ
- BSI - Schutzbedarf Standard
  - Fachanwendung: 123



- Richtlinien als Vorlage
- Vererbung & Verfeinerung

Marktführende Vision und Partnerschaften



Bedrohungs-Intelligence

Erste Lösung mit vShield-Unterstützung

Erste Lösung mit Hypervisor-basiertem Schutz

Deep Security in privater und öffentlicher Cloud

Unterstützung für Netzwerke der nächsten Generation mit Datei- und Netzwerk-sicherheit

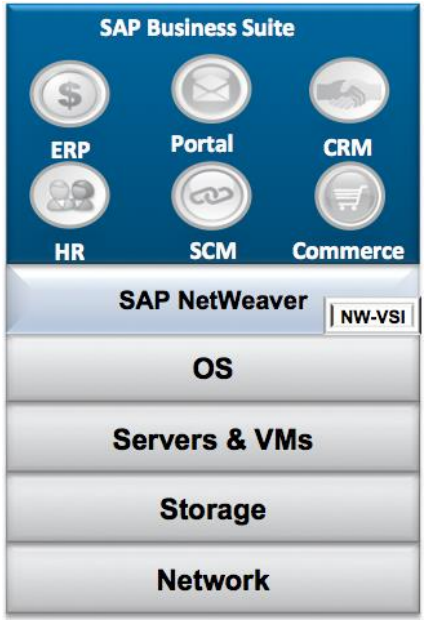
Sichtbarkeit im Rechenzentrums-betrieb und Sicherheit

Sicherheit in wichtigen Cloud-Märkten verfügbar

Integrierte Sicherheit in Cloud Managed Service-Angeboten

Schutz von Microservices und Docker-Containern

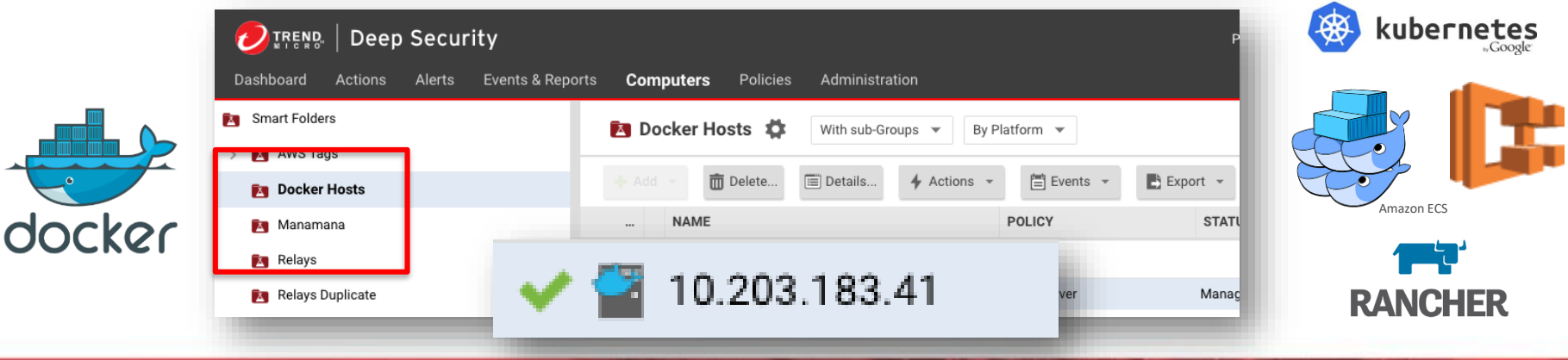
Schützen von Unternehmenssystemen



- SAP-Adapter in Deep Security Agent integriert (einzelner Agent für Server- und Anwendungssicherheit)
- Funktioniert nahtlos mit SAP VSI 2.0
  - NetWeaver, HANA, Fiori
- Scannt nach Malware und schützt vor XSS-Angriffen

