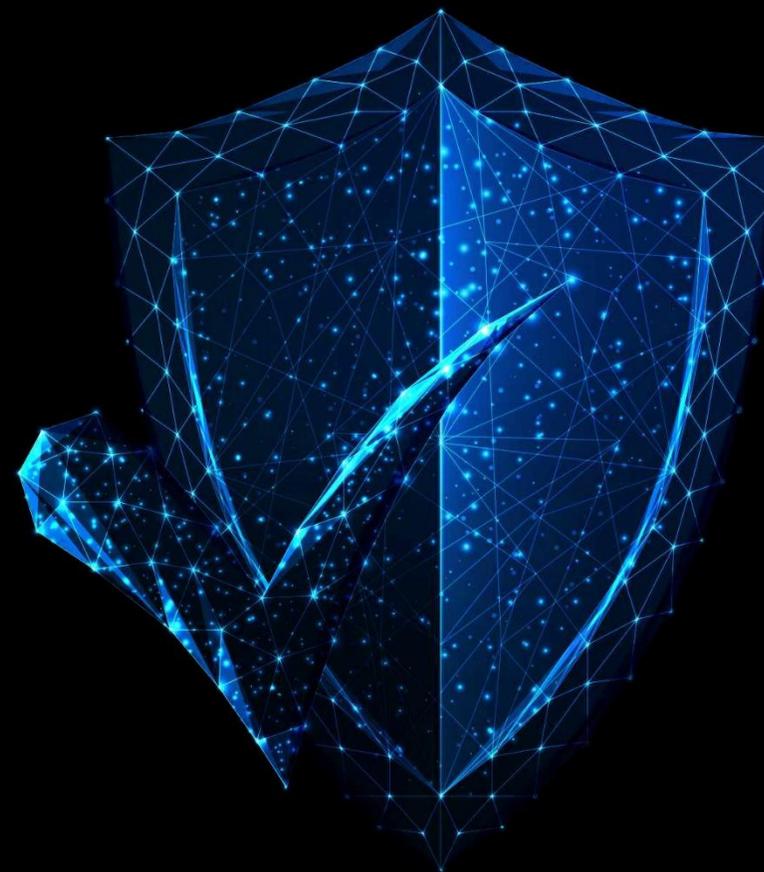


e3



## **e3 Data Loss Prevention**

Datenschutz ohne Kompromisse



## Anwendungsszenarien Data Loss Prevention



Externe und interne **Mitarbeitende** sind entweder aus Versehen (well meaning) oder mit Absicht (malicious) für den grössten Teil der verlorenen Daten verantwortlich. Dabei gilt **E-Mail** nach wie vor als kritischster Kanal.



Mit zunehmender Bedeutung der **Cloud** ist absehbar, dass der Web-Kanal und die Cloud bald den «Spitzenplatz» einnehmen werden. Die grenzenlose **Kollaboration** hat den Datenschutz «umfassender» gemacht.



Das Entdecken der Daten ist davon geprägt, zu wissen, welche Daten wie geschützt werden müssen. Gibt es **regulatorische** Anforderungen oder steht der Schutz der **Geschäftsgeheimnisse / Intellectual Property** im Vordergrund.



Immer aktuell bleibt der Schutz der **Kundendaten**. Das neue Schweizer **Datenschutzgesetz** setzt dem Bearbeiter von Kundendaten neu enge Grenzen, was mit persönlichen Informationen geschehen darf.



Für eine adäquate Lösung ist das Management von Vorfällen entscheidend. Hier fallen die meisten Kosten an. Somit lohnen sich Optimierung im **Incident Management** besonders. Je günstiger Fälle abgewickelt werden können, desto genauer können kritische Incidents geprüft werden. Und je genauer geprüft werden kann, desto geringer ist das Risiko.







## e3 DLP = DLP supercharged



### ◆ Automation

Der durchschnittliche Verarbeitungsaufwand für einen einzelnen DLP-Event beträgt 20-30 Minuten. Die Automation von Einzelschritten durch **e3 DLP** sorgt für eine Reduktion auf zwischen 1-10 Minuten.

Der Gesamteffekt dieser Automation sorgt für eine Gesamtkostenreduktion von 50-60% im Vergleich mit einer herkömmlichen DLP-Lösung.

In Zeiten sich erhöhender Sicherheitskosten sind Einsparungsmöglichkeiten wertvoll und bieten auch Raum, die Einsparungen wieder in erhöhten Schutz zu investieren.

