Reimagining Security in the Privacy Era

Sandeep Agarwal

CTO, Security
Cisco India & South Asia

Contents

Executive Summary

In the current era of hyper-connectivity and rapid digital transformation, data has become the lifeblood of the global economy. For India, a nation poised to lead the digital frontier under the vision of "Viksit Bharat," this transformation is both an opportunity and a profound responsibility. The explosion of data generation, while fueling innovation and growth, has simultaneously elevated data privacy from a niche compliance requirement to a strategic boardroom imperative.

The introduction of the Digital Personal Data Protection (DPDP) Act of 2023, coupled with the detailed DPDP Rules of 2025, represents a landmark shift in India's regulatory landscape. These frameworks move beyond theoretical privacy rights to mandate operational excellence in how personal data is collected, processed, and protected. For modern enterprises, the core challenge is no longer just "protecting the perimeter"; it is about ensuring the integrity, confidentiality, and availability of personal data throughout its entire lifecycle.

This white paper, "Reimagining Security in the Privacy Era," asserts that security is not just an adjunct to privacy—it is its fundamental cornerstone. A robust privacy program is impossible without a resilient security architecture. As businesses embrace multi-cloud infrastructures and AI-driven workflows, the "complexity tax" often hinders effective data protection. This paper explores how a privacy-first approach, grounded in transparency and accountability, fosters deep customer trust. Furthermore, it outlines how Cisco's comprehensive security portfolio empowers organizations to navigate this evolving regulatory landscape with confidence, ensuring that compliance is not a barrier to innovation but a catalyst for cyber resilience.

Context

The DPDP Act of 2023

The Digital Personal Data Protection Act of 2023, established the foundational rights of "Data Principals" (individuals) and the obligations of "Data Fiduciaries" (entities that determine the purpose and means of data processing).

The Act broadly requires companies (termed as “Data Fiduciaries”) to:

- Provide a **clear notice** explaining the purpose and categories of data collected
- Obtain **explicit, informed, and unambiguous consent** for data processing
- Implement **data minimization** (collecting only necessary data)
- Enforce **storage limitation** (erasing data when the purpose is no longer served)
- Establish mechanisms to **uphold individual rights and redress grievances**
- Ensure robust **security measures** to prevent and detect breaches and promptly issue required notifications

The DPDP Rules of 2025

The operational reality of the DPDP mandates was crystallized with the 2025 Rules, which provide the granular "how-to" for compliance.

Key pillars of the 2025 Rules include:

Notice and Consent

Fiduciaries must provide clear, plain-language notices that are itemized and independent of other information, enabling informed consent.

Rights of the Data Principal

Enhanced mechanisms for individuals to withdraw consent, access their data, or seek grievance redressal with the ease of a single click.

Security Controls

Technical and organizational measures to ensure effective observance of security safeguards and prompt notification of personal data breaches.

Significant Data Fiduciary (SDF) Status

Organizations processing vast amounts of sensitive data or posing high risks to society are designated as SDFs, triggering additional obligations such as annual audits and Data Protection Impact Assessments (DPIA).

Scope and Impact

The DPDP Act represents a foundational reset for the Indian digital ecosystem. For decades, data protection in India was governed by a patchwork of appendices that treated privacy as a secondary consideration.

> The DPDP Act transitions the nation into a comprehensive, rights-based regime that places the "Data Principal"—the individual—at the center of the digital economy. Rather than a superficial legal update, this shift is a structural transformation that redefines the relationship between organizations and the data they steward.

The impact of the DPDP Act is defined by its sector-agnostic reach. Unlike previous frameworks that were often restricted to specific industries like banking or healthcare, the DPDP Act applies to any entity that processes digital personal data within the territory of India.

This encompasses a vast spectrum of the economy including, but not limited to:

Global Technology Giants

Financial Institutions

FMCG Companies

E-Commerce Platforms

Small and Medium Enterprises (SMEs)

Healthcare and Life Sciences

Furthermore, the Act's jurisdiction extends to the processing of personal data outside India if it is in connection with any activity related to offering goods or services to Data Principals within India.

This extraterritoriality ensures that the high standards of Indian data protection follow the data, regardless of where the server resides.

A critical nuance of the Act's scope is its focus on the "digital" nature of data.

The DPDP Act governs

- Personal data collected in digital form.
- Non-digital data that is subsequently digitized.