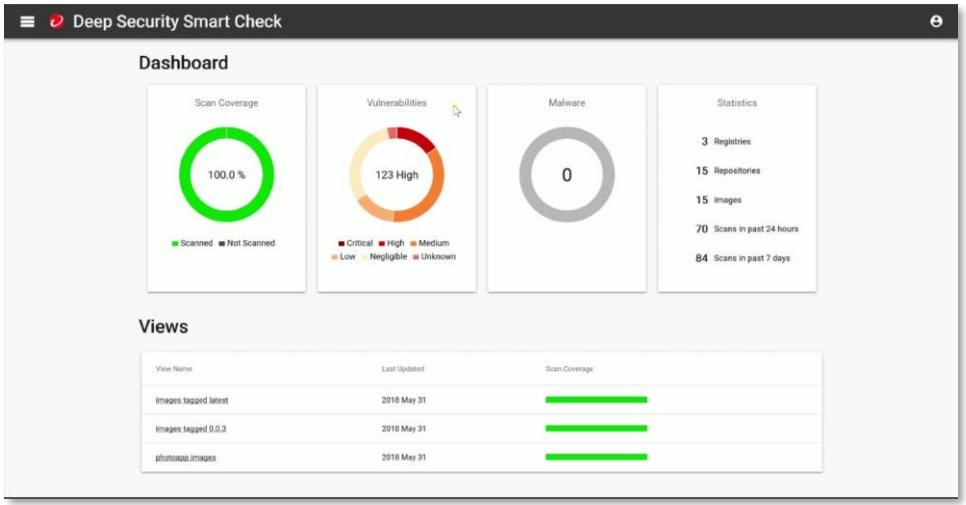
Erweiterung auf Docker-Container

- Schutz von Host UND Docker-Containern, die darauf ausgeführt werden
- Erzielen einer einheitlichen Sicherheit in allen Workloads



Deep Security: Smart Check

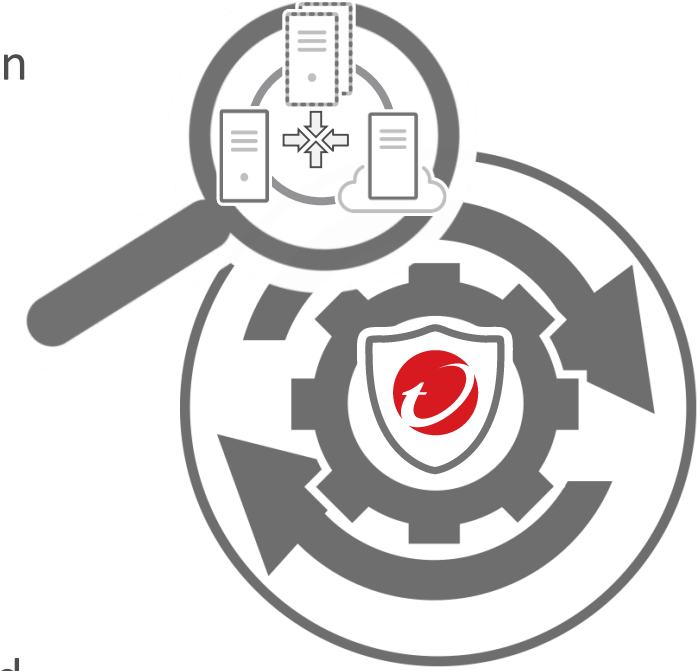
- Automatisierbare Analyse von Docker Images auf Schadsoftware und Schwachstellen vor der Bereitstellung



