

# CA Orchestra Data Loss Prevention

IN JEDEM UNTERNEHMEN GIBT ES SENSIBLE UND VERTRAULICHE DATEN, DIE FÜR DEN ERFOLG ENTSCHEIDEND SIND - VON FINANZDATEN UND KUNDENINFORMATIONEN BIS ZU PATENTEN UND PRODUKTFORMELN. WICHTIG FÜR DEN GESCHÄFTSBETRIEB DES UNTERNEHMENS IST, DASS DIESE DATEN MIT UMSICHT VERWENDET WERDEN. DARÜBER HINAUS MÜSSEN SIE ABER AUCH VOR MISSBRAUCH UND VERLUST GESCHÜTZT WERDEN. MIT CA ORCHESTRIA DATA LOSS PREVENTION SIND UNTERNEHMEN IN DER LAGE, KRITISCHE DATEN DORT, WO SIE GESPEICHERT BZW. GENUTZT WERDEN, ZU SCHÜTZEN UND ZU KONTROLLIEREN. DIES SENKT DIE RISIKEN DURCH UNKONTROLLIERTE INFORMATIONEN UND HILFT BEI DER EINHALTUNG VON RICHTLINIEN UND DATENSCHUTZBESTIMMUNGEN.

## ÜBERBLICK

Jedes Unternehmen muss seine IT-Infrastruktur und die unterschiedlichen sensiblen Daten schützen. Dazu muss es wissen, wie kritische Daten im Unternehmen verwendet und wo sie gespeichert werden.

Angesichts der vielen unternehmenseigenen und gesetzlichen Richtlinien, der Sorge um den Schutz von Kunden- und Mitarbeiterdaten und steigender Kosten bei Datenverlusten nimmt diese Herausforderung unweigerlich an Komplexität zu. Ein weiterer komplizierender Faktor ist, dass es in Unternehmen immer mehr Schwachstellen mit potenzieller Gefährdung gibt und zahlreiche Arten von Daten jeweils ein eigenes Maß an Schutz erfordern.

## NUTZEN

- CA Orchestra Data Loss Prevention unterstützt Ihr Unternehmen bei folgenden Zielen:
- Identifizierung und Analyse von Daten an verschiedenen Kontrollpunkten, z. B. am Endpunkt, im Nachrichtenserver und im Netzwerk
  - Minimierung des Risikos spektakulärer Verluste persönlicher Daten und geschützter Patientinformationen
  - Verhinderung der versehentlichen oder vorsätzlichen Veröffentlichung vertraulicher Informationen
  - Einhaltung von behördlichen und branchenspezifischen Datenschutzvorschriften
  - Vermeidung von Verstößen gegen allgemeine Sicherheits- und Verhaltensregeln des Unternehmens.

## VORTEILE

CA Orchestra Data Loss Prevention überwacht ein breites Spektrum von Datenaktivitäten und bietet verschiedene Gegenmaßnahmen. So wird ein ausgewogenes Verhältnis von ungestörtem Betrieb und effektiver Richtlinienumsetzung im gesamten Unternehmen gewährleistet. Die Lösung bietet in kritischen Unternehmensbereichen ein konfigurierbares Maß an Kontrolle, z. B. am Endpunkt, im Netzwerk, im Nachrichtenserver und für gespeicherte Daten.

Durch Nutzung eines Richtlinienkatalogs, einer einheitlichen Verwaltungsplattform und eines benutzerdefinierten Serviceprogramms können Unternehmen zugleich einen soliden ROI und eine schnelle Amortisierung erreichen.

