# Preserving Customer Privacy with Zero Trust

Ensuring privacy is more than just complying with regulations, it is an essential element for demonstrating the transparency and accountability that fuels brand trust. A zero trust approach can help organizations protect customer privacy with access controls that are based on least privilege, giving access to only those with a legitimate need and for the agreed upon purpose. By assuming compromise is inevitable, your organization is prepared to quickly detect, investigate, and respond to potential breaches of customer data. This can help limit damage and improve resiliency.

"80 percent of breached organizations stated that customer PII was compromised during the breach."

- Cost of a Data Breach [1]
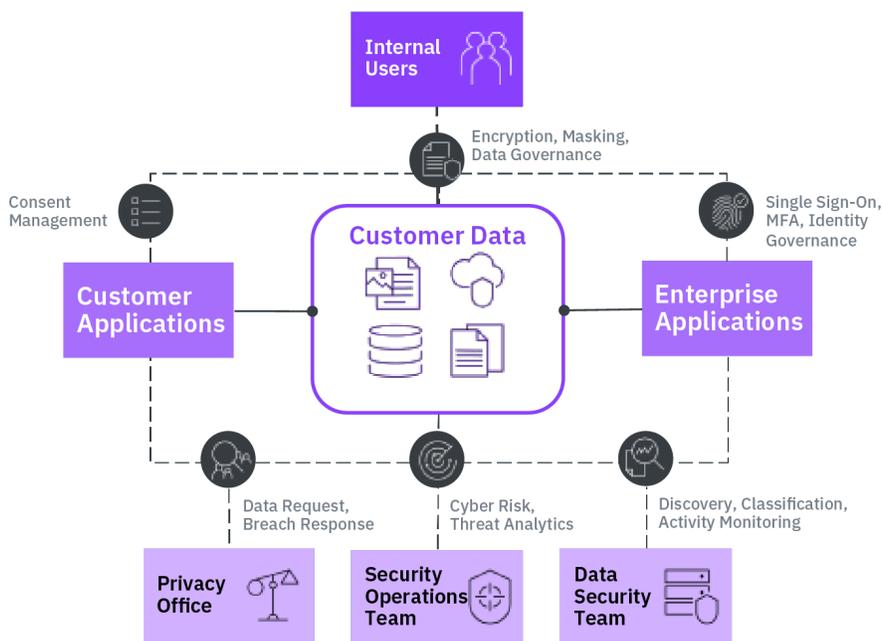
Protecting personal data is essential for building brand trust

[1] Ponemon Institute, Cost of a Data Breach Report 2020, sponsored by IBM Security, July 2020

IBM

IBM Security Solution Blueprint

To put zero trust into action to protect customer privacy you'll want to consider each of the critical capabilities indicated (●) for the specific security challenge you want to address.

Map privacy challenges to zero trust capabilities:

	Understanding your personal data landscape	Enabling secure data usage and sharing	Automating and streamlining response
Get Insights			
Cyber Risk Management	●	○	●
Data Discovery & Classification	●	●	●
Data Lineage	●	●	●
Enforce Protection			
Access Management	○	●	○
Activity Monitoring	●	●	●
Encryption & Data Masking	○	●	○
Identity & Data Governance	●	●	●
Multi-factor Authentication	○	●	○
Threat Analytics	○	●	●
Detect & Respond			
Breach Response for Privacy	○	○	●
Consent Management	●	●	●
Data Subject Rights Fulfillment	○	○	●

Key metrics for success:

1. How quickly can you respond to and address customer requests for what personal data you keep and how you use or intend to use it?

2. What percentage of personal data have you discovered and classified? And how frequently are you conducting this assessment? (*i.e. Do you know where your data resides, who it belongs to, who has access, and how it's being used?)*

3. What percentage of security incidents required a customer breach notification?

Need assistance applying zero trust to your privacy initiatives?

Contact us to schedule a no-cost Framing and Discovery Workshop. With this garage-style workshop, our experts will work with you to:

- Map out your business goals and define a zero trust strategy tailored to your specific needs

- Understand the landscape and capabilities offered by your current investments and identify gaps

- Clarify and prioritize zero trust projects and initiatives to ensure demonstrable success.

Visit: https://www.ibm.com/garage and select *schedule a consult* to book your workshop. You'll walk away with a prioritized list of zero trust initiatives, a detailed journey map, actionable next steps, and all exercises organized in a PDF outcomes deck.

---

[1] Ponemon Institute, Cost of a Data Breach Report 2020, sponsored by IBM Security, July 2020

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

For more information

To learn more about IBM's zero trust approach, please contact your IBM representative or IBM Business Partner, or visit the following website:
http://ibm.com/security/zero-trust