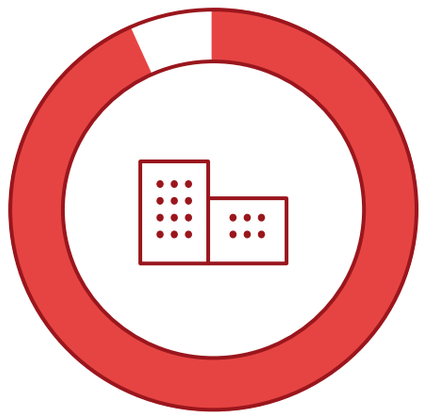
pandasecurity.com

Security Guide

zum Schutz vor Cyber-Erpressung

Mehr als 90 Prozent der kleinen und mittelständischen Unternehmen in Europa waren schon einmal Opfer eines Cyber-Angriffs.

In vielen Fällen kam es dabei zum Diebstahl sensibler Informationen.



91 Prozent der KMUs waren bereits Ziel von IT-Attacken.

Quelle: Shopper Software Seguridad en Pymes, Nielsen, April 2015

Die Gefahr von Malware-Angriffen zu ignorieren ist ein Risiko, das Sie auf keinen Fall eingehen sollten.

Panda gibt Ihnen Tipps, wie Sie Ihr Unternehmen bestmöglich schützen können.

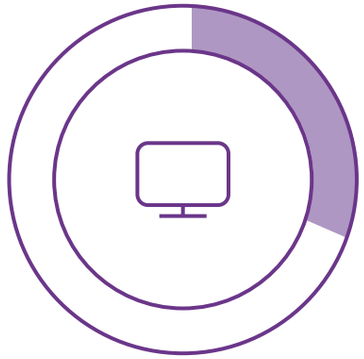
Was ist Cyber-Erpressung?

Bei der Cyber-Erpressung werden die Opfer eines IT-Angriffs gezwungen (Löse-)Geld zu zahlen, um die Folgeschäden des Angriffs zu begrenzen.

Eine der gängigsten Methoden der Cyber-Erpressung nutzt für Ihre Attacken die sogenannte Ransomware. Diese verschlüsselt wertvolle Informationen und Daten des Opfers. Für die Entschlüsselung und Rückgabe der Daten verlangen die Hacker ein Lösegeld.

Nachdem das Erpressungsopfer das von den Cyber-Kriminellen geforderte Lösegeld gezahlt hat, erhält es gewöhnlich eine E-Mail mit dem Code für die Entschlüsselung seiner Daten. Die Zahlung erfolgt generell in Bitcoins, einer digitalen Währung, die in echtes Geld umgetauscht werden kann (1 Bitcoin = ca. 390 €). Die Cyber-Kriminellen nutzen diese Zahlungsmethode, da sie ihnen eine größtmögliche Anonymität gewährt. Leider ist die Zahlung des Lösegeldes jedoch keinesfalls eine Garantie dafür, dass das Unternehmen in Zukunft nicht mehr angegriffen wird.

In der Regel verbreitet sich die Ransomware durch Besuche auf infizierten Webseiten, via Software-Download oder mithilfe von Phishing-Mails. Dabei werden Social-Engineering-Techniken benutzt, die die Opfer dazu verleiten, auf bestimmte Dateien oder Links zu klicken, durch die die Schadsoftware ins System eingeschleust wird.



39%

Unsichere und betrügerische Webseiten

23%

Software-Downloads

19%

Malware, die per E-Mail empfangen wird

Infektionsquellen
Quelle: Shopper Software Seguridad en Pymes, Nielsen, April 2015

Wie nutzen Cyber-Kriminelle Ransomware für ihre Angriffe?

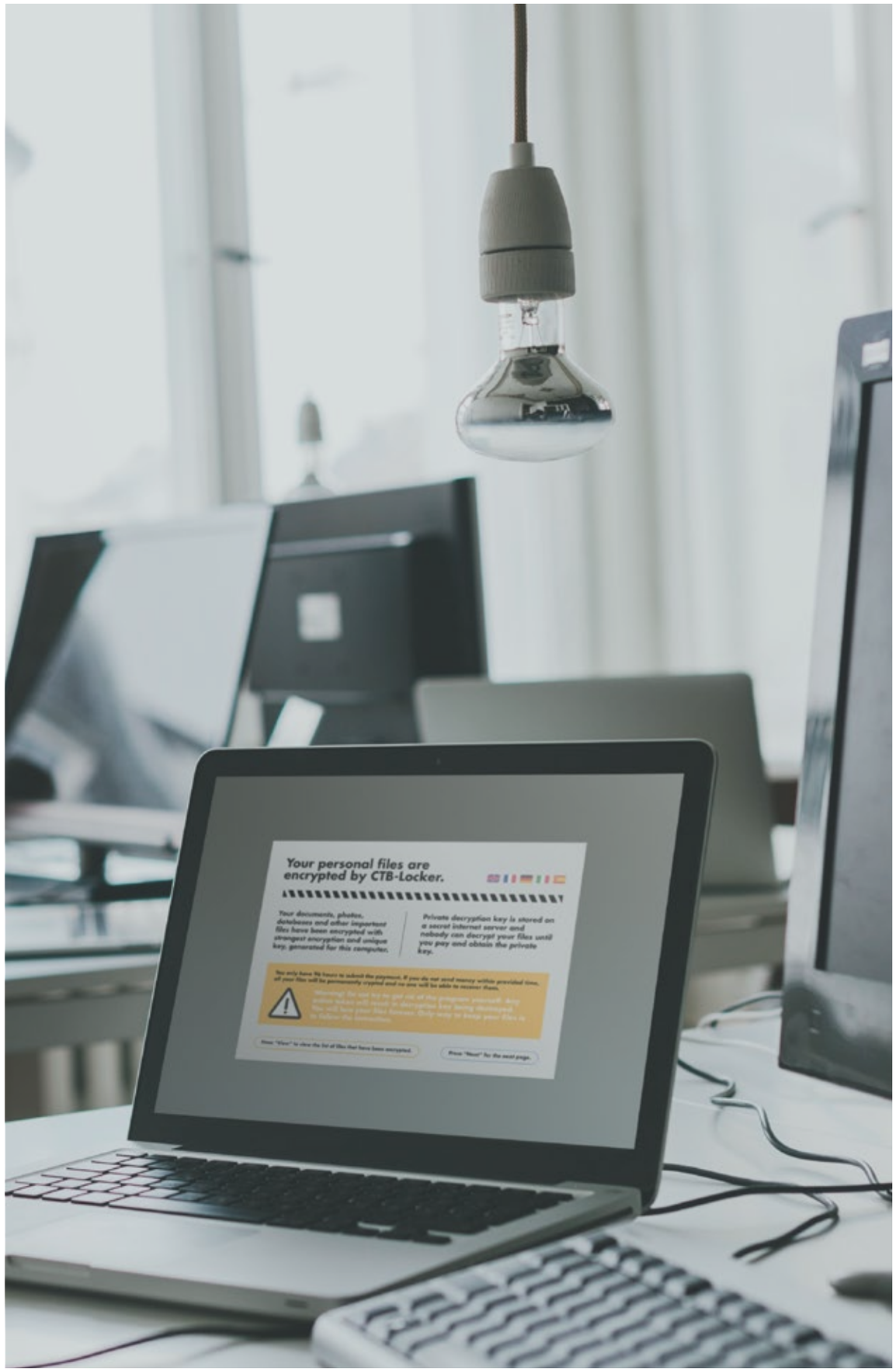
Ransomware wie Cryptolocker, CryptoWall oder CoinVault bedroht die Integrität aller Dateien, die sich auf den Computern innerhalb eines Netzwerks befinden.