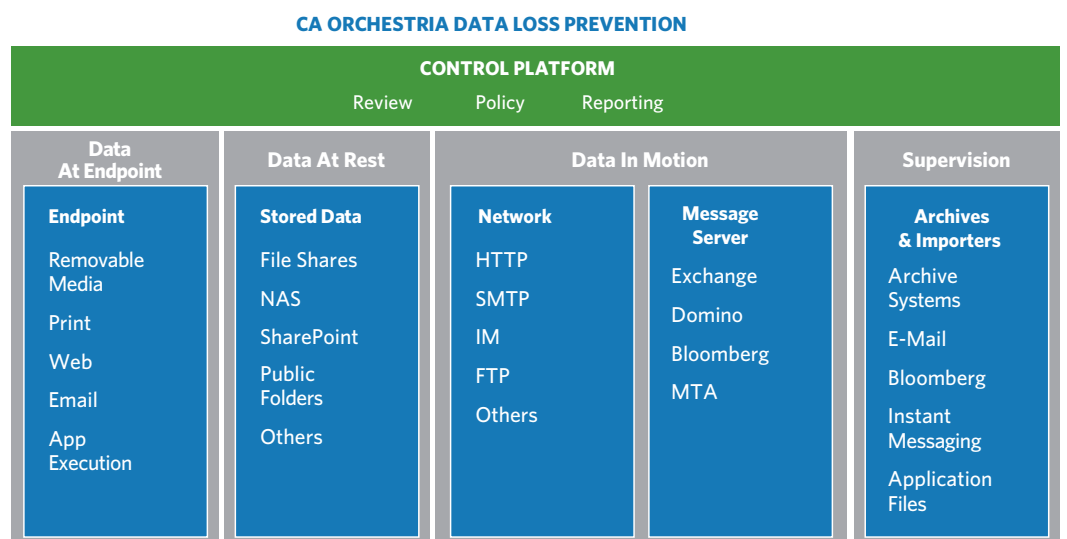
## CA Orchestria Data Loss Prevention identifiziert, klassifiziert und überwacht die Nutzung vertraulicher Daten im gesamten Unternehmen

Diese Lösung enthält eine umfassende Suite integrierter Produkte, mit deren Hilfe Unternehmen das Risiko bei der Verwendung nicht kontrollierter Informationen in den Griff bekommen und Datenverluste vermeiden können. CA Orchestria DLP ist eine skalierbare, präzise und kosteneffektive Lösung, mit der sich Datenverkehr im Netzwerk und Nachrichtensystem, gerade verwendete Daten am Endpunkt sowie auf Servern und in Repositories gespeicherte Daten im gesamten Unternehmen schützen und kontrollieren lassen. CA Orchestria DLP ist eine leistungsstarke Lösung, die mit nur einer Infrastruktur und Plattform allen Risiken an unterschiedlichen Kontrollpunkten begegnet.

### ABBILDUNG A

CA Orchestria DLP bietet Informationskontrolle und Schutz vor Datenverlust im gesamten Unternehmen mit nur einer Infrastruktur und Plattform.

### UMFASSENDE SCHUTZ VOR DATENVERLUST



## Wichtige Funktionen

### Plattform

**ZENTRALE PLATTFORM** Die Plattform ist eine gemeinsame Komponente der DLP-Komplettlösung. Sie ist auf die Anforderungen kleiner, mittlerer und großer Unternehmen skalierbar und bietet Unterstützung bei fortlaufendem Schutz und kontinuierlicher Kontrolle der Daten im gesamten Unternehmen.

**LEISTUNGSSTARKES REPORTING** Dank der leistungsstarken Reportingfunktionen kann das Risikoprofil der Informationen im gesamten Unternehmen nachvollzogen werden. Das Dashboard bietet die grafische Darstellung von Vorfällen und integrierte Drilldownfunktionen, um einzelne Vorfälle im Detail zu betrachten, umfassend zu prüfen und einer Ursachenanalyse zu unterziehen.

**GEEIGNETE MASSNAHMEN** Nach Aufdeckung einer Datenschutzverletzung kann die Lösung verschiedene Aktionen auslösen, z. B. Erfassen, Sperren, Warnen, Quarantäne, Verschlüsseln, Benachrichtigen, Umleiten, Klassifizieren/Kennzeichnen, Alarmieren, Verschieben, Löschen usw.