For organizations that have spent years undergoing digital transformation, this means that their entire digitized historical archive, as well as their real-time data streams, now fall under the scrutiny of the Act.

This creates an immediate need for processes that are impossible to execute at scale without a robust, automated security architecture.

Perhaps the most significant impact on the Indian boardroom is the Act's enforcement mechanism. Non-compliance is no longer a manageable operational risk; it has made data privacy a boardroom-level governance issue.

With financial penalties for failing to implement reasonable security safeguards or failing to notify a breach reaching up to ₹250 crore per instance, data privacy has officially ascended to a top-tier governance priority.

This staggering liability of non-compliance necessitates a shift.

A move away from:
"Check-the-box" auditing

Toward:
A culture of continuous resilience and trust

In this new era, privacy is not a hurdle to be cleared but a standard of excellence that must be engineered into the very fabric of an organization's digital infrastructure.

An Opportunity to Deliver Greater Resilience

For many organizations, the initial reaction to the DPDP Act of 2023 and the 2025 Rules has been to treat them as a legal compliance exercise—a task of updating privacy policies, refining consent forms, and "manually assessing" security safeguards to ensure they meet the minimum regulatory threshold.

However, viewing the DPDP Act through the narrow lens of a "privacy posture" is a strategic miscalculation. To truly meet the spirit of the Act, organizations must move beyond the superficiality of checkbox compliance and undertake a deeper transformation:

Evolving from traditional Cyber Security to true Cyber Resilience.

The DPDP Act is fundamentally about the fiduciary duty an organization owes to the Data Principal. This duty cannot be fulfilled by a static security posture that merely looks good on paper during an audit.

In a landscape of sophisticated and persistent threats operating at machine speed, the "spirit" of the mandate—protecting the rights and data of citizens—requires an infrastructure that is resilient by design.

While traditional cyber security focuses on building higher walls to keep threats out, cyber resilience focuses on:

The organization's ability to detect and absorb an attack

Minimize the impact on personal data

Recover with "agent speed" to ensure continued processing

Treating security as a cursory element of a privacy program often leads to the "complexity tax"—a fragmented architecture of disconnected tools that creates blind spots precisely where personal data is most vulnerable.

A resilient approach, by contrast, adopts a platform-centric mindset. It recognizes that "Reasonable Security Safeguards" are not a static destination but a continuous operational state.

It requires moving from siloed visibility to a unified intelligence layer where identity, network, and endpoint telemetry converge to protect the Data Principal's information across its entire lifecycle.

Ultimately, the DPDP Act offers Indian enterprises a choice: maintain a reactive security posture that manages legal risk or build a resilient digital foundation that inspires radical customer trust. By focusing on resilience—the ability to prevent, detect, investigate, and remediate at scale—organizations do more than just avoid penalties; they honor their role as trusted stewards in India's digital future. In the privacy era, resilience is the only true measure of compliance.

The Cisco Approach

We believe that regulations like the DPDP Act are not merely compliance hurdles but are the ultimate catalysts for meaningful digital transformation. For Indian enterprises, this Act serves as a strategic inflection point—a chance to shed the "complexity tax" of fragmented, siloed security tools and transition toward a unified cyber resilience strategy. Achieving the spirit of the Act—radical transparency and uncompromising data protection—requires a technology partner who understands that privacy is an engineering outcome, not just a legal one.

Partnering with Cisco means choosing an architecture that is resilient by design. We recognize that while a significant portion of the DPDP Rules focuses on the administrative front-end of privacy, such as:

Seeking clear, revocable consent

Managing Data Principal rights

These functions are only as reliable as the underlying security infrastructure. A breach of "reasonable security safeguards" renders even the most robust consent framework moot.

In this paper, we explore the specific ways Cisco helps transform an organization's security posture from reactive to proactive. Our analysis focuses on the twin pillars of the 2025 Rules:

Rule 6

Mandates the adoption of "reasonable security safeguards."

Rule 7

Governs the rigorous management and notification of personal data breaches.

By providing a unified platform that integrates identity intelligence, cloud-native visibility, and automated response, Cisco empowers organizations to address evolving privacy requirements while simultaneously simplifying the operation of their security stack. We achieve this by fusing machine-scale defense into the infrastructure, such that segmentation, enforcement, and visibility become an in-built part of your fabric. Through this partnership, companies can rethink their privacy posture not as a separate workstream, but as a fundamental byproduct of a modern, resilient digital enterprise.

