Relativity

RelativityOne – Identity und Access Management

Sicherheit bei RelativityOne – ein ganzheitliches Konzept

Wir von Relativity sind davon überzeugt, dass die Schnittmenge von Cyber-Sicherheit und Produktsicherheit in allen Branchen immer wichtiger wird. Ganz unabhängig davon, wie eine potenzielle Schwachstelle beschaffen sein könnte oder welcher Angriff drohen könnte: Unsere Lösungen verfolgen konsequent drei Phasen: Vorbeugen, Erkennen und Reagieren. Im Rahmen dieser Strategie setzen wir auf eine umfassende Verteidigung in Verbindung mit proaktiver Bedrohungsaufklärung. So ist sichergestellt, dass die gesamte Angriffsfläche berücksichtigt wird. Das macht es für Angreifer extrem schwierig.

„Defense in Depth“

Unser Sicherheitsprogramm beruht auf einem mehrschichtigen Verfahren. Vom Access Management, also der Zugriffsverwaltung, bis zur eigentlichen Infrastruktur unterliegt alles dem Grundsatz „Defense in Depth“.

Die Grundpfeiler unserer Defense in Depth Strategie:

- Wir setzen modernste Tools für Prävention und Erkennung ein, um Bedrohungsakteure zu stoppen, bevor sie verwertbare Informationen abgreifen oder ihr kriminelles Vorhaben in die Tat umsetzen können.
- Wir scannen unsere Quellcodes und unsere Infrastruktur auf mehreren Ebenen des Softwareentwicklungszyklus, um Schwachstellen und Fehler zu erkennen.
- Wir setzen auf ein umfassendes Identity- und Access-Management (IAM), das sowohl intern entwickelte Tools als auch branchenführende Technologien umfasst. So stellen wir sicher, dass die Daten unserer Kunden geschützt sind und nur die von den Kunden benannten Personen darauf zugreifen können.

In diesem Whitepaper gehen wir insbesondere auf diesen letzten Punkt ein. Hierzu zeigen wir Ihnen im Überblick, wie wir Ihre und unsere Daten durch ein leistungsstarkes und umfassendes IAM-Programm schützen.

Sicherheit auf Basis von Identität und Zugriff

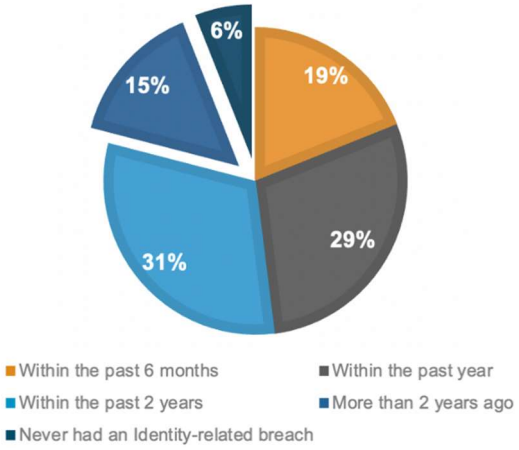
Jedes Sicherheitsprogramm beruht auf dem Grundsatz, dass dem richtigen Benutzer der jeweils notwendige Zugriff gewährt wird. Um eine solide Basis für Identität und Zugriff bereitzustellen, haben wir bei Relativity mehrere Schichten entwickelt.

Erstens zählt hierzu eine automatisierte Governance, die keinen dauerhaften Zugriff auf die Benutzeroberfläche des RelativityOne Front-End und auf die zugrunde liegenden Back-End-Komponenten der Infrastructure as a Service (IaaS) zulässt. Zudem haben wir eine Anwendung für den Just-in-Time (JIT) Zugriff entwickelt. Mit dem JIT-Zugriff lässt sich die Zeit, in der ein Benutzer Zugriff auf eine RelativityOne-Instanz hat, genau auf die von ihm benötigte Zeit begrenzen.

Mit Privileged Access Management (PAM) haben wir außerdem die veraltete gemeinsame Nutzung von Kennwörtern abgeschafft und die Multifaktor-Authentifizierung (MFA) für sämtliche Zugriffe eingerichtet.

Die letzte Schicht unseres Defense-in Depth-Konzepts für RelativityOne ist das Monitoring des Verhaltens von Benutzern und Entitäten (User and Entity Behavior Analytics, UEBA) über unser 24x7 Security Operations Center. Mit dem UEBA-Monitoring ist sichergestellt, dass Muster zu verdächtigen Aktivitäten, die von der Norm abweichen, sowohl von menschlichen als auch von maschinellen Benutzern erkannt werden.

79 % der Unternehmen gaben an, dass IAM in den letzten zwei Jahren den Großteil der Datenschutzverletzungen ausgemacht hat.