Die Schadsoftware arbeitet immer nach demselben einfachen Prinzip: Sie verschlüsselt Dokumente und Daten und verlangt ein Lösegeld für die Entschlüsselung. Der Kontakt mit den Kriminellen erfolgt via „Tor“, einem Netzwerk zur Anonymisierung von Verbindungsdaten, das es den Kriminellen ermöglicht, anonym mit ihrem Opfern in Verbindung zu treten und so von den Strafverfolgungsbehörden nicht entdeckt zu werden.

Sollte Ihre Firma von Ransomware betroffen sein, haben Sie normalerweise eine eng begrenzte Zeit, um das Lösegeld zu zahlen. Zudem warnen die Angreifer davor, dass sich die Kosten für die Entschlüsselung Ihrer Daten erhöhen, wenn Sie nicht innerhalb dieser Frist zahlen.

Sollten Sie dann trotz angebotener Fristverlängerung keine vollständige Zahlung leisten, drohen die Erpresser mit der Löschung des Entschlüsselungs-Key. Die Firmendaten sind dann unwiderruflich verloren.

Doch Vorsicht: Selbst wenn Sie das Lösegeld zahlen, gibt es keine Garantie dafür, dass Sie Ihre Daten zurückerhalten.



Was tun, wenn Sie Opfer einer Cyber-Erpressung werden?

Lassen Sie sich nicht von Cyber-Kriminellen erpressen.

Es gibt keine Garantie dafür, dass eine Lösegeldzahlung das Problem lösen wird.

Tatsächlich haben die Opfer in vielen Fällen keinen Entschlüsselungs-Key (oder gar einen beschädigten Key) erhalten, obwohl sie das Lösegeld gezahlt hatten.

Zudem kommt es häufig zu wiederholter Erpressung. Mit Rückgabe der Informationen installieren die Cyber-Kriminellen Prozesse, die die Firmendaten bei Bedarf erneut verschlüsseln.

In anderen Fällen handelten die Hacker einen höheren Betrag aus, als den ursprünglich geforderten, nachdem die Zahlungsbereitschaft signalisiert wurde.

Löschen Sie sämtliche Spuren von Malware von Ihren Computern.

Um die Ransomware vollständig aus Ihren Systemen zu entfernen, empfehlen wir Ihnen die **Nutzung des Panda Cloud Cleaner** im Offline-Modus.

Der Cloud Cleaner ist eine kostenfreie Lösung von Panda Security, die Ihren PC analysiert und feststellt, ob und inwiefern dieser mit Malware infiziert wurde. Zudem ist das Tool darauf spezialisiert, alle Spuren fortschrittlicher Schadsoftware von den betroffenen Computern zu entfernen

.

Stellen Sie alle verschlüsselten Dateien wieder her.

Dazu ist es erforderlich, dass Sie zuvor die File History (Windows 8.1 und 10) oder System Protection (Windows 7 und Vista) aktiviert haben. So können die Veränderungen, die die Malware an den Dateien vorgenommen hat, rückgängig gemacht werden.

Zusätzlich empfehlen wir unbedingt, regelmäßig Sicherheitskopien von unentbehrlichen Dateien anzufertigen. Diese sollten auf einem externen, netzwerkunabhängigen System gespeichert sein. Und Achtung: Sollten Sie erst kurz vor dem Angriff ein Backup Ihrer wichtigen Dokumente gemacht haben, raten wir Ihnen, diese zunächst nach Überresten der Malware zu scannen, bevor Sie sie wiederherstellen.

Denken Sie stets daran, dass die Popularität von Ransomware in den vergangenen Monaten extrem gestiegen ist.

In der Tat ist Ransomware mittlerweile zu einem Milliarden-Dollar-Geschäft geworden. Laut einer Studie der US-amerikanischen Cyber Threat Alliance hat eine einzige Form von Ransomware, CryptoWall 3.0, allein im Jahre 2015 mehr als 325 Millionen Dollar an Lösegeldzahlungen von US-amerikanischen Opfern eingebracht.

