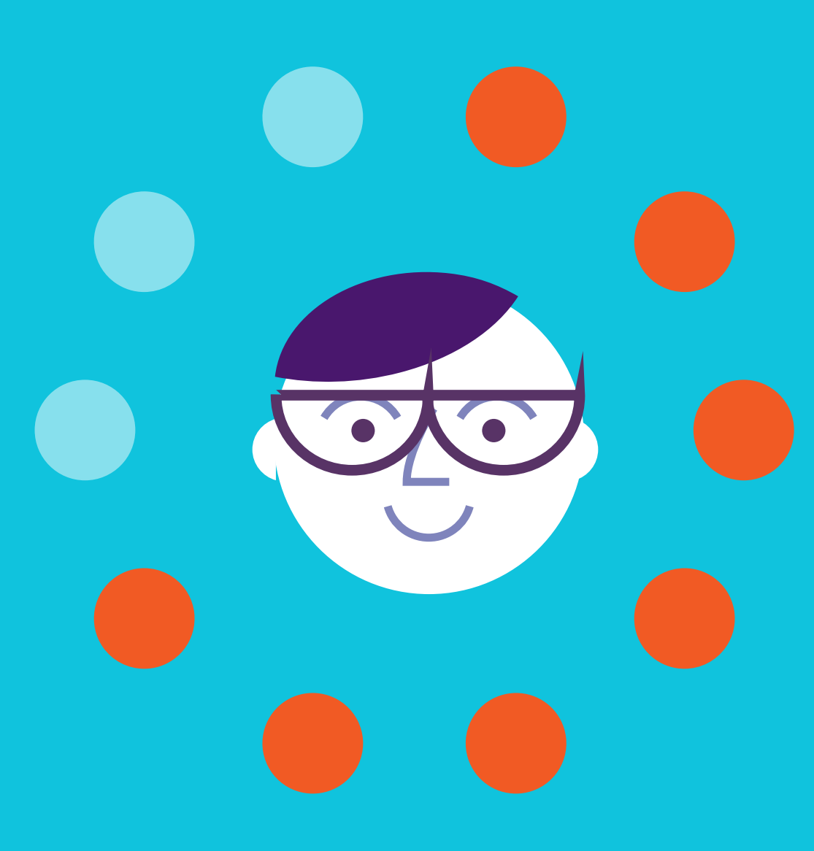
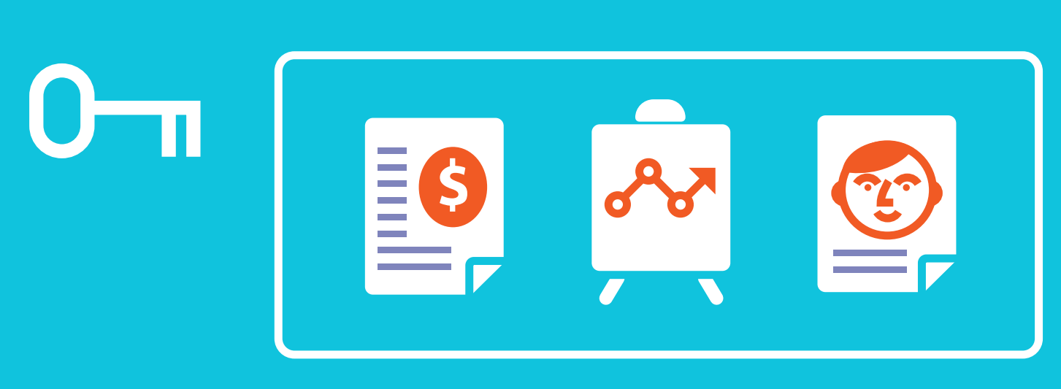
5 Schritte, die aufzeigen ob Ihre Datensicherheit durch interne Sicherheitslücken bedroht wird

