Unified Data Security Business to Customer

Managing security, risk and compliance

Forcepoint

Brochure

North American Business to Customer (B2C) organizations, especially in retail and healthcare, face stringent data privacy and security regulations. Customer PII (Personally Identifiable Information), patient PHI (Protected Health Information), payment card data and other sensitive information must be protected across myriad systems and cloud services. Recent high-profile breaches exposed tens of millions of customer records, causing lasting brand damage and regulatory penalties. CISOs and compliance officers are seeking end-to-end data security solutions rather than disparate tools to address these challenges.

Forcepoint Data Security Cloud platform encompassing DSPM, DDR, DLP and CASB enables B2C organizations including retail and healthcare enterprises to manage risk holistically and comply with key regulations (CCPA, GDPR, HIPAA, PCI DSS, ISO 27001, NIS2) with less complexity.

Modern Data Protection Challenges in B2C Organizations

B2C enterprises today operate in a complex threat and regulatory landscape. Compliance requirements like CCPA, GDPR, HIPAA, PCI DSS and ISO 27001 demand strict controls over customer data. Meeting these obligations is difficult when data lives everywhere (on-prem and cloud locations) and flows across SaaS applications, web traffic, email and endpoint channels. Data security compliance requires enforcement of controls across all those channels, plus strong visibility into data usage for audits. In practice, many organizations struggle with:

Limited visibility into data flows

It's challenging to know where sensitive data resides and how it moves. Understanding data flows is essential for protecting it and complying with policies like GDPR, HIPAA or PCI DSS. Without insight (data lineage), firms risk blind spots (e.g., unknown caches of personal data or unchecked sharing of patient records).

Inconsistent policy enforcement

Using siloed tools can lead to gaps where sensitive data can leak. Effective compliance means applying the same security policies everywhere personal data travels. Ad hoc solutions make it hard to prove consistent controls to regulators.

Resource-intensive compliance tasks

Responding to Data Subject Access Requests (DSARs) or demonstrating compliance often requires manually finding all personal data related to an individual across systems. This can be extremely time-consuming without unified search and classification.

Evolving threats and misuse

Advanced threats (malicious insiders, malware) and simple human errors both contribute to data breaches. Retailers fear credit card theft; healthcare providers fear PHI leaks. Security teams need to detect and stop misuse in real time, before massive breaches occur.

The stakes are high: Non-compliance can result in hefty fines (e.g., under GDPR/CCPA), and breaches undermine customer trust. A unified approach is needed to regain control.

Forcepoint Data Security Cloud Platform

The Forcepoint Data Security Cloud offers an integrated platform combining Data Security Posture Management (DSPM), Data Detection and Response (DDR), Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) capabilities.

Instead of a patchwork of point products, these solutions work together in one framework delivering data discovery across SaaS, cloud and on-premises environments, AI-powered risk assessment and remediation and cross-channel data protection. This unified approach aligns with what today's security leaders seek: holistic, end-to-end data security managed through one console.

Key components and capabilities include:

Data Visibility and Risk Posture (DSPM + DDR)

Forcepoint DSPM continuously discovers and classifies sensitive data across unstructured repositories (databases, SharePoint, cloud drives). It maps where data is stored, who has access and how it's shared, building an extensive inventory of personal data. This is crucial for compliance – you can't protect or report on data if you don't know it exists.

DDR's data lineage tracking shows how data flows through a specific cloud location. Understanding these flows is key to GDPR/CCPA readiness.

On top of this, **Forcepoint DDR** adds continuous monitoring of data activity and risk remediation. It uses AI-driven analytics to detect policy violations (for example, changing permissions to a file with sensitive PII to "public" access) and can alert security admins to remove permissions or to move or quarantine files.

DDR and DSPM together give security teams timely risk intelligence from a unified dashboard, highlighting high-risk data and suspicious events across the enterprise. CISOs gain a top-down view of their biggest data security priorities, in one place.

