

## DA UNTERNEHMEN IMMER MEHR SICHERHEITSDATEN VERWALTEN MÜSSEN, KÖNNEN SICH DIE ABTEILUNGEN NICHT MEHR GEBÜHREND AUF WICHTIGE DETAILS KONZENTRIEREN

Diese Daten können zur Erkennung von Sicherheitsproblemen und -verletzungen, die durch externe Faktoren und interne Mitarbeiter verursacht werden, genutzt werden. IT-Abteilungen sind überlastet. Die große Menge an verwalteten Daten und das Aufkommen von Malware der nächsten Generation führen dazu, dass viele Details übersehen oder einfach überhaupt nicht registriert werden, was die Sicherheit des gesamten Systems gefährdet.

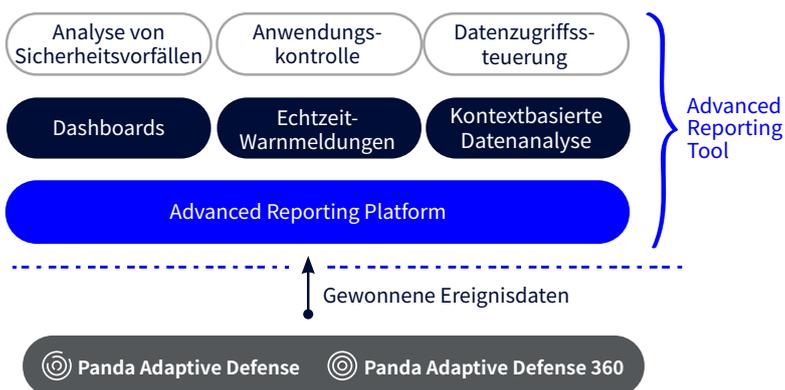
## DIE LÖSUNG: PANDA ADAPTIVE DEFENSE 360 UND ADVANCED REPORTING TOOL

Die **Advanced Reporting Plattform** automatisiert die Speicherung und den Abgleich der von Panda Adaptive Defense 360 aus Endpunkten gewonnenen Prozessdaten mitsamt Kontext.

Mithilfe dieser Daten kann das Advanced Reporting Tool automatisch Sicherheitsinformationen generieren und Tools bereitstellen, mit denen Unternehmen Angriffe und ungewöhnliche Verhaltensmuster unabhängig vom Entstehungsort präzise bestimmen sowie internen Missbrauch der Firmennetzwerke und -systeme erkennen können

Mit dem Advanced Reporting Tool können Unternehmen riesige Datenmengen durchsuchen, untersuchen und analysieren. So ermöglichen sie IT- und Sicherheitseinblicke in die Infrastruktur, in Anlagen und Gebäuden oder bei der Wartung.

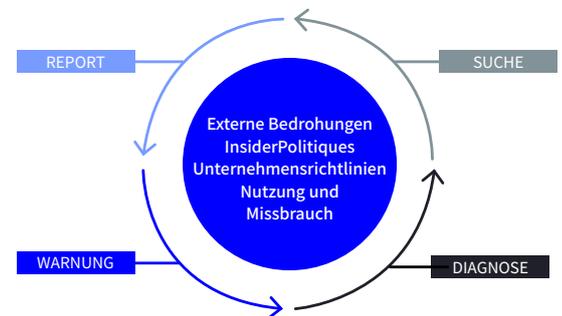
Das Advanced Reporting Tool liefert die Daten, die benötigt



werden, um detaillierte Rückschlüsse in Bezug auf das IT- und Sicherheitsmanagement des Unternehmens zu ziehen. Auf dieser Grundlage kann dann ein Aktionsplan mit nachfolgenden Punkten definiert werden:

- **Bestimmung des Ursprungs von Sicherheitsbedrohungen**, um zukünftige Angriffe zu verhindern
- Implementierung von **restriktiven Richtlinien für den Zugriff auf wichtige Firmendaten**
- Überwachung und Kontrolle des **Missbrauchs von Unternehmensressourcen** mit möglichen Auswirkungen auf die Unternehmens- und Mitarbeiterleistung
- **Korrektur des Verhaltens von Mitarbeitern**, sofern diese sich nicht an die Nutzungsrichtlinien des Unternehmens halten

## HAUPTVORTEILE



### 1. Finden Sie relevante Informationen

🔍 Maximieren Sie Ihren Einblick in alle auf den eingesetzten Geräten laufenden Prozesse und erhöhen Sie die Effizienz und Produktivität der IT-Abteilung.

🔍 Greifen Sie auf Protokolldaten zu, um die Sicherheit der Unternehmensressourcen und Nutzungsindikatoren zu analysieren.

🔍 Erhalten Sie detaillierte Informationen, um Sicherheitsrisiken sowie den Missbrauch der IT-Infrastruktur durch Insider zu identifizieren.

### 2. Diagnostizieren Sie Netzwerkprobleme

🔧 Reduzieren Sie die Anzahl der benötigten Tools und Datenquellen, um zu verstehen, was auf den Netzwerkgeräten passiert und welche Bedeutung dies für die Sicherheit und die Nutzung der Vermögenswerte Ihres Unternehmens hat.

🔧 Gewinnen Sie Informationen über die Ressourcennutzung und die Verhaltensmuster von Anwendern, um ihren potenziellen Einfluss auf das Unternehmen zu demonstrieren. Nutzen Sie diese Informationen, um Richtlinien für Kosteneinsparungen zu implementieren.

### 3. Seien Sie wachsam

📡 Wandeln Sie entdeckte Anomalien in Echtzeit-Warnungen und Reports um.

📡 Ermitteln Sie Sicherheitsabweichungen sowie den Missbrauch von IT-Ressourcen durch Mitarbeiter in Echtzeit.

### 4. Generieren Sie horizontale und vertikale Informationen

📄 Generieren Sie konfigurierbare detaillierte Reports, um methodische Analysen des Sicherheitsstatus Ihres Unternehmens durchzuführen. Stellen Sie Fälle des Missbrauchs von Vermögenswerten sowie Verhaltensanomalien fest.

📄 Analysieren Sie den Status wichtiger Sicherheitsindikatoren und verfolgen Sie deren Entwicklung zur Evaluierung der eingeführten Korrekturmaßnahmen.

## FLEXIBLE, AUF IHREN BEDARF ABGESTIMMTE ANALYSEN

Das **Advanced Reporting Tool (ART)** umfasst Dashboards mit Schlüsselindikatoren, Suchoptionen und Standardwarnmeldungen für drei zentrale Bereiche:

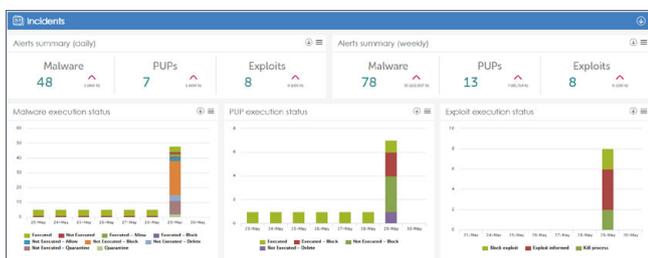
- **Sicherheitsvorfälle**
- **Zugriff auf wichtige Informationen**
- **Nutzung von Anwendungen und Netzwerkressourcen**

**Suchvorgänge** und **Warnmeldungen** können dabei an die individuellen Gegebenheiten Ihres Unternehmens angepasst werden.