Powered by EndpointProtector.com

1 Überprüfen Sie, auf welche Dokumente Ihre Mitarbeiter Zugriff haben

Daten zu Finanzen, Kunden, Marketingstrategien

7 von 10

Beschäftigten haben Zugriff auf vertrauliche Daten und nutzen diese auch bei der täglichen Arbeit

6 von 10

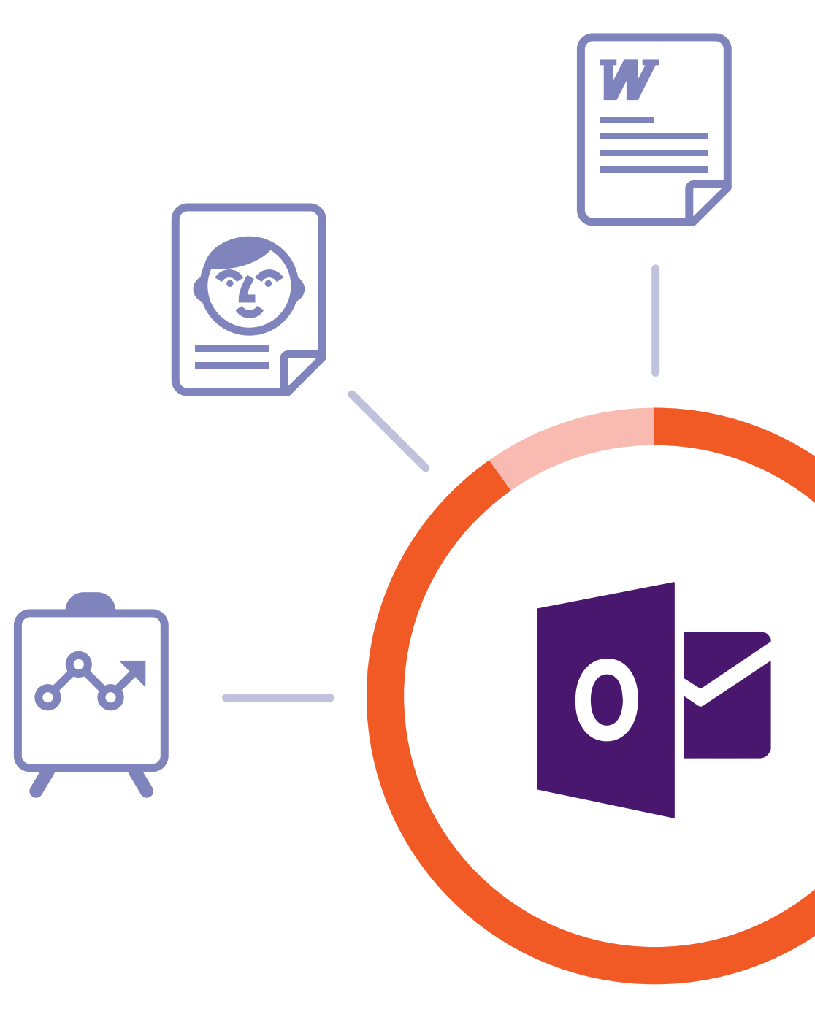
Beschäftigte wissen nicht, welche Daten vertraulich behandelt werden müssen und welche nicht

4 von 10

Beschäftigten haben bereits die Erfahrung gemacht, dass vertrauliche Daten in sozialen Netzwerken oder auf ähnlichen Plattformen gepostet wurden

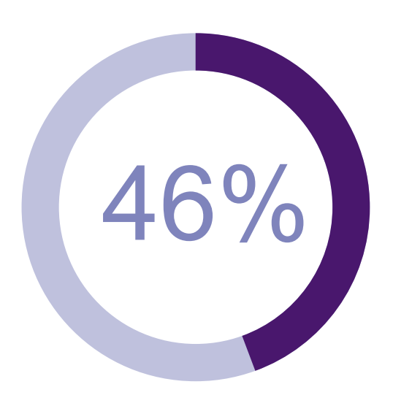
2 Stellen Sie fest, welche Mittel Ihre Mitarbeiter einsetzen, um Daten auszutauschen