Reasonable Security Safeguards

Rule 6 of the DPDP Act of 2025 mandates that every Data Fiduciary must implement "reasonable security safeguards" to prevent personal data breaches. These safeguards must cover both the Fiduciary's own processing and any processing done on their behalf by a Data Processor.

Cisco provides a unified architecture to address these requirements across five critical domains:

Data Security: Encryption and Obfuscation

Rule 6(1)(a) specifically identifies encryption, obfuscation, masking, and tokenization as appropriate data security measures.

Under the DPDP Rules, data security is not a static requirement but a continuous obligation to protect personal data from unauthorized access or alteration. To meet this mandate effectively, organizations must view data security holistically across its entire lifecycle:

In-transit

At-rest

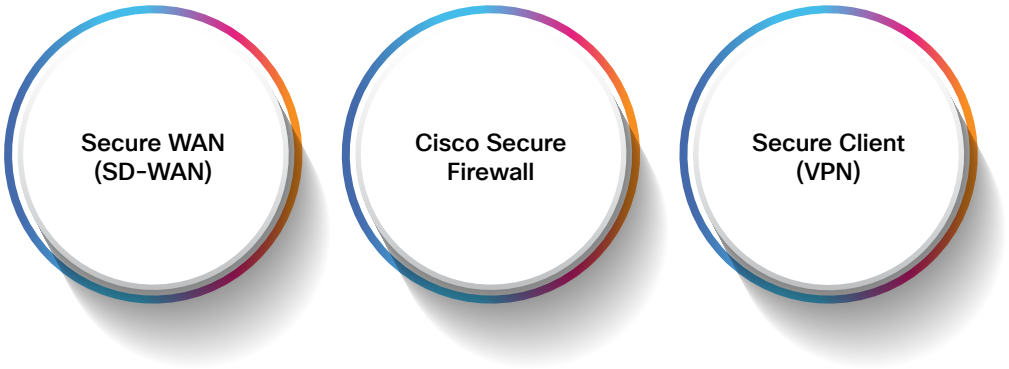
In-use

While many compliance programs focus heavily on protecting data stored in databases (at-rest), a truly resilient privacy framework recognizes that personal data is most vulnerable when it is in motion or being processed. Securing one state while neglecting others creates a "broken link" in the chain of custody, potentially leading to the very breaches the Act seeks to prevent.

When addressing data in-transit, the traditional reliance on Transport Layer Security (TLS) is no longer sufficient to guarantee privacy. While TLS encrypts the payload, it often leaves metadata—such as DNS queries—exposed in plain text. Secure DNS is a critical, yet frequently overlooked, component as it prevents adversaries from intercepting the initial "handshake" of a digital connection to map out user activity or redirect traffic .breaches the Act seeks to prevent.

Furthermore, the rapid advancement of quantum computing has introduced a temporal dimension to data security. Encrypted data intercepted today can be stored by adversaries with the intent of decrypting it once cryptographically relevant quantum computers become available. This "Harvest Now, Decrypt Later" (HNDL) strategy means that long-lived personal data, such as national IDs or health records, requires protection that is resilient against both classical and quantum threats today.

Cisco has been at the forefront of powering and securing global internet communications for over four decades, providing the foundational infrastructure that enables secure data transit at a planetary scale. Our heritage in building the world's most resilient networks is evident through:



This ensures that personal data is protected by the highest standards of industrial-grade encryption from the moment it leaves an endpoint. By integrating security directly into the networking fabric, Cisco enables organizations to enforce consistent encryption policies across hybrid-cloud environments, ensuring that the mandates of the DPDP Act are met without introducing operational friction.