Wie wird der Zugriff auf RelativityOne gesteuert?

Der Zugriff auf RelativityOne wird auf drei Ebenen gesteuert:

- RelativityOne Front-End-Anwendung
- IaaS-Back-End-Komponenten, die RelativityOne unterstützen
- Cloud-Plattform, auf der RelativityOne eingesetzt wird

Der Zugriff in RelativityOne wird über Komponentengruppen gesteuert. Eine Komponente entspricht dabei einem Dienst oder einer Komponente von RelativityOne. Beispielsweise entspricht die Komponentengruppe SQL-PaaS unseren Ressourcen, die unseren Dienst SQL-PaaS unterstützen. Wenn ein Mitarbeiter von Relativity um Zugriff auf eine Komponentengruppe bittet, wird der Zugriff nur gewährt, wenn seine Rolle die Unterstützung dieser Komponente erfordert. In dem genannten Beispiel erhält nur ein Beschäftigter, der den Dienst SQL-PaaS entwickelt und unterstützt, Zugriff auf die Komponentengruppe SQL-PaaS.

Der Zugriff wird auf allen drei Ebenen durch unsere Erkennungs- und Monitoringsysteme überwacht und protokolliert. Warnmeldungen werden an unser Security Operations Center (SOC) weitergeleitet. Der Zugriff auf das Front-End und auf Infrastrukturkomponenten wird automatisch über eine intern entwickelte Self-Service-Anwendung gesteuert. Zur Fehlerbehebung können Beschäftigte diese für den benötigten Just-in-Time(JIT)-Zugriff auf die einzelne Komponente nutzen.

Ein JIT-Zugriff gewährt den Zugriff mit den geringstmöglichen Rechten für die minimal notwendige Zeit. Der Zugriff wird also für einen bestimmten Zeitraum gewährt und nach Ablauf dieses Zeitraums automatisch wieder entzogen. Auf diese Weise kann ein Mitarbeiter von Relativity, der mit der Fehlerbehebung für einen Kunden beauftragt ist, für einen begrenzten Zeitraum JIT-Zugriff auf einen einzelnen Mandanten oder die Rechte für eine einzelne Cloud-Komponente erhalten.

Wie geht es weiter, nachdem ein Relativity-Mitarbeiter Zugriff auf das Front-End erhalten hat?

Ein Relativity-Mitarbeiter, der Zugriff auf das Front-End erhalten hat, kann noch auf keine Workspaces zugreifen. Das verhindert die Lockbox-Funktion des Kunden welche standardmäßig aktiviert ist. Systemadministratoren und das Support Team können erst auf einen Workspace zugreifen, wenn sie zuvor zu einer vordefinierten Gruppe hinzugefügt worden sind. Auf diese Weise haben Kunden die Kontrolle darüber, wer auf ihre Workspaces zugreift.

Wenn ein Relativity-Mitarbeiter Zugriff auf einen Workspace des Kunden erhalten soll, muss der Kunde den betreffenden Relativity-Mitarbeiter zu einer vorab genehmigten Relativity-Gruppe hinzufügen. Nach Abschluss der Fehlerbehebung kann der Kunde den Zugriff wieder entfernen. Der Zugriff auf unsere Front-End-Instanzen erfolgt über ein Single Sign-On mit Okta. Wenn Passwort Provider zu Authentication Providern hinzugefügt werden, werden sie von denselben Anwendungen entfernt, die auch JIT unterstützen.

Wie sorgen wir für Transparenz gegenüber unseren Kunden?

Kunden können den Zugriff von RelativityOne über eine der folgenden Optionen überwachen:

Audit API

- Kunden können Informationen über Änderungen an ihren Lockbox-Einstellungen abrufen.

Sicherheitsbenachrichtigungen zur Kunden-Lockbox

- Administratoren, die zur Gruppe *Security Notifications* hinzugefügt wurden, erhalten automatisch E-Mail-Benachrichtigungen, sobald der Support von Relativity zu einem Workspace hinzugefügt wird. Das gleiche gilt, wenn die Kunden-Lockbox deaktiviert wird.

Relativity-Skripte

- Kunden können Informationen über die Zugehörigkeit oder den Zugriff auf einen Workspace per Skript abrufen. Darüber hinaus lassen sich Skripte auch nutzen, um Berichte individuell nach Bedarf anzupassen. Das Skript „User Workspace Access and Last Login“ zeigt beispielsweise an, wann sich ein Benutzer zuletzt angemeldet hat und auf welche Workspaces er zugegriffen hat.