Skype, Dropbox, Outlook, USB-Schnittstellen



90%

aller Beschäftigten verwenden Outlook, um Daten mit ihren Arbeitskollegen und anderen Empfängern auszutauschen



aller Beschäftigten kopieren Firmendaten auf private Rechner oder loggen sich zu Hause im Unternehmensnetzwerk ein, um von dort zu arbeiten

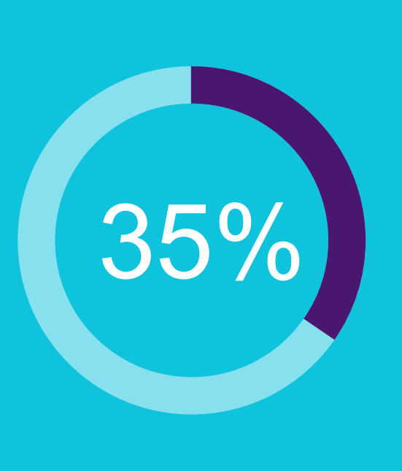
TOP 3

Zu den drei weltweit häufigsten Ursachen für Sicherheitslücken gehören verlorene oder gestohlene unverschlüsselte USB-Speicher

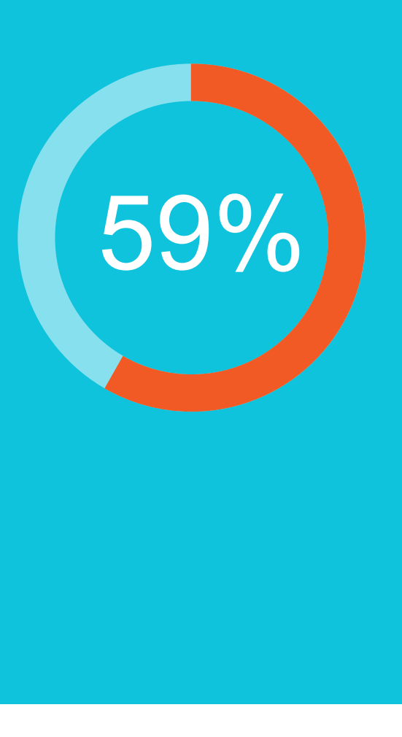
3 Testen Sie mit einem Quiz das Wissen Ihrer Mitarbeiter hinsichtlich Datensicherheit

18%

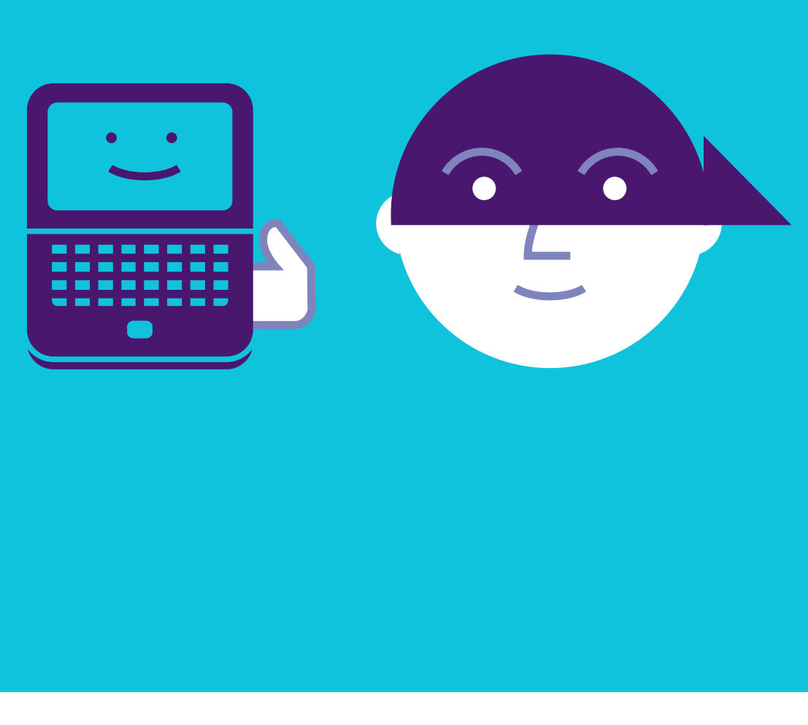
Beschäftigten teilen sich Passwörter mit Kollegen