**MODULARE FUNKTIONEN** Ausgewählte Kontrollfunktionen können eingesetzt und bei Bedarf mühelos weitere Funktionen dazugeschaltet werden.

**VORDEFINIERTER RICHTLINIEN** Anhand von Richtlinien wird bestimmt, ob es sich bei einer Aktivität um einen Verstoß handelt. Anschließend wird eine entsprechende Maßnahme eingeleitet. Dank der in CA Orchestra DLP vordefinierten Richtlinien ist es nicht mehr notwendig, Richtlinien und Regeln von Grund auf neu zu erstellen. Jede dieser Beispielrichtlinien wurde auf Basis realer Anwendungsfälle in Unternehmen entwickelt. Für verschiedene Kontrollpunkte (Netzwerk, Nachrichtenserver, Endpunkt oder gespeicherte Daten) können vereinheitlichte Richtlinien angewendet werden.

**SICHERE PRÜFUNG UND WORKFLOW** Abrufen und Analysieren von Verstößen erfolgen über eine einzige webbasierte Prüfanwendung. CA Orchestra DLP bietet für die Überprüfung einen umfassenden Workflow mit Ereignisablaufplan, Eskalation und Genehmigung per Mausklick, vordefinierten Aktionsvorlagen, geschützten Prüfprotokollen und der Möglichkeit, Kommentare zu Vorfällen mit offenen Problemen als Freitext hinzuzufügen.

### **Am Endpunkt**

**KONTROLLE DER DATEN AM ENDPUNKT** Analyse der Benutzeraktivität am Endpunkt, wenn Dateien auf Wechselmedien wie USB-Speichergeräte kopiert oder verschoben werden. Je nach Anwendung, Gerät und Inhalt der Datei wird in Echtzeit verhindert, dass die Datei auf dem Wechselmedium gespeichert wird.

**DRUCKKONTROLLE** Analyse der Benutzeraktivität am Endpunkt, wenn Dateien an Drucker im Unternehmen gesendet werden. Je nach Drucker oder Inhalt der Datei wird in Echtzeit verhindert, dass die Datei an den Drucker übertragen wird.

**KONTROLLE VON OFF-LINE-AKTIVITÄTEN** Verwendung derselben Schutz- und Kontrollrichtlinien für Aktivitäten am Endpunkt bei bestehender Verbindung mit dem Firmennetzwerk oder beim Arbeiten zu Hause, in einem Hotel oder offline in einem Flugzeug.

### **Ruhende Daten**

**ERKENNEN VON RUHENDEN DATEN** Sie erhalten Einblicke in Daten, die aktuell nicht bewegt werden, und verhindern Zugriff oder versehentliche Offenlegung vertraulicher Informationen. Sie können Daten im ganzen Unternehmen scannen, identifizieren, kontrollieren und schützen – in Dateiservern, Archiven, Desktops, Collaboration-Tools und anderen Repositories.

**INTELLIGENTE KENNZEICHNUNG VON DOKUMENTEN** CA Orchestra DLP kann Microsoft Office-Dokumenten schon beim Einscannen Smart Tags hinzufügen. Diese Tags können für weitere Kontrollen verwendet werden und unterstützen die Optimierung der Aufbewahrungs- und Speicherressourcen des Unternehmens.

**UNABHÄNGIGE GLEICHZEITIGE SCANS** Scanserver können zahlreiche Aufgaben ausführen, jede mit eigenen definierten Scanorten. Die Aufgaben können einmalig, fortlaufend, mit vordefinierter Frequenz oder jeden Tag zu einer bestimmten Zeit ausgeführt werden. Es ist möglich, die Priorität einer Aufgabe auf maximierte Scanleistung oder minimale Systembelastung einzustellen.

