

Das britische Kommunikationsunternehmen Communitis setzt auf Forcepoint, um personenbezogene Endkundendaten seiner Auftraggeber aus der Finanz-, Versicherungs- und Versorgungsbranche sowie Behörden zu schützen

Die Marketing- und Kommunikationsagentur vertraut auf Forcepoint als Partner, um ihre digitale Transformation abzusichern und flexible Sicherheit zu bieten, damit die Produktivität ihres Kreativteams und die Kommunikation mit den Endkunden ihrer Auftraggeber gewährleistet ist.

Communitis stellt einigen der größten britischen Regierungsbehörden, Finanzdienstleistern und Versicherungsunternehmen Dienstleistungen in den Bereichen Kommunikation und Druckmanagement sowie Kreativ- und Point-of-Sale-Marketing für globale Marken bereit. Diese Aufgaben erfordern erstklassige Cyber-Sicherheitslösungen für Daten, Internet, E-Mail und Cloud. Communitis vertraut zum Schutz seiner Mitarbeiter und Daten seit vielen Jahren auf Forcepoint Web Security, Email Security und DLP. Kürzlich hat das Unternehmen beschlossen, seine Sicherheitsarchitektur mit Forcepoint Dynamic Data Protection für den risikogerechten Datenschutz und CASB für Transparenz bei der Cloud-Nutzung zu optimieren, um seine Sicherheitsstrategie besser auf die Anforderungen der digitalen Transformation abzustimmen.

KUNDENPROFIL:

Marketing und transaktionsorientierte Unternehmenskommunikation, Kreativagentur und Point-of-Sale-Bereitstellung.

BRANCHE:

Marketing und Kommunikation

HAUPTSITZ:

Vereinigtes Königreich

PRODUKTE:

- › Forcepoint Web Security
- › Forcepoint Email Security
- › Forcepoint DLP
- › Forcepoint DDP
- › Forcepoint CASB

Kontoauszüge, Versicherungsdokumente, Kreditkartenabrechnungen und Steuererklärungen sind ein fester Bestandteil unseres täglichen Lebens und für die Kommunikation von Finanzdienstleistern und Behörden mit ihren Kunden unerlässlich. Früher war es normal, dass diese Papierdokumente mit der täglichen Post kamen, aber heute kommunizieren selbst die traditionellsten Unternehmen mit ihren Kunden über den Kanal, der ihren Bedürfnissen am besten entspricht – ob in einem Briefumschlag in den Briefkasten oder digital per E-Mail oder Online-Portal. Die britische Marketing- und Kommunikationsagentur Communitis unterstützt führende britische Banken, Versicherungsgesellschaften und Versorgungsunternehmen wie British Gas dabei, diese One-to-One-Kommunikation effektiv und sicher zu gestalten.

Als Teil der US-amerikanischen OSG Group beschäftigt Communitis mit Hauptsitz in London rund 1500 Mitarbeiter, die Kunden in ganz Europa betreuen. Ein Teil des Unternehmens konzentriert sich auf die Konzeption, die Erstellung und den Versand dieser wichtigen Kundenkommunikation über verschiedene Kanäle. Der andere Teil erstellt und versendet One-to-Many-Markenkommunikation für globale Marken branchenübergreifend über diverse Kanäle in die ganze Welt. Für beide Teile des Unternehmens ist die effektivste Cyber-Sicherheit erforderlich, um sicherzustellen, dass sowohl die PII-Daten der Endkunden als auch die Materialien der Auftraggeber geschützt sind. Die beiden Teile unterscheiden sich allerdings erheblich, so dass flexible, risikobasierte Sicherheitsmaßnahmen unerlässlich sind.

„Die Arbeit, die wir für unsere Auftraggeber leisten, bedeutet, dass eine Menge personenbezogener Daten durch unser Netzwerk fließt. Wir müssen sicherstellen, dass die Informationen sicher sind, und beispielsweise proprietäres Marketingmaterial, das eine große Marke veröffentlichen will, schützen“, so Michelle Griffey, Chief Risk Officer bei Communitis. „Communitis hat in den letzten zehn Jahren unsere Expertise und das Vertrauen unserer Auftraggeber in die Sicherheit ihrer Daten gewährleisten. Das ist entscheidend in unserem Geschäft.“

Der Wechsel in die Cloud ist eine Gratwanderung, bietet aber Vorteile für Auftraggeber und Endkunden gleichermaßen

Vor kurzem hat Communitis damit begonnen, den Sprung in die digitale Transformation zu wagen, indem es einen Teil seiner Aktivitäten und Daten in die Cloud verlagert hat – allerdings nur, wenn dort die Sicherheit gewährleistet werden kann.