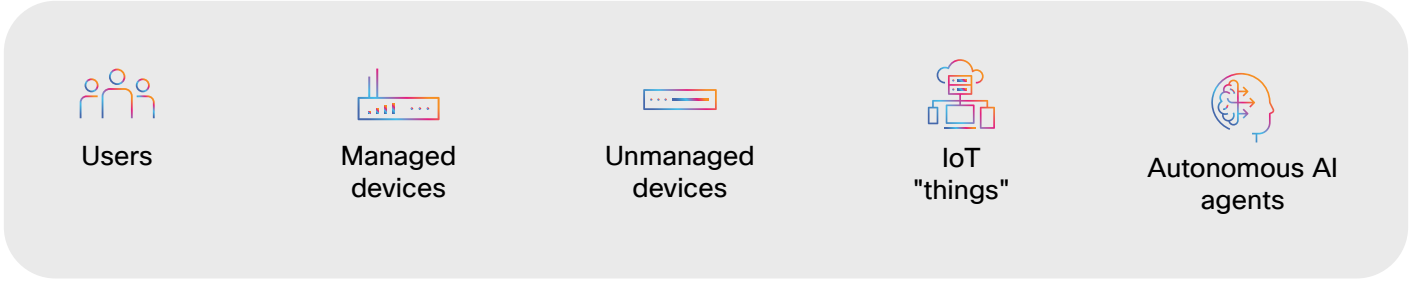
Beyond traditional transit security, Cisco is a pioneer in addressing the next-generation of privacy risks via:

Cisco Umbrella provides a first line of defense at the DNS layer, ensuring that the "starting point" of every digital interaction is encrypted and shielded from surveillance. Simultaneously, by integrating PQC into our networking and security hardware, Cisco ensures that data remains protected against the looming threat of quantum decryption. This multi-layered approach ensures that even if data in flight is accessed, the underlying personal data remains obfuscated and mathematically inaccessible to unauthorized parties.

Access Control: Zero Trust and Identity

Rule 6(1)(b) requires appropriate measures to control access to the computer resources used by such Data Fiduciary or such a Data Processor. Effective compliance requires fine-grained controls over who can access systems and applications that house personal data.

In the contemporary digital enterprise, the concept of a "perimeter" has undergone a fundamental transformation. Historically, access control was synonymous with the network edge—a binary gatekeeper that determined who was "inside" and who was "outside." However, under the DPDP framework, controlling access to "computer resources" requires a significantly more nuanced, multi-layered approach. Today's perimeter is no longer a static line in the sand; it is a dynamic, identity-centric boundary that must govern a complex ecosystem of:



This modern access challenge is compounded by the shift toward multi-hybrid cloud environments. As personal data is distributed across private data centers, public cloud instances, and SaaS platforms, the risk surface expands exponentially. "Appropriate measures" for access control must therefore transcend simple phishing-resistant authentication or static granular authorization. A resilient strategy requires a continuous evaluation of context—assessing the security posture of the device, the behavior of the user or agent, and the sensitivity of the resource being accessed in real time. Access is no longer a one-time event at login; it is a persistent state of verified trust that must be maintained throughout the entire session.

Cisco addresses this multi-dimensional challenge through the synergistic integration of:

Cisco Duo acts as the first line of defense, providing phishing-resistant Multi-Factor Authentication (MFA) and passwordless capabilities that ensure only verified users and healthy devices can initiate a request. Meanwhile, Cisco ISE serves as the critical policy engine for the internal landscape, providing deep visibility and control over the "things" and devices connecting to the campus or branch network. ISE ensures that IoT devices or AI-driven local agents are restricted to specific network segments, preventing them from ever reaching sensitive personal data repositories unless explicitly authorized.

When these technologies are orchestrated through Cisco Secure Access, our Universal ZTNA (Zero Trust Network Access) solution, the organization achieves a "unified policy" experience. Whether a user is connecting from a coffee shop in Colaba, Mumbai, or a secure office in Bandra Kurla Complex, Cisco Secure Access applies a consistent security posture, seamlessly routing them to private applications or global SaaS platforms while silently enforcing the granular access controls mandated by the DPDP Rules.

By combining:

Duo's identity certainty + **ISE's hardware-level visibility** + **Secure Access's cloud-scale enforcement**

Cisco enables Data Fiduciaries to move beyond fragmented security tools toward a single, cohesive architecture that secures the modern-day perimeter against unauthorized access at every layer.

Visibility: Logging and Monitoring

Rule 6(1)(c) mandates "visibility of access to personal data" through logs and monitoring to detect and investigate unauthorized access. Crucially, Rule 6(1)(e) requires these logs to be retained for at least one year.

