

SELECTING THE RIGHT ENCRYPTION: WHAT RISKS DO YOU NEED TO ADDRESS?

➔ As tempting as it may be to simply use a security technology that has worked in one area as the solution for another, the right approach is to carefully consider **what risks you are trying to address**, and to choose the technologies that are most appropriate to address them. Here is a glimpse of [Aberdeen's insights](#) on two specific examples: “data at rest” in *back-end systems*, and “data in use” at the *endpoints*.

Risks (Actions)	Description	% of Actual Incidents (Servers)	% of Actual Incidents (Endpoints)	Encryption Aligned with ≥80% of Actual Incidents
<input type="checkbox"/> Hacking	Intentionally circumventing security controls to access or harm an asset without authorization	51.3%	4.5%	Data at Rest in the Back-End: File-level encryption
<input type="checkbox"/> Misuse	Inappropriate or malicious use of assets by an actor with authorized access	20.3%	5.0%	
<input type="checkbox"/> Error	An action that causes or significantly contributes to an incident, and which deviates from the normal processes of the organization	13.6%	12.2%	Data in Use at the Endpoints: Full-disk encryption
<input type="checkbox"/> Physical	Deliberate actions on assets that involve possession, proximity or force	2.8%	68.6%	
<input type="checkbox"/> Malware	Malicious software that makes an unauthorized change in the state or function of an asset	4.5%	6.0%	
<input type="checkbox"/> Social	Exploiting human behaviors as the means to install malware, gather info, gain access, etc.	3.4%	2.0%	
<input type="checkbox"/> Environmental	Incidents caused by natural events (e.g., earthquakes, floods) or other hazards (e.g., power, water, temperature) associated with the environment in which assets are located	0.3%	0.0%	
<input type="checkbox"/> Unknown	Not otherwise categorized	3.9%	1.5%	

Source: analysis of actual data breach incidents is based on [VERIS Community Database](#); adapted by Aberdeen Group, June 2015



➔ Read the full report: [Selecting Encryption for “Data at Rest” in Back-End Systems: What Risks are You Trying to Address?](#) July 2015