## INFORMATIONEN ÜBER SICHERHEITSVORFÄLLE

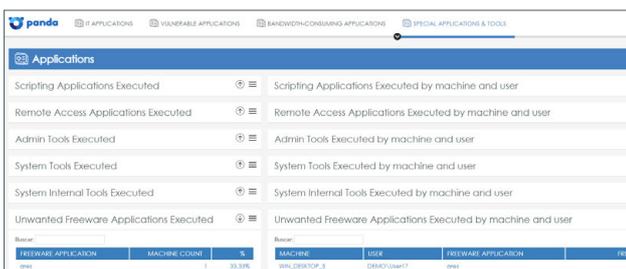
Generieren Sie **detaillierte Sicherheitsinformationen**, indem Sie die während der Angriffsversuche aufgetretenen Ereignisse zeitnah verarbeiten und abgleichen:

- Zeitleisten mit Informationen zu Malware, PUPs und Exploits, die im vergangenen Jahr entdeckt wurden
- Computer mit den meisten Infektionsversuchen und entdeckten Malware-Exemplaren
- Computer mit gefährdeten Anwendungen
- Ausführungsstatus von Malware, PUPs und Exploits auf Netzwerkcomputern



Das ART umfasst Widgets für **Schatten-IT** und visualisiert so die ausgeführten Anwendungen, die möglicherweise außerhalb des Einflussbereichs der IT liegen:

- Am häufigsten und am seltensten ausgeführte Anwendungen
- Scripting-Anwendungen (PowerShell, Linux-Shell, Windows cmd usw.)
- Remote-Access-Anwendungen (TeamViewer, VNC usw.)
- Unerwünschte Freeware-Anwendungen (Emule, Torrent usw.)



| Application                     | Machine Count | Machine | User       | Application | ID  |
|---------------------------------|---------------|---------|------------|-------------|-----|
| Scripting Applications Executed | 1             | 30.8%   | WPCENTOP_2 | SCRIPTUSER1 | msc |

## MUSTER BEI DER NUTZUNG VON NETZWERKRESSOURCEN

Verfolgen Sie **Muster bei der Nutzung von IT-Ressourcen**, um **Sicherheitsrichtlinien festzulegen und durchzusetzen**:

- Feststellen, welche Unternehmensanwendungen und Nicht- Unternehmensanwendungen in Ihrem Netzwerk ausgeführt werden
- Anfällige Anwendungen, die im Netzwerk ausgeführt oder installiert werden und zu einer Infektion führen oder sich auf die Unternehmensleistung auswirken können
- Steuerung der MS-Office-Lizenzen, Vergleich zwischen genutzten und erworbenen Lizenzen
- Anwendungen mit dem höchsten Bandbreitenverbrauch

## KONTROLLE DES ZUGRIFFS AUF GESCHÄFTSDATEN

Zeigt den **Zugriff auf vertrauliche Dateien im Netzwerk**:

- Dateien, die am häufigsten von Netzwerkanwendern abgerufen und ausgeführt werden
- eitleisten und Karten mit Informationen zu den Daten, die im vergangenen Jahr gesendet wurden
- Identifizierung der Anwender, die auf bestimmte Computer im Netzwerk zugegriffen haben
- Länder, zu denen die meisten Verbindungen von Ihrem Netzwerk hergestellt werden



## ECHTZEIT - WARNMELDUNGEN

**Konfigurieren Sie Warnmeldungen** für mögliche Sicherheitsverletzungen oder Verstöße gegen die Datenmanagementrichtlinie des Unternehmens:

- Standardwarnmeldungen zur Anzeige von Risikosituationen
- Unternehmensspezifische Warnmeldungen, die auf Anfragen von Anwendern basieren
- Sieben Methoden der Informationsdarstellung (mittels Bildschirmanzeige oder per E-Mail, JSON, Service Desk, Jira, Pushover und PagerDuty)

**Spezielle Anwendungs- und Tooltabellen im Advanced Reporting Tool:**

<http://go.pandasecurity.com/reporting-tool/requirements>

**Anwendungs- und Tooltabellen im Advanced Reporting Tool – Schatten-IT:**

<http://go.pandasecurity.com/reporting-tool/tools>