To achieve the "visibility of access" required by Rule 6(1)(c), modern organizations must look beyond traditional, siloed logging practices. In a fragmented digital landscape where personal data resides across multi-cloud environments, SaaS applications, and on-premises databases, visibility is often obscured by "identity sprawl." To overcome this, organizations require a sophisticated layer of Identity Intelligence. This approach involves aggregating authentication and access insights from across the entire identity stack, regardless of the vendor. By doing so, security teams can move from simply collecting data to building a continuous, contextual understanding of user behavior and posture risks.

This identity-centric insight must be anchored by a comprehensive log analytics platform that serves as the organization's "regulatory memory." While Rule 6(1)(e) mandates a minimum of one-year log retention, the operational objective is to transform that data into a coherent "risk story." A robust analytics engine does not merely store logs; it correlates long-term identity data with telemetry from:

- Firewalls
- Endpoints
- Cloud workloads

This correlation is essential for detecting sophisticated threats—such as lateral movement or insider misuse—that often unfold over weeks or months. By bridging the gap between identity insights and historical log data, organizations can ensure that every access event is not only recorded but also scrutinized for its impact on the security of personal data.

Cisco facilitates this high-level visibility by integrating:

Cisco Identity Intelligence serves as a multi-sourced, vendor-agnostic solution that surfaces critical identity anomalies and posture gaps, while Splunk serves as the ultimate visibility engine, capable of ingesting and analyzing logs across the entire hybrid-cloud estate. With Splunk, organizations can automate 1-year log retention and implement real-time monitoring for suspicious access patterns directly satisfying the DPDP Act's 365-day retention mandate.

Together, they create a Unified Identity Timeline within the Splunk environment by highlighting event volumes, failures and risky behaviors across multi-vendor identity stacks.

For instance, through integrations like the Cisco Duo Suspicious Activity analytics story in Splunk, security teams can automatically identify insecure policy settings or risky administrator actions. This powerful combination transforms compliance from a reactive auditing exercise into a proactive, context-rich defense, enabling faster investigation and prioritized response to risks that could lead to a personal data breach.

Resilience:
Detection, Investigation and Recovery

> Rules 6(1)(d) and 6(1)(e) emphasize "continued processing" in the event of a compromise, necessitating robust threat detection, incident response, and systems recovery, including backups.

In a privacy-focused regulatory regime, the definition of security resilience shifts from safeguarding corporate confidential information to fulfilling a solemn "fiduciary" duty to protect the personal information of citizens. When an organization acts as a Data Fiduciary, the data it processes is a proxy for the digital identities, financial safety, and personal rights of Data Principals. In this context, a security breach is not merely an operational failure; it is a violation of trust that can cause immediate and lasting damage to innocent individuals. Consequently, any delay in the detection and investigation of unauthorized access directly compounds the risk of harm, making rapid response a primary requirement of the DPDP framework.

To meet the DPDP Act's mandates for "continued processing" and "remediation to prevent recurrence," organizations must transition away from fragmented security tools that rely on manual correlation. A cloud-native, managed approach is required—one that natively stitches together disparate signals from email, endpoints, networks, cloud environments, and identity systems out of the box.

This integrated visibility is especially critical for organizations that do not have the luxury of investing in massive, complex Security Operations Center (SOC) setups. For larger enterprises that require more granular control, these high-fidelity signals must be layered with the below, within a next-generation SIEM:

Application-level telemetry

Workload data

The ultimate objective is "agent speed"—leveraging automation and AI to investigate and respond the moment a detection is flagged, ensuring that the exposure of personal data is contained instantly.

Cisco XDR (Extended Detection and Response) is purpose-built to deliver this level of resilience by simplifying the detection of unauthorized access across the entire attack surface.

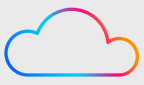
It provides high-fidelity detection across:


Identity


Network

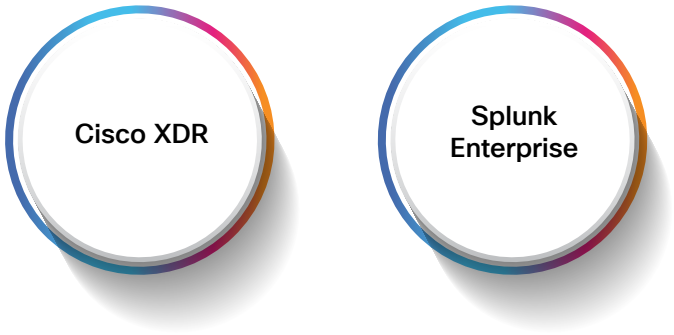

Email


Endpoint


Cloud

By correlating signals from multiple sources, including Cisco-native and third-party, Cisco XDR provides high-fidelity alerts that focus on genuine risks rather than background noise. This allows security teams to respond to potential breaches by identifying and containing them in minutes before they escalate. When a threat is detected, Cisco XDR enables immediate remediation actions, such as isolating a compromised host or automatically suspending a user's credentials, directly addressing the DPDP Act's requirement for ensuring safety measures are enacted without delay and preventing recurrence.