Notably, Forcepoint DSPM provides a Data Subject Access Request (DSAR) search tool to quickly locate all personal data related to an individual, simplifying compliance with GDPR/CCPA rights requests. Generating DSAR responses or "right to be forgotten" reports can thus be done in hours instead of weeks.

Consistent Policy Enforcement (DLP + CASB)

Forcepoint's DLP and CASB solutions ensure that once data is discovered and classified, it stays protected everywhere.

Forcepoint DLP applies centrally managed policies to data on endpoints, network, email, web and cloud channels. For example, a policy to prevent sharing of customer Social Security Numbers or credit card numbers can be enforced uniformly whether someone tries to email that data, copy it to a USB drive or upload it to a cloud app.

In the same platform, **Forcepoint CASB** governs and protects data in cloud services (like Microsoft 365, Salesforce or Box), controlling external sharing, downloads and risky cloud activities. Integration of Forcepoint CASB with Forcepoint DLP ensures security policies are unified across on-prem and cloud environments, eliminating gaps.

In practice, this means you can extend data security to web, cloud, email, endpoint and network from one platform, exactly the "everywhere" coverage regulators expect.

Forcepoint provides 1,700+ pre-built classifiers and policy templates aligned to common sensitive data types and regulations, jump- starting your ability to detect PII, PHI, PCI data, etc. These out-of-the-box policies map to local data privacy laws and standards, simplifying compliance configuration.

The platform's unified policy engine and console significantly reduce management overhead compared to maintaining separate endpoint and CASB DLP instances. This Data Security Everywhere approach allows administrators to enforce policies across all channels from a single interface, ensuring consistent enforcement and full visibility over sensitive data wherever it resides.

In short, DLP and CASB work hand-in-hand to stop unauthorized data sharing and exfiltration at every egress point, from a careless employee email to a malicious cloud upload.

Key Use Cases and Benefits for Compliance

Forcepoint Data Security Cloud delivers a unified data security platform bringing tangible benefits to customer-facing enterprises. Here are critical use cases for retail and healthcare organizations:

Protecting Customer PII and Patient PHI

Automatically discover and classify personal data (names, addresses, SSNs, health records) across the business. Enforce policies to restrict access to authorized personnel only, and block any attempt to send sensitive PII/PHI outside approved systems. This safeguards privacy and helps meet CCPA/GDPR obligations for protecting personal data. Forcepoint's data classification and labeling ensure adherence to regulations like GDPR, HIPAA and CCPA across all data environments. For a healthcare provider, the platform can recognize data such as medical record numbers or insurance IDs as PHI and prevent them from being emailed unencrypted, supporting HIPAA compliance on data confidentiality.

Preventing Credit Card Data Breaches (PCI DSS)

Identify and secure payment card information wherever it's stored in databases, POS systems or spreadsheets. Forcepoint DLP has built-in detectors for credit card numbers (following PCI DSS patterns) to flag any improper storage or transfer. CASB policies can prevent sharing files containing cardholder data to public and unauthorized external users.

These measures help retailers avoid breaches of payment data. (One retail breach exposed 40 million+ card numbers; unified DLP/CASB could help catch such bulk exfiltration or ensure data is encrypted as required by PCI DSS.) Consistent controls and monitoring make it easier to pass PCI audits and protect customers' financial info.

Stopping Unauthorized Data Sharing

In both retail and healthcare, employees may unwittingly upload sensitive data to personal cloud drives or share it via personal email or messaging. Forcepoint DLP and Forcepoint CASB monitor user actions and can block unauthorized uploads or emails containing sensitive data in real time. For example, if a retail employee tries to export a list of customers and upload it to a personal Dropbox, the unified policy can detect customer PII and stop the transfer. Similarly, if a healthcare worker tries to forward medical test results to a personal Gmail, the email DLP is able to stop the attempt. These controls prevent data leaks and demonstrate compliance with policies on data handling (supporting ISO 27001 control objectives around information transfer security).