### Datenverkehr

**SICHERER DATENVERKEHR** Sie erhalten Transparenz und verhindern den Verlust oder Missbrauch von Daten im gesamten Unternehmensnetzwerk. CA Orchestra DLP Network Appliance bietet Schutz am Netzwerkperimeter durch Analyse von Informationen in Protokollen wie E-Mail, IM, Web (HTTP), FTP usw. und entsprechende Maßnahmen.

**AKTIVER ODER PASSIVER NETZWERKMODUS** Network Appliance kann an Ports oder dem äußeren SPAN-Netzwerkhub eingesetzt werden.

**EINZIGARTIGE AUSFALLSICHERHEIT** Die integrierte Hard- und Software unterstützt beim Ausfall eines Geräts die Aufrechterhaltung der Netzwerkkonnektivität. So kann der Netzwerkverkehr wieder aufgenommen werden, auch wenn die Network Appliance an Leistung verliert.

**KONTROLLE VON MESSAGING-UMGEBUNGEN** E-Mail-Nachrichten werden am Nachrichtenserver, z. B. Microsoft Exchange und Lotus Domino, analysiert. Überprüft werden können interne, ausgehende und eingehende Nachrichten. So können E-Mail-Aktivitäten ohne den Einsatz von Endpunkt- oder Netzwerkkomponenten überwacht werden.

### Überwachung und Kennzeichnung

**INTELLIGENTE PRÜFUNG** Orchestra Intelligent Review analysiert dokumentierte Nachrichten und Dateien auf eventuelle Verletzungen und ermöglicht es den Prüfern, schädliche Aktivitäten schnell zu identifizieren, zu überprüfen und zu eskalieren.

**INTELLIGENTE KENNZEICHNUNG** Orchestra erstellt Smart Tags (Metadatatags) und überträgt Datensätze bzw. Informationen zusammen mit den Tags und allen relevanten Metadaten an ein geeignetes Archiv oder eine ECM-Plattform.

---

## Umfassender Schutz und umfassende Kontrolle für Ihre Informationen

In der Geschäftswelt von heute haben Mitarbeiter und Geschäftspartner Zugriff auf mehr Daten in mehr Formaten als jemals zuvor. Unternehmen müssen sich entsprechend vor dem Missbrauch dieser Daten schützen. Was die Sache kompliziert ist, sind die vielen Formen des Missbrauchs, z. B. Offenlegung vertraulicher Informationen, Weitergabe von persönlichen Daten und Patienteninformationen, missbräuchliche Freigabe und/oder unsachgemäßer Schutz geistigen Eigentums. Informationen zu schützen und zu kontrollieren ist nicht nur wichtig, um den effektiven Geschäftsbetrieb zu gewährleisten und Wettbewerbsvorteile zu erhalten, sondern wird in vielen Fällen auch durch die zahlreichen Vorschriften und Richtlinien gefordert.

Konsistente, präzise und wirkungsvolle Schutz- und Kontrollmechanismen für die Informationen im gesamten Unternehmen sind dabei von zentraler Bedeutung. Die Produkte von CA Orchestra DLP unterstützen Sie dabei, Ihre Informationen optimal zu schützen und bieten u. a. folgende Vorteile:

- Verringerung des beabsichtigten oder unbeabsichtigten Missbrauchs von Informationen im gesamten Unternehmen
- Aufklärung der Endbenutzer über die korrekte Nutzung der Informationen
- Verbesserte Compliance bei der Kommunikation und Verwendung sensibler Daten
- Anwendung bewährter, höchst präziser vordefinierter Richtlinien zur Einhaltung von Datenschutzerfordernungen

---

## Einige Erwägungen zu Compliance

Heutzutage müssen Unternehmen zahlreiche Compliance-Anforderungen erfüllen, die sich aus gesetzlichen bzw. behördlichen Vorschriften oder Richtlinien zum Datenschutz und zur Sicherheit oder betrieblichen Anforderungen ergeben. Hinzu kommt, dass diese Anforderungen in vielen Ländern ganz unterschiedlich sind. Folglich kann für eine bestimmte Information mehr als eine Vorschrift oder Richtlinie gelten. CA Orchestra DLP unterstützt Sie dabei, Ihre Informationen unter Berücksichtigung dieser Anforderungen zu identifizieren und zu überwachen – und das bei minimalen Auswirkungen auf Ihr Tagesgeschäft.