For organizations seeking a comprehensive "risk story" across their entire landscape, the following integration provides an unparalleled forensic and response engine:



While Cisco XDR provides pre-correlated, high-speed incident detection, Splunk serves as the next-generation SIEM that captures the "long tail" of data, including complex application and workload telemetry. Together, they allow organizations to conduct deep, automated investigations that satisfy the Data Protection Board's requirements for root-cause analysis. Through Splunk's orchestration capabilities, security teams can respond with "agent speed," automating the transition from detection to recovery. This ensures that the organization maintains the "continued processing" required by the Rules, even in the face of a sophisticated compromise.

Lastly, the DPDP Rules require an organization to maintain "continued processing" even when primary data stores are compromised through:

- Accidental destruction
- Malicious encryption

Under the DPDP Act's fiduciary model, a loss of access to personal data is a direct breach of availability, making robust, immutable backups a regulatory necessity rather than just an IT best practice. Adopting these recovery mechanisms ensures that data remains accessible and protected, thereby minimizing the impact of a compromise on the Data Principal.

To operationalize this level of resilience, Cisco XDR integrates seamlessly with Cohesity, combining advanced threat detection with modern data protection. Integrating Cohesity DataProtect with Cisco XDR allows SOC and IT teams to automatically take a snapshot of business-critical data as often as needed, early in the incident response process. Later, when Cisco XDR identifies a ransomware event or data destruction attempt, the joint solution facilitates "Clean Room" recovery, allowing security teams to pinpoint the last known uncorrupted snapshot and restore personal data into a verified safe environment.

Governance and Assurance

Finally, Rules 6(1)(f) and 6(1)(g) require "appropriate technical and organizational measures" to ensure effective observance of security safeguards—whether directly by the Data Fiduciary or by a Data Processor acting on their behalf. While this mandate encompasses a broad spectrum of a security program—from policy frameworks to employee training—there are certain non-negotiable building blocks that form the bedrock of a resilient organization. These foundations ensure that security is not a "best effort" compliance activity but a continuous, enforceable state that aligns with the fiduciary duty to protect personal data.

The first of these foundational blocks is **Universal Zero-Trust Access**. In an era where data is accessed from anywhere and by anything, the concept of a "trusted network" is obsolete. A successful program must extend zero-trust principles beyond just human users to include devices, IoT "things" and now AI agents. By enforcing a "never trust, always verify" posture across all entities, organizations ensure that access to systems housing personal data is granted only after continuous verification of identity, device health, and context. This universal approach eliminates the security gaps often found at the intersection of different access methods.

Furthermore, resilience requires the ability to contain a breach through a **Hybrid Mesh Firewall** architecture. Micro-segmentation ensures that communication between applications, hosts, and networks is tightly controlled and segmented based on intent. By implementing universal micro-segmentation, organizations create "digital compartments" that prevent unauthorized lateral movement—a common tactic used to escalate access to sensitive data repositories and exfiltrate large volumes of personal data. However, these internal controls must be matched by a hardened "front door." Because most breaches originate through compromised credentials, malicious emails, or infected devices, a successful governance framework must prioritize the integration of identity, endpoint, and email security. Hardening these primary entry points is essential for the effective observance of the Act's security mandates.

Cisco enables this comprehensive governance through the **Cisco User Protection Suite**, which integrates **Cisco Duo, Secure Email**, and **Secure Endpoint**. This suite ensures that the most common attack vectors—phishing and malware—are neutralized before they can reach personal data. Cisco Duo provides phishing-resistant MFA, while Secure Email (Email Threat Defense) and Secure Endpoint work in tandem to detect and block sophisticated threats at the user level.