Berichte zur Kunden-Lockbox

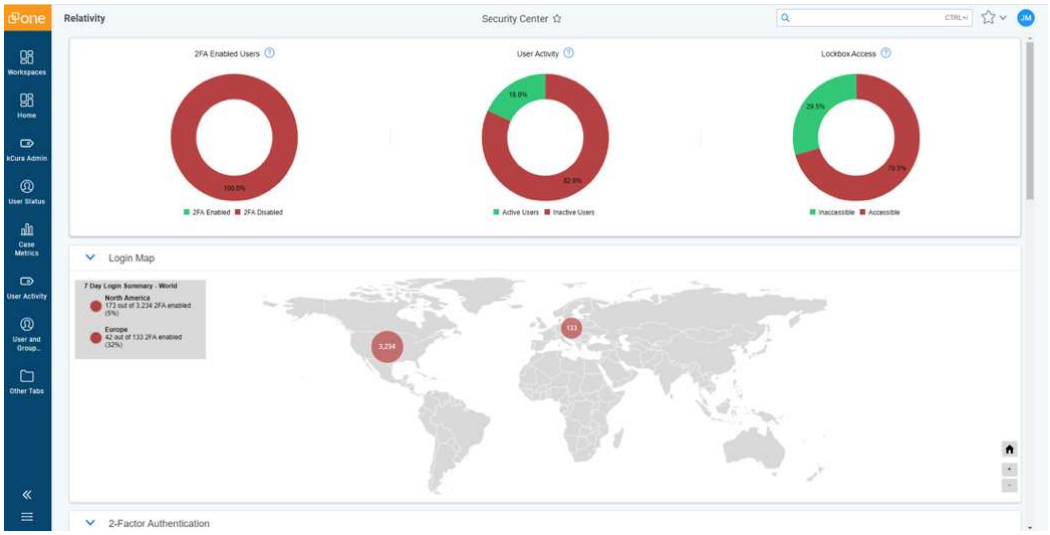
- Kunden können Berichte zur Lockbox-Nutzung per Skript (t-sql) abrufen.

Sicherheits-Logs von RelativityOne

- Hierzu zählen Infrastrukturprotokolle, wie Aspera-Authentifizierungsprotokolle, Protokolle zur Erkennung von Malware, Sicherheitsprotokolle und Keyvault-Protokolle zu den kundenseitig verwalteten Schlüsseln („Customer Managed Keys“). (Änderungen sind in Abhängigkeit von Anpassungen an die Infrastruktur von RelativityOne vorbehalten.)

RelativityOne Security Center

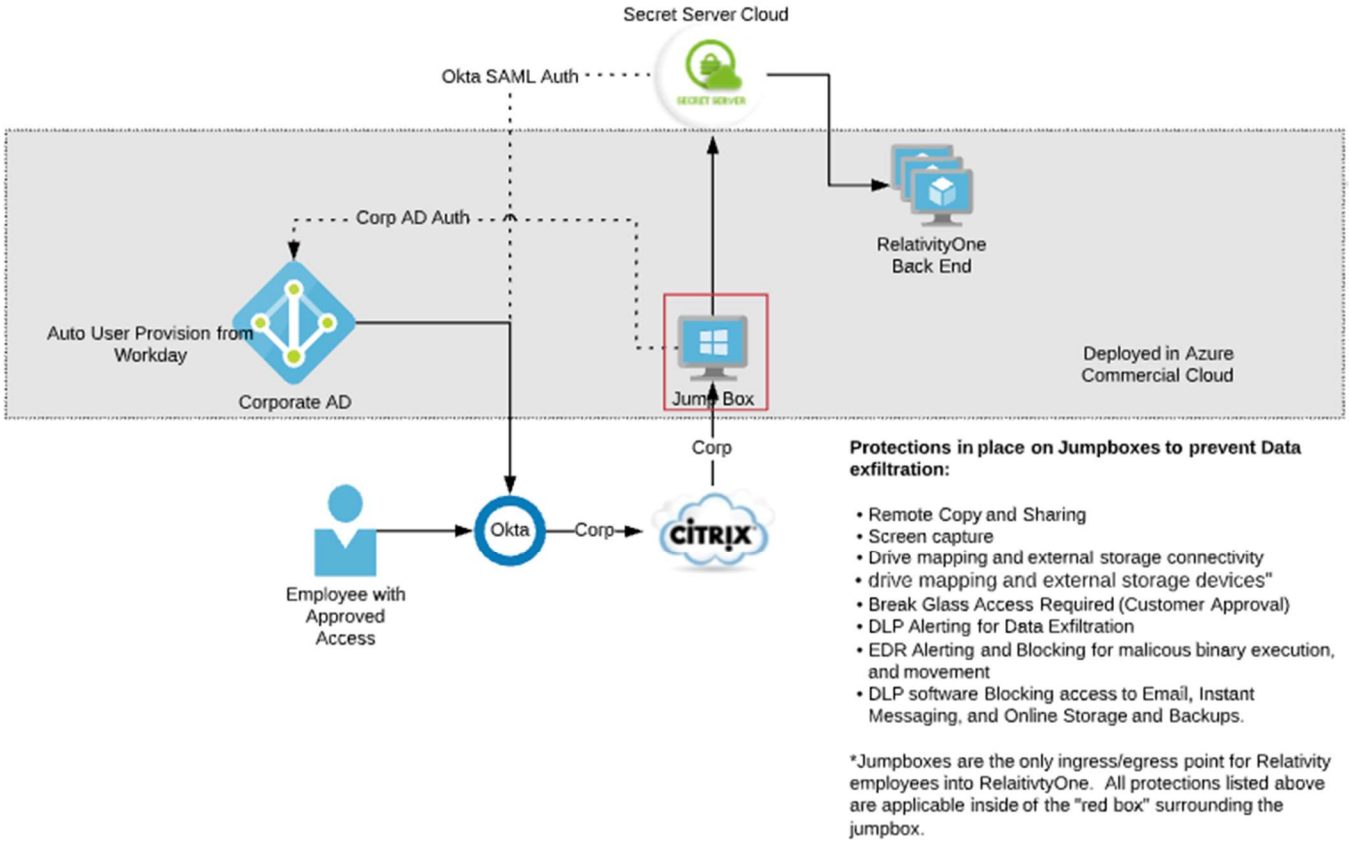
- Mit dieser Admin-Anwendung lassen sich verschiedene Sicherheitseinstellungen einsehen. Dazu zählen die Verwendung einer Zwei-Faktor-Authentifizierung durch die Benutzer, Benutzeraktivitäten, Zugriff auf Kunden-Lockboxes und Login-Maps von Benutzern.