Die zunehmende Anzahl von Malware-Mutationen sowie ständig neuentwickelte Ransomwaretypen machen es den traditionellen, blacklist-basierten Antivirenlösungen schwer, diese fortschrittlichen Bedrohungen zu entdecken.

Deshalb ist es unerlässlich, eine moderne Sicherheitslösung zu haben, die auch fortschrittliche Bedrohungen entdeckt und Ihre Computer vor gezielten und Zero-Day-Angriffen sowie neuen Versionen von Ransomware schützt.

Was ist Malware und welche sind die häufigsten Malware-Typen?

Als Malware wird jede Art von Schadprogramm oder IT-Code bezeichnet, deren Ziel es ist, Netzwerke und Computer zu infiltrieren, um Schaden anzurichten, zu spionieren und Informationen zu stehlen. Die gefährlichsten Arten von Malware sind:

RANSOMWARE

Sie blockiert den PC, entzieht dem Anwender die Kontrolle über seine Daten und Arbeitsprozesse, verschlüsselt Dateien und fordert ein Lösegeld für die Rückgabe der Daten.

EXPLOIT

Es nutzt Sicherheitslücken oder Schwachstellen in den Kommunikationsprotokollen aus, um in Ihren Computer zu gelangen.

SPYWARE

Sie sammelt Namen, Zugangsdaten, Passwörter und alle Arten von Informationen über Ihre Firma.

PHISHING

Über gefälschte E-Mails, Webseiten oder SMS werden Daten von Internetnutzern abgefangen. Ziel dieser Art von Betrug ist es, an persönliche Zugangsdaten und Passwörter für Bankkonten und ähnliches zu gelangen und diese zu missbrauchen.

TROJANER

Sie installieren verschiedene Anwendungen, sodass Hacker die Kontrolle über den Computer übernehmen können. Sie kontrollieren Ihre Dateien und stehlen vertrauliche Informationen.

APT (ADVANCED PERSISTENT THREAT)

Ein Advanced Persistent Threat (deutsch: fortschrittliche andauernde Bedrohung) ist ein zielgerichteter Angriff auf Ihre IT-Infrastruktur. Hierbei verschafft sich eine unautorisierte Person Zugriff auf Ihr Netzwerk und hält sich dort möglichst lange unentdeckt auf, um möglichst viele sensible Daten zu stehlen.

SCAM

Unter einem Scam versteht man einen großangelegten Online-Betrug, dessen Ziel es ist, die Opfer zu einer Geldzahlung zu bewegen, zum Beispiel um an eine angebliche Gewinnspielprämie zu kommen oder eine erfundene Erbschaft zu erhalten.

BACKDOOR

Durch das Öffnen einer „Hintertür“ werden Sicherheitsmaßnahmen umgangen, um die Kontrolle über Ihr Computersystem zu übernehmen.

KEYLOGGER

Sie protokollieren alle Eingaben des Benutzers an der Tastatur. Keylogger werden von Cyberkriminellen genutzt, um an vertrauliche Daten – wie Kennwörter oder PINs – zu gelangen.

BOT

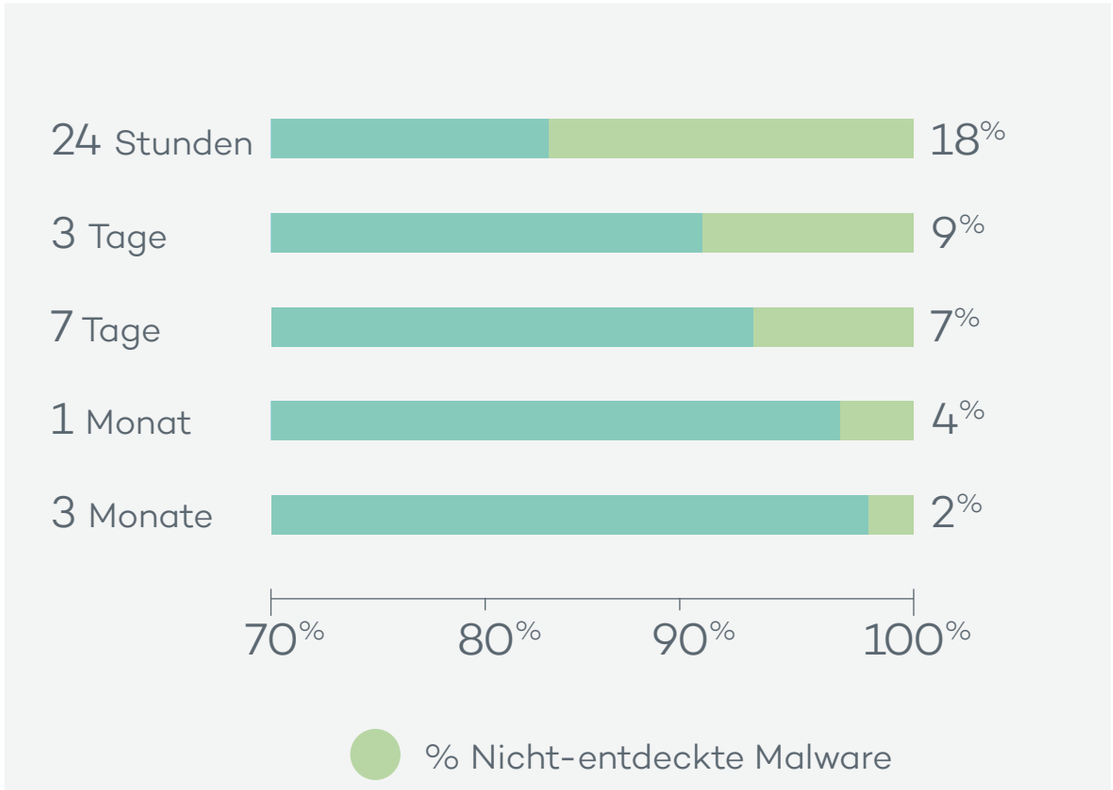
Das ist ein Computerprogramm, das bestimmte Aufgaben automatisiert und selbstständig ausführt. Bots werden zum Beispiel für das Sammeln von E-Mail-Adressen eingesetzt.