To complete the architecture, **Cisco Secure Access, Cisco ISE (Identity Services Engine), Cisco Secure Firewall** and **Cisco Secure Workload** work in unison to provide a seamless security fabric. **Cisco Secure Access** provides the Universal ZTNA (Zero Trust Network Access) required to secure user and device connections to any application, regardless of location. This is seamlessly complemented by Cisco ISE, which extends this zero-trust rigor to the "things" on the network, providing the deep visibility and profiling necessary to ensure that IoT devices or hardware agents cannot become an unprotected entry point for a data breach.

To enforce the "spirit" of organizational governance, **Cisco Secure Firewall**, and **Cisco Secure Workload** operate together with other Cisco offerings to provide a Hybrid Mesh Firewall capability. This allows organizations to define a single, consistent segmentation policy that follows the data across on-premises data centers and public cloud environments. By automating micro-segmentation, Cisco removes the "complexity tax" often associated with granular controls, making it simple to operate a landscape where bad actors are prevented from moving laterally.

This integrated approach ensures that the technical and organizational measures required by the DPDP Rules are not just administrative policies but are automatically enforced across the entire enterprise, from the email inbox to the cloud-native workload.

Personal Data Breaches

The DPDP Act of 2023 and the accompanying DPDP Rules introduce a strict, multi-layered notification framework following any personal data breach:

Intimation to Data Principals:

Upon becoming aware of a breach, a Data Fiduciary must notify each affected individual "without delay" in a concise, clear, and plain manner. This notification must include a description of the breach (its nature, extent, and timing), the likely consequences to the individual, the mitigation measures implemented by the Data Fiduciary, recommended safety actions the individual can take to protect their interests, and business contact information for handling queries.

Intimation to the Data Protection Board (DPB):

Parallel to individual notifications, the Fiduciary must alert the Board "without delay" with an initial description of the incident, its location, and its probable impact. Within 72 hours of discovery, a comprehensive follow-up report must be submitted, detailing the broad facts and root causes leading to the breach, updated scope details, risk-mitigation measures, any findings regarding the threat actor, a summary of notifications sent to users, and the specific remedial measures taken to permanently prevent recurrence.

The Breach Notification Blueprint

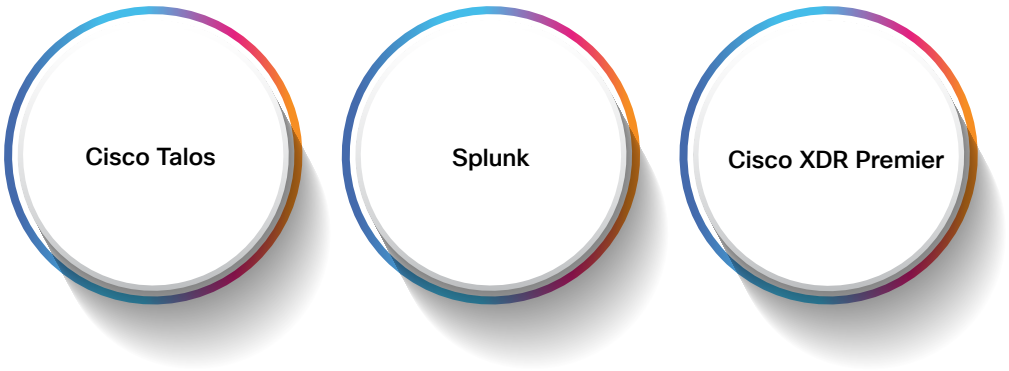
Under the DPDP framework, a personal data breach changes an organization's operational reality instantly. The mandate to notify every affected individual and the Board "without delay," followed by a detailed report within 72 hours containing a root-cause analysis and specific remedial measures, turns incident response (IR) into a high-pressure compliance crucible. Managing these strict, compressed time windows demands a dedicated, expert-led framework designed to handle the velocity of modern cyber attacks while preserving forensic integrity for regulatory reporting.

To systematically survive a breach scenario, an enterprise must anchor its defense across three non-negotiable phases: Planning and Preparedness (Before), Containment and Response (During), and Investigation and Improvement (After).

In the planning phase, an organization must proactively evaluate its capability against regulatory expectations, institutionalize those responses through regular goal-oriented simulations, and eliminate systemic blind spots caused by infrastructure shifts. When an incident inevitably occurs, the immediate operational objective shifts to rapid triaging—identifying the root cause, isolating the impact radius, and shrinking the Mean Time to Respond (MTTR) through orchestrated actions to prevent widespread data exposure and limit downstream individual damages.