Wie wird der Zugriff auf das Back-End gehandhabt?

Der Back-End-Zugriff auf IaaS-Dienste wird über Citrix Jumpboxen in einem privaten Netzwerk „Just in Time“ gewährt. Die Jumpboxen gelten nur für einen bestimmten Zeitraum, sind also kurzlebig. Benutzer sind in diesen Jumpboxen keine Administratoren. Sobald sich ein Benutzer in einer Jumpbox befindet, wird für ihn über eine PAM-Lösung (Privileged Access Management) ein Secret ausgescheckt. Der Benutzer kann diese Secrets grundsätzlich nicht sehen und nur SSMS-/RDP-/SSH-Sitzungen starten. Jedes Secret kann stets nur von einem Benutzer gleichzeitig ausgescheckt werden. Dabei wird ein eindeutiger Audit-Trail erzeugt.

Mit der UEBA-Überwachung ist sichergestellt, dass Muster zu verdächtigen Aktivitäten, die von der Norm abweichen, sowohl von menschlichen als auch von maschinellen Benutzern erkannt werden. Alle Backend-Zugriffe und UEBA-Warnungen werden von unserem 24x7 Security Operations Center überwacht.



Wie werden die Kennwörter verwaltet?

Die gesamte Kennwortverwaltung erfolgt über Okta und Thycotic Secret Server. Alle Mitarbeiter von Relativity nutzen die SSO-Lösung von Okta für sämtliche Anwendungen. Mit Okta Sync haben wir intern eine IAM-Anwendung entwickelt, die sicherstellt, dass Mitarbeiter von Relativity beim Zugriff auf das Front-End ausschließlich Okta verwenden. Password Provider, die Relativity-Mitarbeitern hinzugefügt werden, werden von Okta Sync entfernt.

Fazit

Das Identity and Access Management von Relativity beruht auf dem Grundsatz „Defense in Depth“. Dabei kommen mehrere Kontroll- und Überwachungsschichten zum Einsatz. Unsere Mitarbeiter greifen mit den geringstmöglichen Rechten und nur nach dem Just-in-Time-Prinzip zu, und zwar ausschließlich auf die Komponenten und Ressourcen, die ihrer Rolle zugeordnet sind. Wir protokollieren die Zugriffsaktivitäten und überwachen diese Aktivitäten mithilfe unserer UEBA-Automatisierung auf ungewöhnliche Zugriffsmuster. Wir legen niemals Kennwörter offen. Der Zugriff auf sämtliche Werkzeuge und Umgebungen erfolgt ausschließlich über eine MFA-Lösung.

Wir sind davon überzeugt, dass ein mehrschichtiger Ansatz, der Cyber- und Produktsicherheit miteinander verbindet, für den Schutz der Daten unverzichtbar ist. Relativity nutzt die eigenen robusten IAM-Praktiken, um die Daten seiner Kunden vor jedem zu schützen. Sogar vor uns selbst.