WÜRMER

Ein Computerwurm ist ein Schadprogramm, das sich selbst vervielfältigen kann und so all Ihre Computer im Netzwerk infiziert. Würmer verbrauchen einen Großteil der Netzwerkressourcen und können so zu einer Überlastung führen.

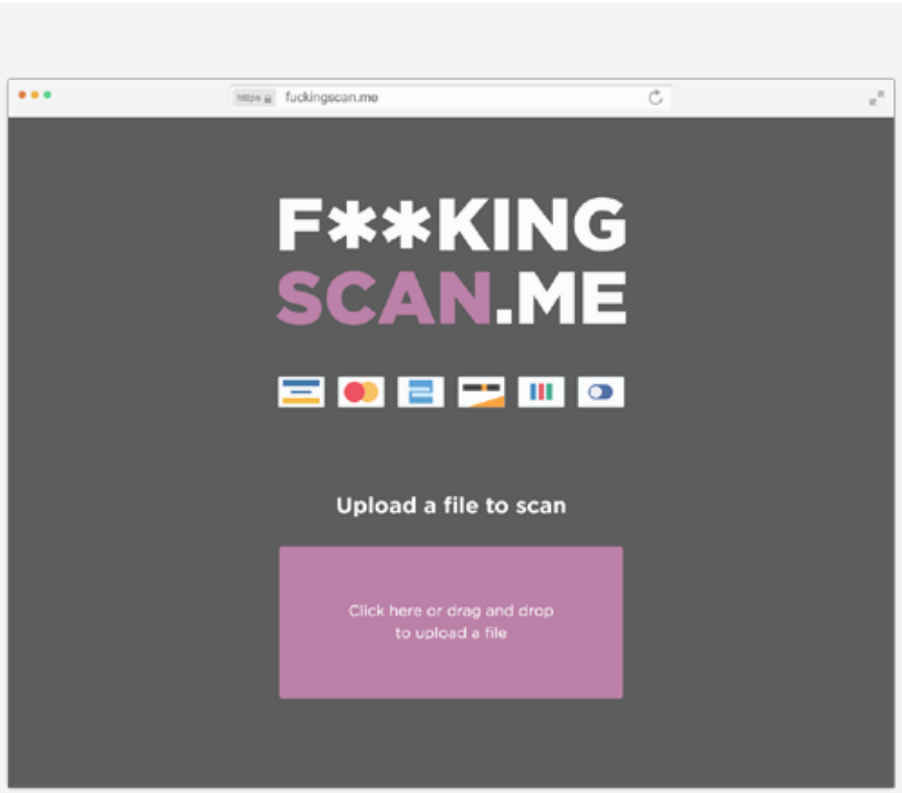
Entwicklung von Malware, Komplexität und Ausgereiftheit

Die Technologien, die von traditionellen Antivirenlösungen genutzt werden (Signaturdateien, Heuristik), sind rein reaktiv. **18 Prozent der neuentwickelten Malware-Exemplare werden von traditionellen, blacklist-basierten Antivirenlösungen innerhalb der ersten 24 Stunden nicht entdeckt. Drei Monate später sind zwei Prozent dieser Schadcodes immer noch unerkannt.**



Können traditionelle Antiviren fortschrittliche Bedrohungen stoppen?

Keine blacklist-basierte Antivirenlösung schafft das. Es gibt sogar Webseiten, auf denen man prüfen kann, ob eine bestimmte Malware von der gängigen Antivirensoftware erkannt wird. **Sobald ein Hacker überprüft hat, dass sein Schadcode von keinem Antivirus entdeckt werden kann, bringt er ihn in Umlauf.**



5 Empfehlungen zum Schutz vor Cyber-Angriffen

1. Sensibilisieren Sie die Anwender

Sorgen Sie dafür, dass Ihre Mitarbeiter die Risiken von Phishing kennen, keine unbekannten Dateien oder Anwendungen herunterladen und unseriöse Webseiten meiden.

2. Seien Sie vorsichtig im Internet

Legen Sie Richtlinien für das Surfen im Internet fest, die die Sicherheit der Webseiten kontrollieren, auf die von den Mitarbeitern zugegriffen werden kann.

3. Eine Lösung, die Ihre Bedürfnisse erfüllt

Prüfen Sie, ob Sie die Schutzlösung haben, die Ihr Unternehmen benötigt, und halten Sie diese immer auf dem neuesten Stand.

Wir empfehlen eine Lösung mit verschiedenen Sicherheitsebenen, die in der Lage ist, fortschrittliche Bedrohungen zu erkennen und zu blockieren.