Mit CA Orchestra DLP können Sie ein breites Spektrum gesetzlicher Auflagen erfüllen, z. B.

- Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA), SEC Regulation S-P
- Health Insurance Portability and Accountability Act (HIPAA)
- PCI Data Security Standard (PCI DSS)
- Fair Credit and Accurate Transactions Act (FACTA) Red Flag
- Office of Foreign Assets Control (OFAC)
- International Traffic in Arms Regulations (ITAR)

**Hinweis:** CA bietet keine juristische Beratung an. Keines der hier genannten Softwareprodukte kann Ihnen die Verantwortung für die Einhaltung der genannten Vorschriften (insbesondere Gesetze, Statuten, Anordnungen, Regelungen, Richtlinien, Normen, Verwaltungsverordnungen, Rechtsverordnungen usw., zusammenfassend als „Vorschriften“ bezeichnet) oder Vertragsverpflichtungen gegenüber Dritten abnehmen. Nehmen Sie zu diesen Vorschriften oder Vertragsverpflichtungen kompetente Rechtsberatung in Anspruch.

---

## Vorteile

CA Orchestra Data Loss Prevention ist Bestandteil der zuverlässigen und bewährten Identity and Access Management (IAM)-Lösung von CA, mit der Sie Ihre IT-Assets auf vielen Plattformen und in zahlreichen Umgebungen schützen können. So stärkt die Lösung Ihre Fähigkeit, die Leistung, Zuverlässigkeit und Effizienz Ihrer gesamten IT-Umgebung zu optimieren. Der nächste Schritt ist die nahtlose Integration der Kontrolle und Verwaltung verschiedener Funktionen, z. B. Betriebs-, Speicher-, Lebenszyklus- und Servicemanagement, in die IT-Sicherheit.

Eine höhere Ebene der Kontrolle wird durch die EITM-Strategie von CA zur Vereinheitlichung und Vereinfachung des IT-Managements im gesamten Unternehmen verwirklicht. EITM ist ein dynamischer Ansatz, der das Management von Anwendungen, Datenbanken, Netzwerken, Sicherheit, Speicherung und Systemen abteilungs- und bereichsübergreifend integriert und automatisiert, um das Potenzial all dieser IT-Ressourcen auszuschöpfen. Das umfangreiche CA-Portfolio mit modularen IT-Managementlösungen unterstützt Sie dabei, Risiken besser in den Griff zu bekommen, Kosten zu senken und Ihren Service zu optimieren. Damit stellen Sie sicher, dass Ihre IT-Umgebung die Geschäftsanforderungen des Unternehmens erfüllt.

---

## Nächste Schritte

CA Orchestra Data Loss Prevention ist eine der marktführenden Lösungen zum Schutz und zur Kontrolle von Informationen. Überzeugen Sie sich selbst, wie die Lösung Ihr Unternehmen dabei unterstützen kann, wichtige Informationsressourcen zu schützen und Vorschriften besser einzuhalten.

---

Weitere Informationen, wie CA Orchestra Data Loss Prevention Sie dabei unterstützt, das IT-Management mit dem Ziel besserer Geschäftsergebnisse zu vereinheitlichen und zu vereinfachen, finden Sie unter <http://www.ca.com/dlp>.



**Weitere Informationen, wie CA das  
IT-Management vereinheitlicht und  
vereinfacht, finden Sie unter:**

CA Deutschland GmbH  
[ca.com/de](http://ca.com/de)

CA Software Österreich GmbH  
[ca.com/at](http://ca.com/at)

CA (Schweiz) IT Solutions Management AG  
[ca.com/ch/de](http://ca.com/ch/de)