Beschäftigten sind der Meinung, dass sie nicht für Datensicherheit verantwortlich sind

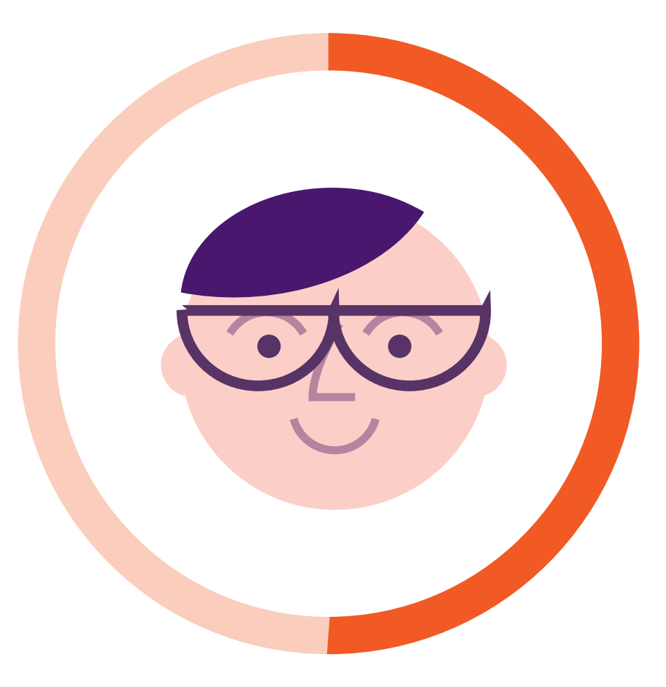


Beschäftigten denken, dass der Verlust eines Firmenhandys oder Notebooks mit Unternehmensdaten keine allzu große Gefahr darstellt



4 Finden Sie heraus, ob Ihre aktuellen Sicherheitswerkzeuge innerbetriebliche Datenlecks aufdecken würden, wenn diese auftreten

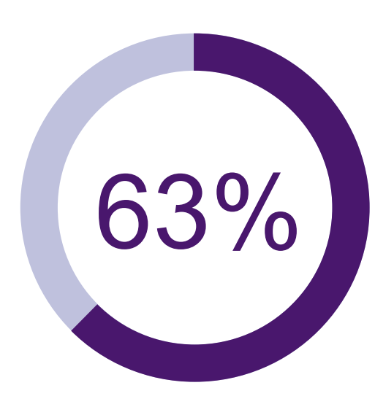
Können Sie die Person erkennen welche den Finanzreport an einen verdächtigen Empfänger gesendet hat?



50%

der Beschäftigten haben E-Mails an falsche Ansprechpartner verschickt

Was tun Sie, wenn Mitarbeiter vertrauliche Daten auf Google Drive kopieren?



der Unternehmen konnten ohne Verwendung einer Lösung zur Datenverlust-Prävention die Ursache einer Sicherheitslücke nicht genau definieren

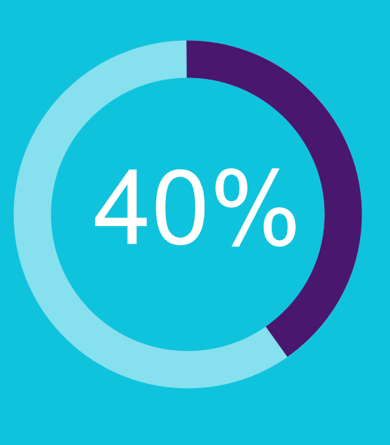
Wissen Sie, wie viele Mitarbeiter ihre geschäftlichen E-Mails auch auf ihrem persönlichen Smartphone lesen?