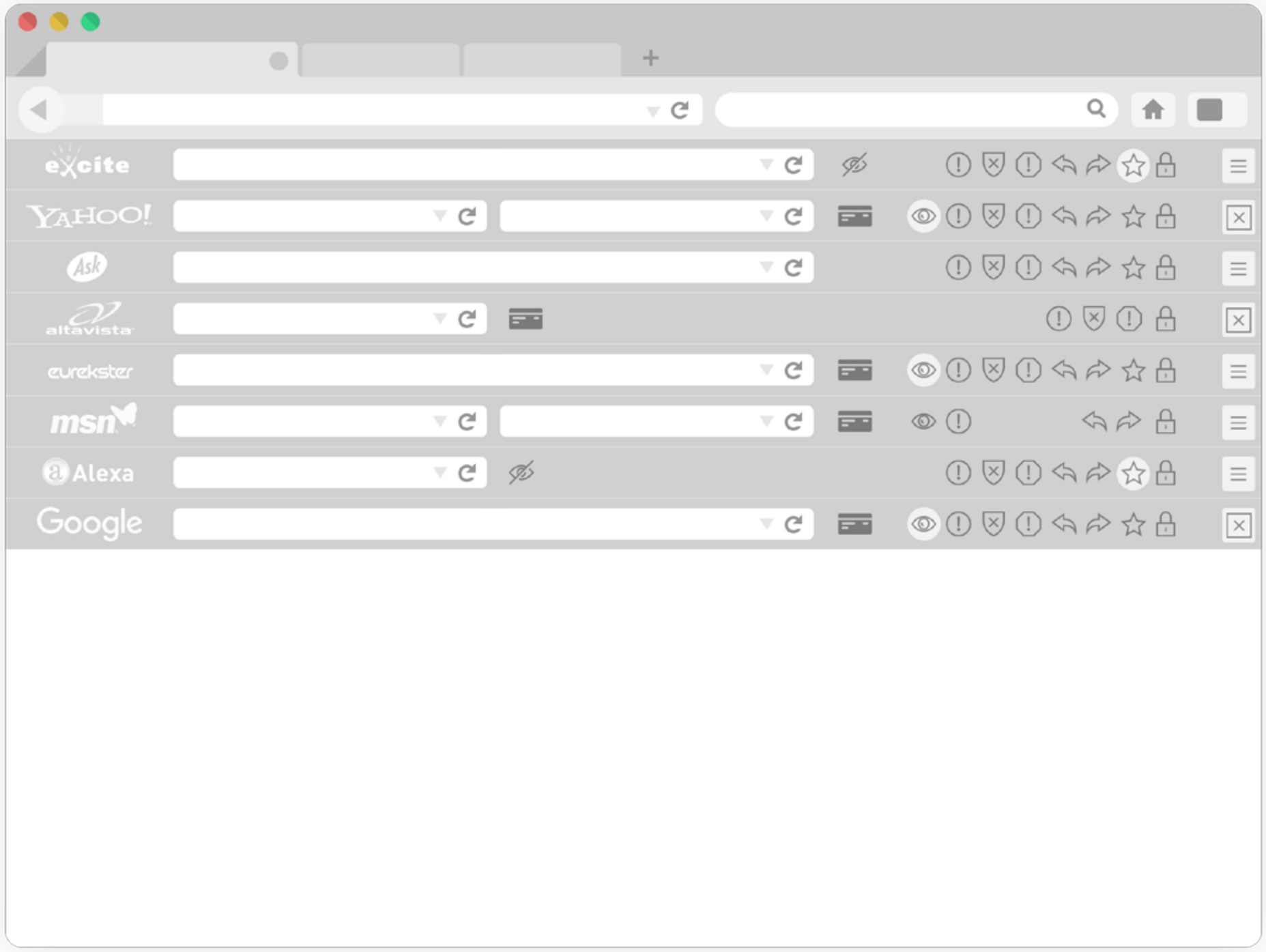
4. Entwickeln Sie interne Protokolle

Richten Sie Protokolle und Sicherheits-maßnahmen ein, um die Installation und Ausführung der gesamten Software zu kontrollieren. Sie sollten außerdem Ihren Bestand an Anwendungen regelmäßig überprüfen und nicht-genutzte Software löschen.

5. Halten Sie Ihre Systeme & Apps immer auf dem neuesten Stand

Legen Sie eine Richtlinie für das Aktualisieren Ihrer Anwendungen fest sowie für das Sperren oder Beseitigen von Apps, wenn diese vom Unternehmen nicht benötigt werden.

Es ist äußerst wichtig, sich vor Sicherheitslücken in bestimmten Anwendungen zu schützen, auch wenn diese generell vertrauenswürdig sind (wie zum Beispiel Java, Office, Chrome, Mozilla oder Adobe). Denn diese Schwachstellen könnten von Cyber-Kriminellen ausgenutzt werden, wenn sie nicht durch die regelmäßig veröffentlichten Patches beseitigt werden.