www.trendmicro.com/smartcheck

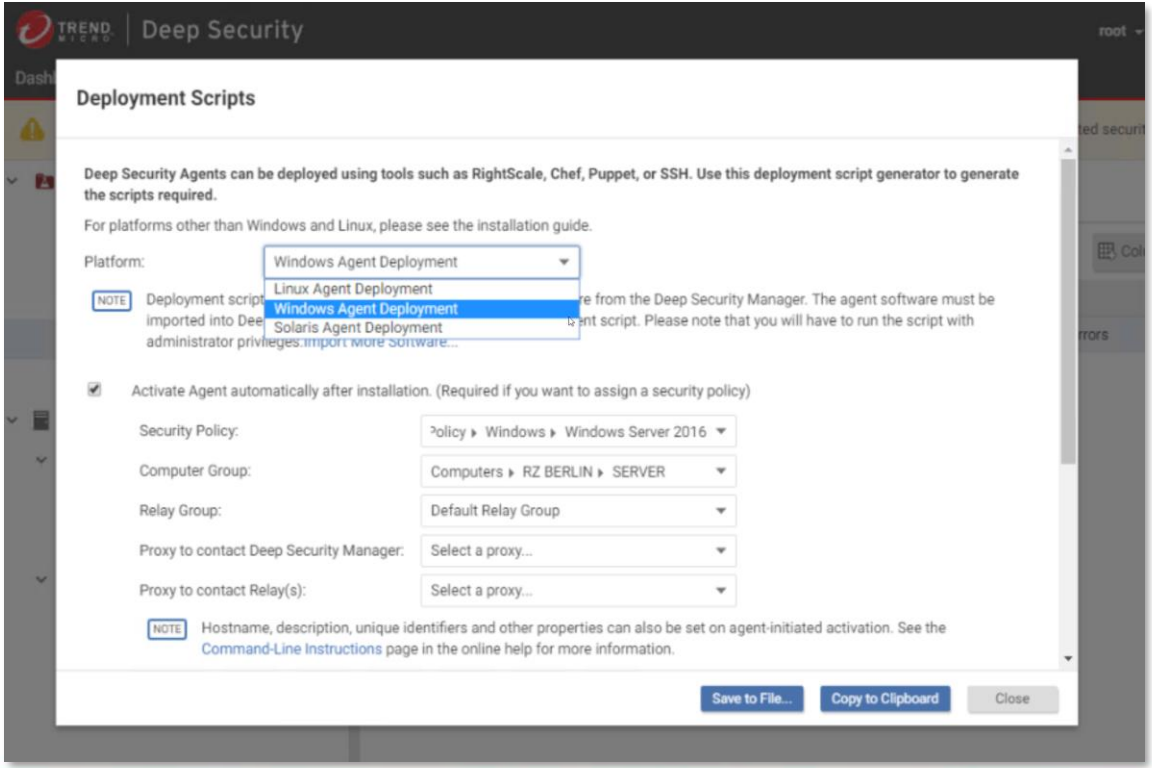
Beseitigen manueller Sicherheitsprozesse

- Umfassende Sichtbarkeit über Umgebungen hinweg erhalten
- Automatisches Skalieren nach oben oder unten – ganz ohne Sicherheitslücken
- Scannen nach Schwachstellen und Empfehlen oder Anwenden von Sicherheitslösungen basierend auf der Richtlinie
- Installieren von Sicherheitskontrollen, die für eine maximale Leistung erforderlich sind



Deep Security: Agenten Ausbringung

- Zentrale Verwaltungskonsole erstellt Installationsskripte für Windows, Linux und Solaris
  - PowerShell
  - Bash
- Installationsskript kann Gruppen- und Richtlinienzuweisung mit enthalten.
- Auto-Provisioning
  - VMWare, AWS, Azure



Beispiele: Installationsskripte

- Windows

```
<powershell>
#requires -version 4.0
# This script detects platform and architecture.  It then downloads and installs the relevant Deep Security Agent 10 package
if (-NOT ([Security.Principal.WindowsPrincipal]
[Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole] "Administrator")) {
  Write-Warning "You are not running as an Administrator. Please try again with admin privileges."
  exit 1 }
[Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}
$env:LogPath = "$env:appdata\Trend Micro\Deep Security Agent\installer"
New-Item -path $env:LogPath -type directory
Start-Transcript -path "$env:LogPath\dsa_deploy.log" -append
echo "$(Get-Date -format T) - DSA download started"
```