„Es ist ein schmaler Grat, weil wir vertragliche Vereinbarungen mit einem Auftraggeber haben, der vielleicht selbst in die Cloud geht. Der Auftraggeber ist aber vielleicht etwas zurückhaltender, einem Lieferanten dasselbe zu erlauben, weil es ein gewisses Risiko birgt, was die Kontrollmöglichkeiten betrifft“, erläutert Griffey. „Das bedeutet einfach, dass wir vorsichtig sein müssen und diese Entscheidung mit offenen Augen treffen müssen – sowohl im Hinblick auf die Anforderungen unserer Auftraggeber als auch auf unsere eigenen Bedürfnisse und unsere Sicherheit.“

Auch die Auftraggeber und ihre Endkunden treiben diesen Wandel voran. „Früher wurden Kontoauszüge oder Kreditkartenabrechnungen vielleicht in gedruckter Form versendet, aber viele dieser Unternehmen bevorzugen, dass ihre Kunden die Dokumente aus mehreren Gründen online einsehen“, so Griffey.

„Ein Partner, der die Kommunikation über den vom Endkunden gewünschten Kanal liefern kann, ist für unsere Auftraggeber von entscheidender Bedeutung. Wenn eine Person bei ihrer Versicherung anruft, um eine Vertragsänderung vorzunehmen, kann sie eine Bestätigung über den von ihr bevorzugten Kanal anfordern: als gedrucktes Dokument, E-Mail usw. Wenn die E-Mail aus irgendeinem Grund nicht versendet werden kann, werden wir benachrichtigt und veranlassen, dass ein gedrucktes Dokument per Postversand zugestellt wird. So wird sichergestellt, dass unsere Auftraggeber ihre regulatorischen Anforderungen erfüllen.“

Durch COVID-19 wurde dieser Schritt hin zu innovativeren Dienstleistungen bei Communitis beschleunigt. Auftraggeber sind möglicherweise nicht in der Lage, Materialien in verschiedenen Büros an unterschiedlichen Standorten zu produzieren, da immer mehr Mitarbeiter infolge des Lockdowns im Home-Office arbeiten. Aus diesem Grund bietet das Unternehmen seit kurzem einen Hybrid-Mail-Service an. Damit können alle Dokumente von mehreren Mitarbeitern unter einer Marke zusammengefasst, gebündelt und entweder an Druckzentren oder per E-Mail versendet werden, ohne dass ein Mitarbeiter sie aus einem Bürodrukker abholen muss.

CASB und Dynamic Data Protection bieten mehr Transparenz und Flexibilität, um beide Teile des Unternehmens zu unterstützen

Die Agentur verlässt sich bereits seit mehreren Jahren auf Forcepoint Web, Email und DLP, um sicheren Internet-Datenverkehr, sichere E-Mail-



Herausforderungen

Flexible Cyber-Sicherheit bereitstellen, um beide Teile des Unternehmens zu schützen.

Die Sicherheit sensibler personenbezogener Daten von Endkunden sicherstellen, um das Vertrauen der Kunden zu erhalten.

Die digitale Transformation und den Wechsel in die Cloud unterstützen.



Strategie

Forcepoint DDP und CASB zur bestehenden Sicherheitsinfrastruktur hinzufügen.



Ergebnisse

- › Unterstützung der Kreativität und Produktivität in einem Teil des Unternehmens und Schutz von sensiblen personenbezogenen Daten im anderen Teil.
- › Aufbau einer starken Partnerschaft zur Bewältigung von Herausforderungen in der Cyber-Sicherheit.

Kommunikation sowie Datentransparenz und -kontrolle zu gewährleisten, aber der Wechsel zu mehr Cloud-basierten Diensten führte zu einer neuen Ausrichtung der Sicherheitsstrategie von Communitis. Das Unternehmen entschied sich, seine Partnerschaft mit Forcepoint auszubauen und um den Forcepoint Cloud Access Security Broker (CASB) und Dynamic Data Protection (DDP) zu erweitern.