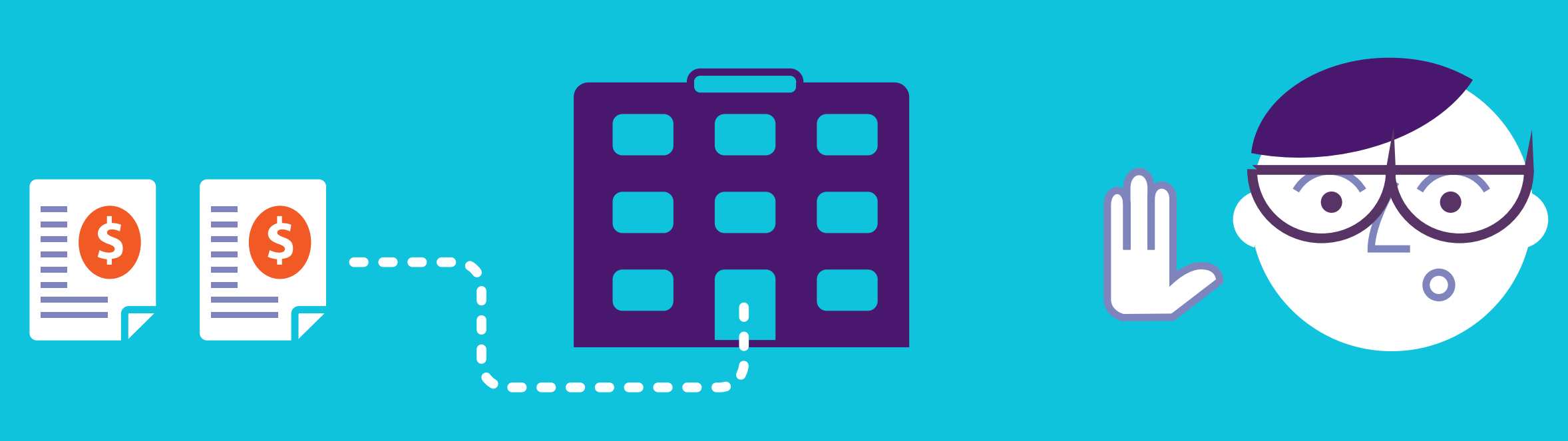
68%

aller Beschäftigten möchten jederzeit auf ihre geschäftlichen E-Mails zugreifen können, um sich bei Bedarf immer über wichtige Vorgänge zu informieren

5 Erkennen Sie, welche finanziellen und sonstigen Schäden Sicherheitslücken in Ihrem Unternehmen verursachen können

Kann sich Ihre Firma das leisten?





aller potenziellen Kunden lehnen eine Zusammenarbeit mit einem Unternehmen ab, in dem bereits eine Sicherheitslücke aufgetreten ist

$4.8 Mio $ beträgt die Höchststrafe, zu der bis 2014 ein Unternehmen wegen einer Sicherheitslücke verklagt wurde, die gegen die HIPAA-Regularien verstoßen hatte*

$3.5 Mio betragen die durchschnittlichen Kosten, die eine Sicherheitslücke verursacht**

Quelle: CoSoSys Forschung auf Kundenbasis mit einem Durchschnitt von 500 Computer aus folgenden Regionen: USA, LATAM, Europa und Asien
*http://www.hhs.gov/news/press/2014pres/05/20140507b.html
**http://www.darkreading.com/attacks-breaches/ponemon-cost-of-a-data-breach-rose-to-$35m-in-2013/d/d-id/1251019