Simplifying DSAR and Compliance Reporting

When a consumer invokes their privacy rights (CCPA or GDPR DSAR), the platform's DSAR search and analytics dramatically cut response time. Security teams can quickly query all data stores for that individual's data, using unified classification tags (e.g., find all files labeled with John Doe's customer ID). This ensures timely, comprehensive responses to access or deletion requests, avoiding regulatory fines for non-compliance. Additionally, Forcepoint provides centralized reporting that maps security events and data flows to regulatory requirements. Auditors can be given detailed logs of who accessed what data and when, evidence of policy enforcement actions and even pre-built compliance reports (e.g., showing no PHI left the network unencrypted over the past quarter). This unified visibility into data usage and incidents makes it easier to demonstrate compliance with HIPAA security rule or GDPR Article 30 record-keeping, for instance.

Compliance Alignment: CCPA, GDPR, HIPAA, PCI DSS, ISO 27001

Forcepoint's unified platform is designed with major regulations in mind, helping organizations meet specific requirements:

California Consumer Privacy Act (CCPA)

CCPA gives California consumers rights to know, delete and stop the sale of their personal information. Forcepoint helps catalog all customer PII (from contact info to purchase histories), so businesses know what data they have and where. Granular policies ensure that personal data is only used for permissible purposes (e.g., preventing unauthorized sharing of customer info with third parties, aiding compliance with "do not sell" requests). The DSAR search capability streamlines responding to consumer access or deletion requests, and comprehensive logging aids in demonstrating compliance during assessments.

General Data Protection Regulation (GDPR)

GDPR mandates data protection by design, breach notification within 72 hours and data subject rights (access, erasure, etc.) across all EU personal data. Forcepoint's platform addresses GDPR by providing enterprise-wide personal data discovery (including finding "dark data" that was previously unknown), mapping data flows even into cloud services and enforcing encryption or blocking of EU personal data transfers to unauthorized recipients. With unified DLP, organizations can apply GDPR- aligned rules uniformly (for instance, blocking export of EU customer data outside approved regions). In the event of a breach, the system's integrated incident timeline and analytics offer visibility into events and timelines involved in a data breach, helping teams investigate and report details as required by GDPR. Additionally, Forcepoint's ability to inventory who accessed personal data and when supports the "accountability" principle of GDPR.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA requires healthcare organizations to ensure the confidentiality and integrity of electronic PHI and to prevent unauthorized disclosures. Forcepoint provides out-of-the-box PHI detectors (for data like patient IDs, diagnostic codes, etc.) and templates for HIPAA compliance. This means healthcare providers can automatically enforce that PHI is not emailed externally or uploaded to non-approved cloud apps. The platform's data lineage and user activity monitoring create an audit trail of PHI access, supporting HIPAA's audit requirements. In practice, a unified security platform was used by one large healthcare network to protect 150,000 physicians across hundreds of locations and maintain compliance with HIPAA and state privacy laws. By unifying CASB and DLP controls, they ensured that even unmanaged devices accessing patient data were governed by the same HIPAA-aligned policies.

PCI DSS (Payment Card Industry Data Security Standard)

PCI DSS applies to any business handling credit/debit card information, with strict technical and process requirements to prevent card data theft. Forcepoint Data Security Cloud supports PCI compliance by discovering any stored cardholder data (PAN, CVV, etc.) in the environment and highlighting locations where it should be secured or removed. Pre-defined PCI DLP policies detect unencrypted payment data-in-motion (for example, blocking an attempt to send a spreadsheet containing card numbers over email). CASB controls can enforce that card data is only stored in encrypted cloud services or not at all. Through consistent enforcement, retailers can ensure that card data never leaves authorized systems, addressing PCI DSS requirements #3 (protect stored data) and #7/#8 (restrict access). If a potential card data leakage incident occurs, DDR can trigger an alert, reducing breach impact. This proactive stance is key, as retailers must not only pass annual PCI audits but avoid the catastrophic breaches that PCI DSS is designed to prevent.