### ◆ Case Management

Die wenigsten Szenarien betreffen einen Einzelfall. Meistens sind mehrere Incidents kombiniert. Dann erlaubt nur die Gesamtsicht auf die Situation ein angemessenes Vorgehen. **e3 DLP** bündelt Events deshalb zu Cases. Es erlaubt eine besser Gesamtbeurteilung und eine günstigere, konsistente und schnellere Verarbeitung.

Diese Cases werden zusätzlich in Kategorien eingeteilt. Jede Kategorie – zum Beispiel Zahlungen – kann dann nach dedizierten Regeln und Workflows verarbeitet werden. Das erhöht die Prozess-Standardisierung.

### ◆ Integration

Jede DLP-Lösung sammelt und liefert Daten. Gesammelt werden Informationen zu beispielsweise Angestellten, Kunden, Organisation, Schutzobjekten etc. Anschliessend liefert die Software dann Vorfälle, Evidenzen, Korrelation und Statistiken. Eine nachhaltige Integration spart Kosten im IT-Betrieb, schafft Freiräume und erhöht die Gesamtqualität der Schutzmechanismen. Das **e3 DLP** bringt die Integration auf ein neues, für jeden Kunden individualisiertes Level.

### ◆ User Interface

Im Umgang mit Events im Rahmen zentraler oder dezentraler Incident-Management-Modelle ist ein eingängiges User Interface wichtig. Nur die benötigten Informationen sollten angezeigt werden (verbessert die Privacy). Gesamtsicht soll einfach ersichtlich sein (Vorfall, Status, bisherige Schritte, etc.) und die verfügbaren Optionen werden verständlich präsentiert. Zusammen mit einem attributbasierten Berechtigungsmodell löst das **e3 DLP** User Interface die grosse Schwäche der meisten DLP-Systeme.

### ◆ Protect Investment

Investitionen in Prozesse sind aufwändig. Umso schöner wäre es, wenn diese Investitionen bei Änderungen gerettet werden könnten. **e3 DLP** ist herstellerunabhängig, so dass auch ein Wechsel der zugrundeliegenden Lösung oder eine Kombination mehrerer Lösungen möglich werden. Dann können die Prozesse in e3 DLP wiederverwendet werden und die Investitionen bleiben geschützt. Weiter müssen die Mitarbeitenden nicht neu ausgebildet werden. Das spart auch in der Zukunft viel Geld.





## e3 DLP: Business Case

e3 DLP automatisiert Prozesse, so dass sie besser, günstiger und schneller abgewickelt werden können. Die grössten Einsparungen können beim Incident Management gemacht werden. Im Vergleich mit einem reinen Hersteller-DLP sieht die Rechnung wie folgt aus:

e3 DLP	Pure	ESS	PRO
Employees	1'000	1'000	1'000
Minutes / Incident	25	12	4
Incident per Employee / Year	10	10	10
Incident Effort / Year	250'000	120'000	40'000
Remediator Minutes / Hour	50	50	50
Remediator Hours / Day	7	7	7
Remediator Days / Year	220	220	220
Remediator Minutes / Year	77'000	77'000	77'000
FTE's / Year	3.25	1.56	0.52

Ein fiktiver Business Case für 1'000 Angestellte. Die Rechnung zeigt auch auf, wieviel FTE durch Automation eingespart werden können.

Der Return on Investment von e3 DLP ist erfahrungsgemäss zwischen 2 und 4 Monaten.

▶▶ Erfahren Sie mehr von unseren Experten!





steht für IT-Sicherheit – seit über 20 Jahren. Unsere Stärke sind zukunftsichere Software-Lösungen zum Schutz vor Cyberangriffen und Datenverlust. Wir machen Unternehmen fit für die digitale Transformation und helfen ihnen, ihre Daten auf Basis der geltenden Vorschriften zu schützen und zu verwalten.

Dafür unterstützen wir Firmen bei der Realisierung zukunftsweisender Geschäftsmodelle, indem wir Chancen schaffen und Risiken senken. Bei allem haben wir stets die gesellschaftlichen und technischen Entwicklungen im Blick, sodass unsere Lösungen auch für die Herausforderungen von morgen gewappnet sind.

#### **e3 AG Schweiz - Zürich**

Binzstrasse 24  
CH-8045 Zürich

» [engage@e3ag.ch](mailto:engage@e3ag.ch)  
» +41 44 400 46 56

#### **e3 AG Schweiz - Bern**

Falkenplatz 3  
CH-3012 Bern

» [engage@e3ag.ch](mailto:engage@e3ag.ch)  
» +41 31 305 46 56

#### **Internationale Locations:**

- » Brasilien
- » Deutschland
- » Niederlande



[e3ag.ch](https://e3ag.ch)



**LinkedIn**