„Wir brauchen CASB, um strategisch auszuarbeiten, wie wir diese Cloud-gestützte zukünftige Welt schützen können, die uns alle betrifft“, erläutert Griffey. Und Forcepoint DDP bietet die Möglichkeit, eine flexiblere Sicherheitslage zu schaffen. Dies ist besonders hilfreich, wenn die beiden Teile des Unternehmens zwei unterschiedliche Konzepte für die Datensicherheit erfordern.

„Es gibt einen sehr differenzierten Sicherheitsbedarf“, so Griffey. „Das Kreativmaterial für eine neue Anzeige oder eine Marketingsendung ist für diesen Auftraggeber genauso wichtig wie die hunderttausend einzelnen personenbezogenen Datensätze, die einer Bank gehören. Aber diese Datensätze benötigen ein anderes Maß an Schutz, denn die Informationen, die man in einem Kontoauszug finden kann und die sich auf Ihr Gehalt, Ihre Hypothek, Ihre Ausgaben, Ihre Kontodaten und Ihren Wohnort beziehen, können in den falschen Händen wirklich sehr gefährlich sein. Daher muss der Schutz dieser Daten natürlich weiter oben auf der Liste stehen.“

„Ich finde DDP unglaublich spannend, weil wir damit anfangen können, unsere Sicherheit viel gezielter zu gestalten.“

MICHELLE GRIFFEY, CHIEF RISK OFFICER, COMMUNITIS

„Ich finde DDP unglaublich spannend, weil wir damit anfangen können, unsere Sicherheit viel gezielter zu gestalten, anstatt quasi eine Mauer zu errichten und niemandem etwas zu erlauben“, erklärt Griffey. „Wir können zwischen der One-to-One-Kommunikation, die ein höheres Maß an Sicherheit erfordert, und dem One-to-Many-Marketing unterscheiden,

bei dem vielleicht an etwas Kreativem gearbeitet und mehr Spielraum für die Zusammenarbeit benötigt wird. Und ich denke, dass wir damit unsere Teams in die Lage versetzen können, ihre Rolle in ihrem Job besser zu erfüllen.“

In der Cyber-Welt kämpfen wir alle auf demselben Schlachtfeld, wo Menschen das größte Risiko und die größte Chance sind

Forcepoint und Communitis haben eng zusammengearbeitet, um alle Schwierigkeiten und Herausforderungen zu überwinden. Als Communitis erwog, CASB hinzuzufügen und die Möglichkeiten von DDP zu prüfen, gab die Zusammenarbeit mit Forcepoint dem Unternehmen die Zuversicht, diese Lösungen ab sofort einzusetzen und gleichzeitig ihr Supportpaket zu erweitern.

„In den letzten Monaten konnten wir direkt mit Forcepoint zusammenzuarbeiten, um Probleme in unserer Umgebung auszubügeln und zu besprechen, wie wir kontinuierlich Verbesserungen vornehmen können“, so David Perkins, Information Assurance bei Communitis. „In den Teams für Informationssicherheit und IT glauben wir, dass wir die besten Lösungen für uns gefunden haben.“

„Ich sehe das als eine Partnerschaft an“, stellt Griffey fest. „Ich denke, wir können zusammenarbeiten, wenn wir eine besondere Herausforderung bei der Implementierung haben, für die wir eine Lösung finden müssen. Dann können wir diese Informationen wieder an Forcepoint zurückmelden, damit sie mit anderen Kunden geteilt werden können. Ich bin sicher: Wenn wir ein Problem haben, dann haben es wahrscheinlich auch andere Kunden. Letztendlich profitieren nicht nur wir, sondern auch andere Kunden von Forcepoint.“

„Daher ist es wichtig, dass wir als Partner mit Sicherheitsunternehmen wie Forcepoint zusammenarbeiten. Wir kämpfen schließlich alle den auf demselben Schlachtfeld, wenn es um die Cyber-Welt geht“, so Griffey. „Und der am Faktor Mensch orientierte Ansatz für die Cyber-Sicherheit von Forcepoint ist von entscheidender Bedeutung, denn letztendlich sind es die Menschen, die potenziell die größten Risiken darstellen – aber sie sind auch unsere größte Chance, uns zu schützen.“



„Letztendlich sind es die Menschen, die potenziell die größten Risiken darstellen – aber sie sind auch unsere größte Chance, uns zu schützen.“

MICHELLE GRIFFEY

CHIEF RISK OFFICER, COMMUNITIS