ISO 27001

This international standard outlines best- practice information security management. While not focused on one data type, it requires organizations to assess risks and implement controls across all aspects of data security. Forcepoint's unified platform helps fulfill many ISO 27001 controls by providing comprehensive data asset inventory, classification, access control and monitoring. For instance, ISO 27001 Annex controls call for data classification (Forcepoint automates this at scale), prevention of data leakage (DLP) and security event logging (DDR alerts and reports). The unified nature of Forcepoint's solution means that an ISO 27001-aligned policy (say, "confidential data must be encrypted in transit") can be implemented uniformly across the IT environment. Organizations can more easily demonstrate an effective, centrally managed security program during ISO audits. Moreover, Forcepoint's own cloud infrastructure is ISO 27001 certified, reflecting its commitment to high security standards.

The Forcepoint Data Security Cloud Advantage
Complete Data Protection with Lower Complexity

Forcepoint's unified data security platform stands out as a fully integrated solution covering the entire customer data lifecycle from creation and storage, to usage, sharing and archival. This integration delivers several business benefits for retail and healthcare enterprises:

All-in-One Protection

Instead of juggling separate tools for DLP, cloud security, data classification, etc., security teams get one platform that does it all. This reduces training burden and ensures no security gaps between products. As Forcepoint CEO Ryan Windham noted, customers asked for deeper integrations; now CISOs have a unified interface to monitor data risks, with consolidated reporting and workflow for faster action.

Consistent Compliance Enforcement

Policies defined once in Forcepoint DLP translate into controls across endpoints, networks and cloud apps seamlessly. This unified policy enforcement minimizes human error and inconsistency. Companies can easily adopt Forcepoint's library of pre-defined policies mapped to regulations (GDPR, HIPAA, PCI, etc.), speeding up compliance readiness. With fewer products to fine-tune, maintaining compliance is simpler even as regulations evolve or expand (such as new state privacy laws).

Enhance Visibility and Analytics

By combining DSPM and DDR, Forcepoint gives unprecedented visibility into where data lives and how it's used. Security officers can identify risky data stores (e.g., an open SharePoint with thousands of PII files) and get alerted immediately. The platform's AI-driven risk analysis through the AI Mesh cuts through noise (reducing false positives) to surface the most critical issues. This risk-aware insight allows proactive mitigation before incidents escalate. It also aids in optimizing data governance, such as finding and deleting redundant or outdated data (ROT) to reduce exposure.

Reduced Complexity and Cost

A unified platform means fewer vendors and integrations to manage. This can lower overall costs (vs. buying separate DSPM, DLP and CASB solutions) and free up IT staff. Streamlined compliance workflows (like one- click report generation for auditors) also save time. Avoiding multiple point tools and leveraging Forcepoint's integrated approach reduces management overhead and ensures comprehensive control with less effort. In essence, organizations achieve strong data protection without the complexity traditionally associated with enterprise data security programs.

Real-World Proven

Forcepoint is a recognized leader in data security, with success stories in both retail and healthcare. Retailers have adopted Forcepoint DSPM and DLP to protect PCI data and maintain customer trust, while a healthcare giant unified CASB and DLP with Forcepoint to enable secure access for 150k physicians and ensure HIPAA compliance. These examples highlight that Forcepoint's platform is battle-tested in demanding, regulated environments.

For North American enterprises in retail, healthcare and other B2C sectors, Forcepoint Data Security Cloud provides the most complete data protection and compliance platform to safeguard customer data. By unifying DSPM, DDR, DLP and CASB, Forcepoint enables organizations to know their data, secure it everywhere and rapidly respond to risk, all from a single, integrated solution. This unified approach empowers CISOs and compliance officers to manage risk proactively while confidently meeting the requirements of CCPA, GDPR, HIPAA, PCI DSS, ISO 27001 and beyond. The result is a stronger security posture, simplified compliance and preserved customer trust. In an era of escalating threats and regulations, Forcepoint's data security platform offers a smarter path to protecting what matters most: the personal data at the heart of your business.

Get a Free Data Risk Assessment

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[FP-Brochure-Unified Data Security Business to Customer] 17Apr2025