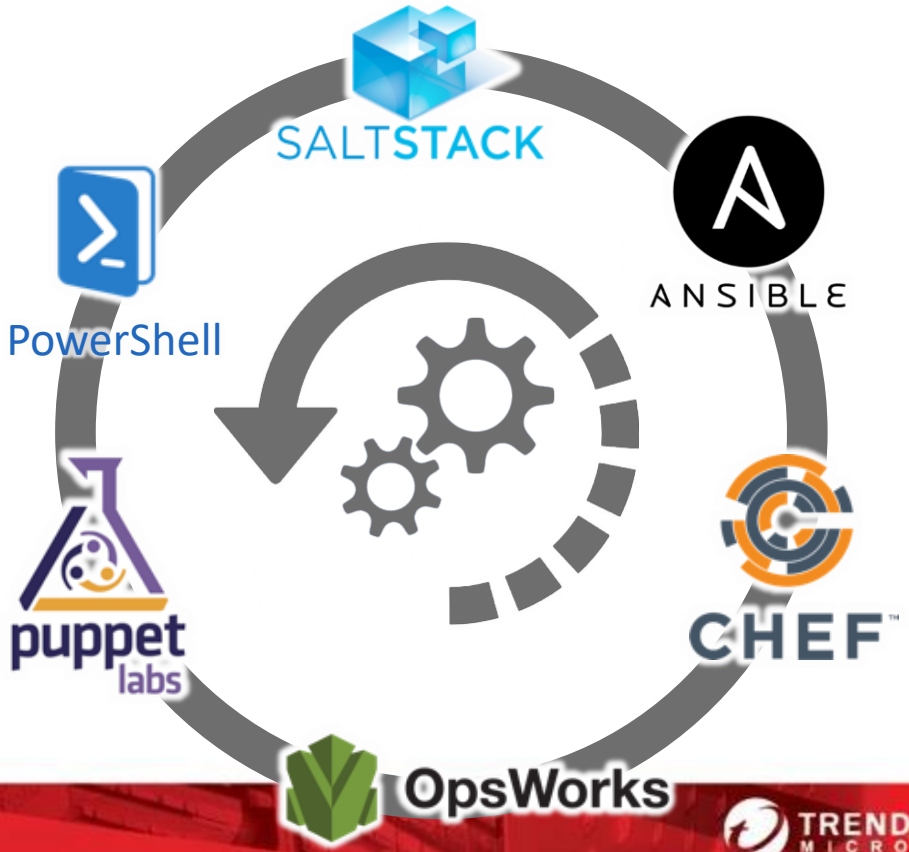
- Linux

```
#!/bin/bash
# This script detects platform and architecture, then downloads and installs the matching Deep Security Agent package
if [[ $(/usr/bin/id -u) -ne 0 ]]; then echo You are not running as the root user.  Please try again with root privileges.;
  logger -t You are not running as the root user.  Please try again with root privileges.;
  exit 1;
fi;
if type curl >/dev/null 2>&1; then
 SOURCEURL='https://192.168.17.200:4119'
 curl $SOURCEURL/software/deploymentscript/platform/linux/ -o /tmp/DownloadInstallAgentPackage --insecure --silent --tlsv1.2

 if [ -s /tmp/DownloadInstallAgentPackage ]; then
    . /tmp/DownloadInstallAgentPackage
```

Reduzierung des Deployment Aufwandes

- Unterstützung von führenden Orchestration und Automation Werkzeugen
- Entwicklung im Staging
- Fortwährende Integration und Deployment Unterstützung



Deep Security

Pre-deployment

Image Scanning

Scannen von Schwachstellen

Virenschutz

Fortlaufende Überprüfen auf Schwachstellen & Schadprogramme

Runtime / Deployed

Network Sicherheit

Intrusion Prevention

Firewall

Scannen von Schwachstellen

Stoppen von Netzangriffen, Schützen angreifbarer Anwendungen und Server

Systemsicherheit

Anwendungs-kontrolle

Integritäts-überwachung

Protokoll Inspection

Abriegelung von Systemen und Erkennen einer verdächtigen Aktivität

Malware Schutz

Anti-Malware

Verhaltenanalyse und Maschinelles Lernen

Sandbox Analyse

Stop malware & targeted attacks

Umgebungen

Containers

Virtual Server

Rechenzentrum

Public Cloud

Platformen

Automatisierung & Integration