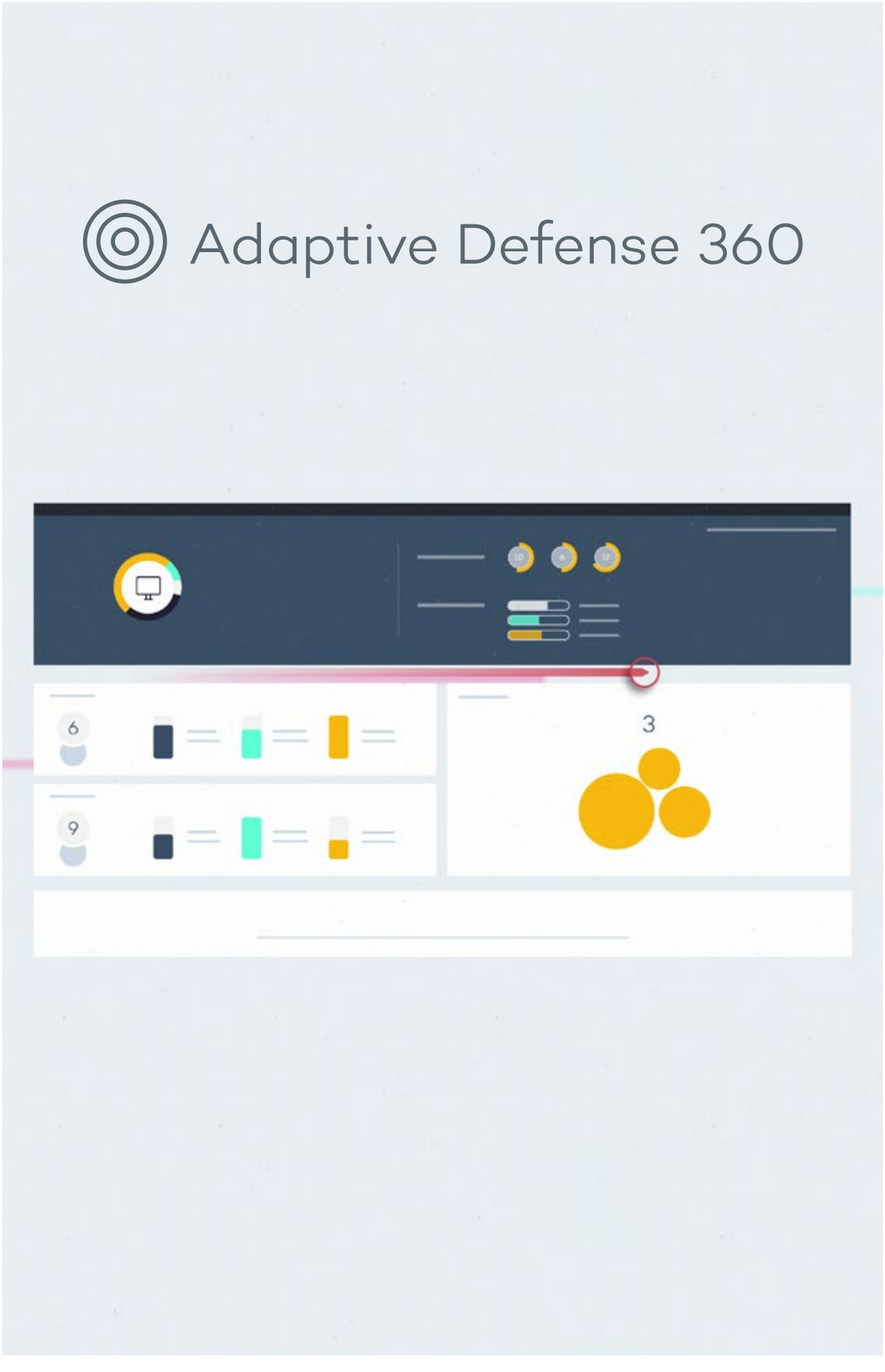
Toolbars stellen ein hohes Sicherheitsrisiko dar.

Wie können Sie Ihr Unternehmen wirklich schützen?

Panda Security hat ein neues Sicherheitsmodell entwickelt, das die totale Kontrolle über ALLE laufenden Prozesse auf ALLEN Endpoints innerhalb eines Netzwerkes ermöglicht.

Panda Security hat laut Marktforschungsinstitut Gartner* die erste und derzeit einzige fortschrittliche Cyber-Sicherheitslösung entwickelt, die Endpoint Protection (EPP)- und Endpoint Detection and Response (EDR)-Fähigkeiten kombiniert.

Dadurch sind wir in der Lage, Ihre Firma vor gezielten und Zero-Day-Angriffen oder anderen Arten von fortschrittlichen Bedrohungen zu schützen, einschließlich Cryptolocker.



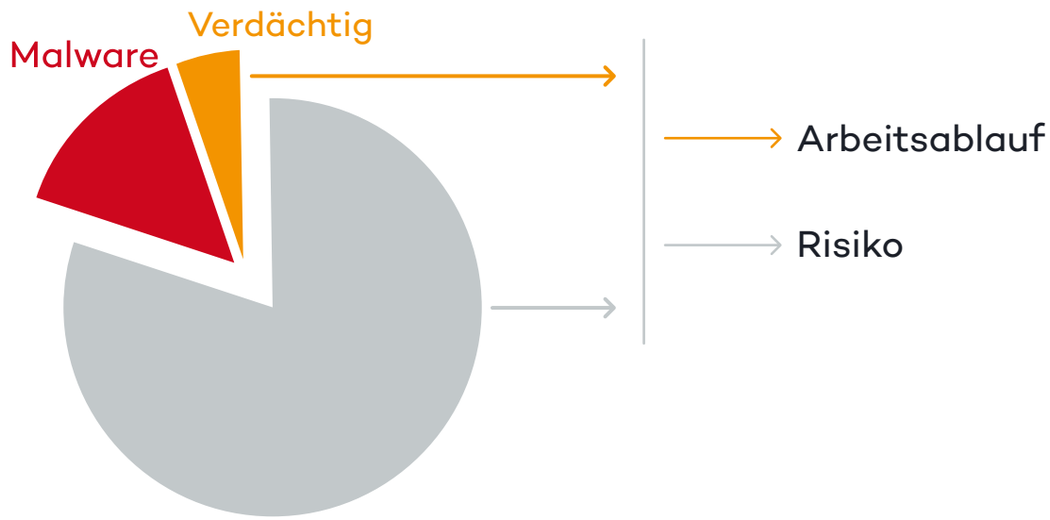
* Quelle: Magic Quadrant for Endpoint Protection Platforms, 22.12.2014

Adaptive Defense 360 bietet die höchstmöglichen Sicherheitslevels und ist damit blacklist-basierten Antivirenlösung weit voraus.

Adaptive Defense 360 überwacht, protokolliert und klassifiziert 100 Prozent der laufenden Anwendungen. Durch die Kombination mit weiteren EDR-Technologien ist diese Sicherheitslösung in der Lage, sämtliche unbekannte Prozesse und jedes ungewöhnliche Verhalten zu erkennen und zu blockieren.