Finally, the post-incident phase must shift toward comprehensive investigation and long-term remediation to satisfy the Board's strict mandates. This requires human-led threat hunting to uncover hidden adversaries that may be nesting deep within the network, coupled with immediate access to digital forensics experts who can reconstruct the attack timeline. Furthermore, true organizational resilience depends on continuously elevating the skills of internal teams within a safe training environment, ensuring that the root-cause lessons learned from a compromise are permanently engineered back into the system to prevent future recurrence.

Cisco addresses these intense temporal mandates through the following unified combination, providing continuous protection across all three phases of a breach:



Phase 1: Planning and Preparedness (Before)

To build a breach-ready posture, **Talos Incident Response Proactive Services** evaluate existing IR plans, roles, responsibilities, and tools to assess an organization's structural readiness to handle complex incidents. This phase requires creating tailored **IR Playbooks** with step-by-step processes to directly support the triage and response workflows defined in your broader IR Plan.

This foundation is further battle-tested at an institutional level using **Table-Top and Purple Team exercises**, which provide goal-oriented security assessments to test your team’s response to real-world scenarios. While a Table-Top exercise does so in a controlled, collaborative setting to identify organizational strengths, gaps, and improvement opportunities, Purple Team exercises actively assess detection and response capabilities against live adversary tradecraft. During these simulations, Talos’ offensive (Red) team directly challenges your internal defensive (Blue) team, exposing hidden vulnerabilities and allowing you to harden areas of opportunity before attackers can exploit them.

Phase 2: Containment and Response (During)

When an alert is triggered, **Cisco XDR Premier** delivers turnkey SOC operations powered by **Managed XDR (MXDR)** services. Managed by an elite team of security experts, this service allows organizations to pinpoint the root cause, determine the impact radius, and prioritize critical incidents quickly and accurately. To dramatically reduce the Mean Time to Respond (MTTR), **Splunk SOAR** orchestrates containment workflows with built-in automated actions and guided playbooks executed through its extensive catalog of ecosystem connectors.

This live containment effort is reinforced by **Talos Incident Response Reactive Services**, providing immediate, emergency security mitigation to minimize operational downtime and accelerate system recovery. This service grants anytime, on-demand access to incident coordination, command-and-control support, and expert remediation guidance for any cyber incident—all continuously fueled by world-class Talos threat intelligence.

Phase 3: Investigation and Improvement (After)

To satisfy the DPDP Act's strict 72-hour detailed reporting requirements, **Talos Threat Hunting** combines expert human analysis and global telemetry to discover stealthy threats hiding in plain sight or deep within your network infrastructure. This service performs a holistic environmental review to identify signs of active or historical adversary activity, leveraging Talos' deep repository of actor tactics, techniques, and procedures (TTPs) and indicators of compromise (IoCs). If a breach requires highly specialized deep dives, the **Talos IR Retainer** grants on-demand access to elite responders within hours to begin comprehensive triage, evidence preservation, and forensic investigation.

Finally, to fulfill the regulatory mandate of continuously improving and preventing recurrence, the **Talos Cyber Range** augments internal security teams' skills through hands-on training in a safe, isolated environment. By immersing defenders in practical scenarios grounded in real-world cyber incidents, Cisco ensures your organization actively weaponizes post-breach insights to permanently harden its security posture.

By unifying these advanced capabilities into a single, cohesive framework, Cisco removes the friction of incident management, transforming a high-pressure compliance mandate into a repeatable, resilient strategy.

Conclusion

India’s ambition of becoming a "Viksit Bharat" (Developed India) by 2047 is inextricably linked to the success of its digital economy.

A vibrant, safe digital transformation is only possible when citizens trust that their personal information is treated with the utmost care.

The DPDP Act of 2023 and the 2025 Rules are not merely regulatory hurdles; they are a landmark framework that will define the standards of corporate behavior in the digital age.

For Indian organizations, this is a pivotal moment to transition from reactive security to proactive "Cyber Resilience."

By adopting a customer-first approach to data governance and treating security as the fundamental bedrock of their privacy programs, businesses can turn compliance into a competitive advantage.

At Cisco, we are committed to being the partner that enables this transformation—providing the "Security Simplicity" and the advanced technologies required to reimagine security in the privacy era.