Traditionelle, blacklist-basierte Antivirenlösungen

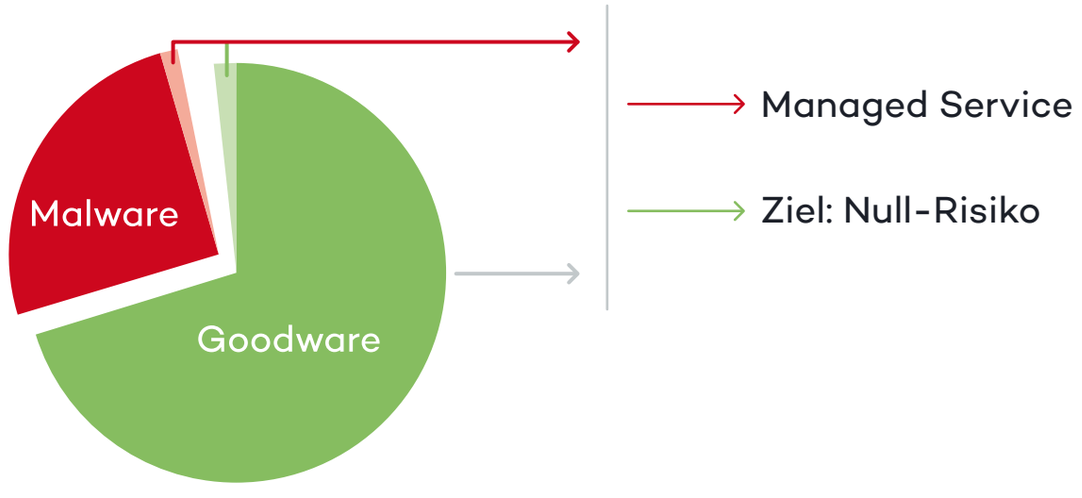
Sie können nur bekannte Malware erkennen.



Da traditionelle Antivirensoftware kein verdächtiges Verhalten klassifizieren kann, stellen fortschrittliche Bedrohungen (insbesondere gezielte und Zero-Day-Attacken) diese Schutzlösungen vor große Probleme.

Adaptive Defense 360

Es überwacht ausnahmslos ALLE aktiven Prozesse.



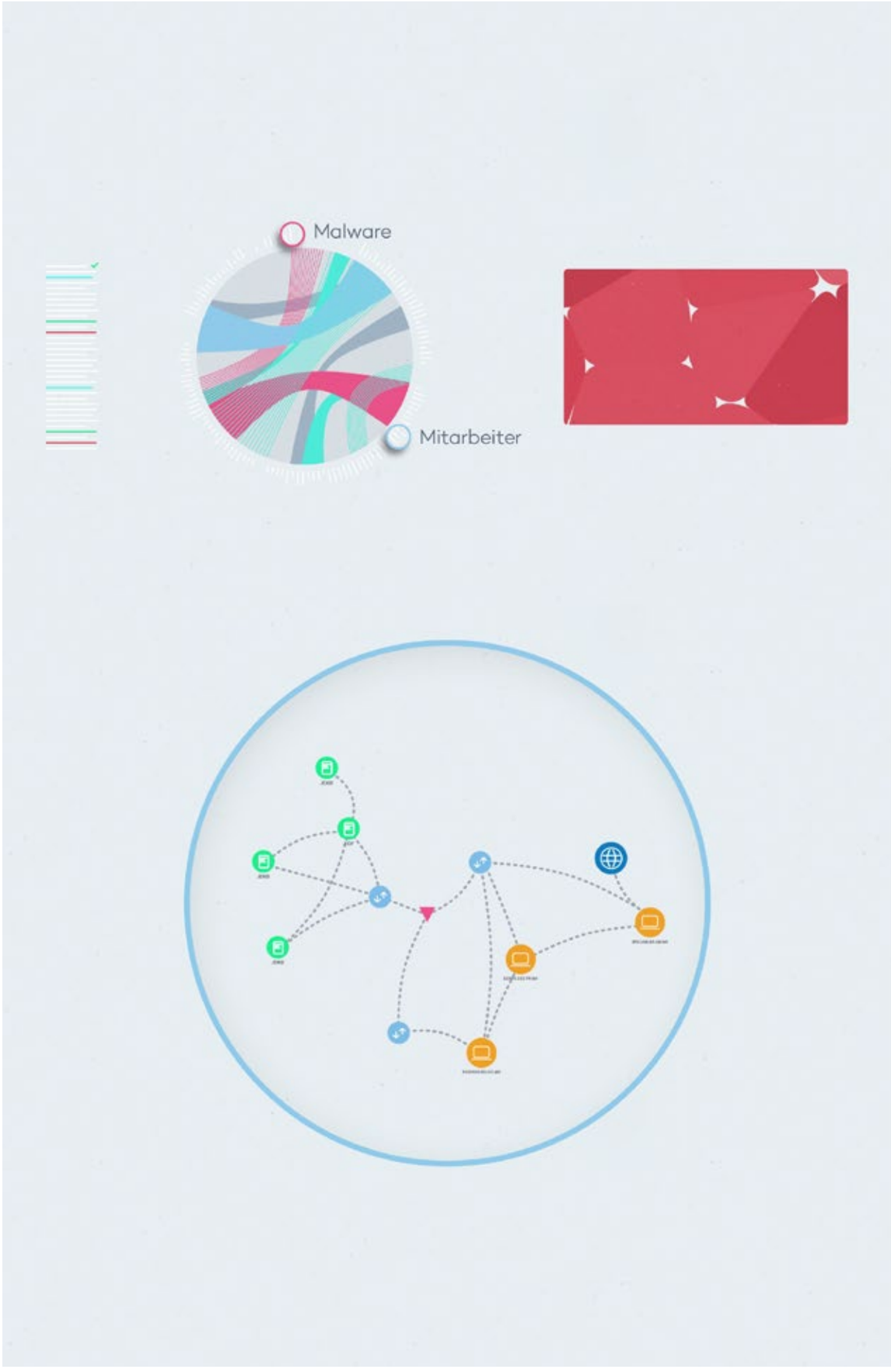
Adaptive Defense 360 erkennt mit hundertprozentiger Sicherheit, ob ein Prozess gut oder schlecht ist. Es klassifiziert absolut alles und lässt keinerlei verdächtige Prozesse zu.

Die Fähigkeit, absolut alles zu kontrollieren, was auf Ihren Computern passiert, ermöglicht Ihnen:

Datenlecks zu erkennen und zu vermeiden, ob sie nun durch Malware oder Ihre Mitarbeiter verursacht werden oder von irgendeinem Archiv, das Daten enthält (PDF, Word, Excel, Txt, ...).

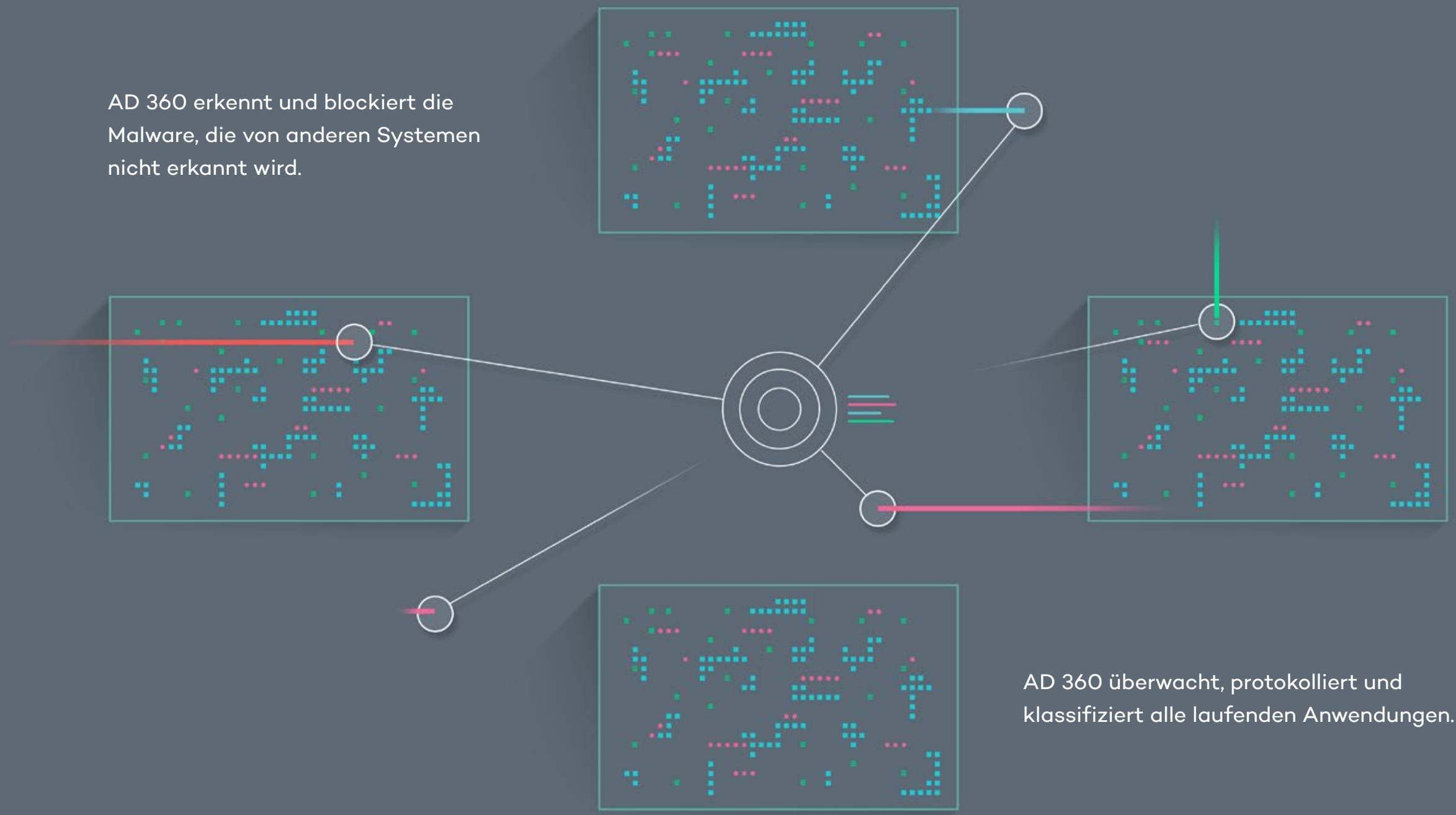
Schwachstellen zu entdecken und zu beseitigen, sowohl auf Ihren Systemen als auch in Ihren Anwendungen. Zudem wird die Nutzung unerwünschter Programme verhindert.

Gezielte Angriffe zu erkennen, die sich gegen Ihre Systeme richten.



Uneingeschränkte Transparenz - Absolute Kontrolle

AD 360 erkennt und blockiert die Malware, die von anderen Systemen nicht erkannt wird.



AD 360 überwacht, protokolliert und klassifiziert alle laufenden Anwendungen.

Adaptive Defense 360 in Zahlen

500K

Schützt bereits mehr als 500.000 Endpoints und Server weltweit.

1.5M

Hat mehr als 1,5 Millionen Anwendungen kategorisiert.

1.1M

Hat allein im vergangenen Jahr über 1,1 Millionen Sicherheitsverletzungen entschärft.

550K

Hat mehr als 550.000 Arbeitsstunden von IT-Administratoren eingespart, was eine geschätzte Kostenersparnis von 34,8 Millionen Euro ergibt.

100%

Hat in allen Umgebungen, in denen es installiert war, Malware entdeckt, unabhängig von den bereits bestehenden Schutzmechanismen.

Daten von 2015

Panda Security verfügt über 25 Jahre Erfahrung in der Entwicklung und Einführung von innovativen IT-Sicherheitslösungen.

Gegenwärtig werden mehr als 30 Millionen Endpoints weltweit von Panda geschützt.