Certes Cyber Insights: **Breaches Are Inevitable. Data Loss Doesn't Have to Be.**

Hackers don't need to break in anymore. They log in with stolen credentials, exploit weak passwords, and siphon data in transit from networks that were never built to stop them. Once they have your data, it becomes ransom, leverage, or revenue.

The latest global attack testing proves the problem: identity checks are failing, detection is lagging, and data theft is skyrocketing. Legacy security defenses can't close the gap.

So, what can you do about it?

We explore where defenses are collapsing and how Certes DPRM (Data Protection and Risk Mitigation) makes sure that even if attackers get in, the data they take is worthless.

Breaches Are Succeeding More Often

46% of environments had at least one cracked password (up from 25% last year). Weak password policies make it easy for attackers to escalate access.

98% success rate for attackers using stolen logins. Once inside, they blend in as if they were a real employee.

Prevention effectiveness dropped from 69% to 62%. Traditional controls are losing ground as attackers improve their techniques.

Attackers **can** steal credentials, but they **can't** use your data if it's protected with Data Protection and Risk Mitigation (DPRM).

If your data isn't protected, your business isn't protected. Full stop.

Data Theft Is the Weakest Link

97% **of businesses do not protect themselves against data exfiltration. This means attackers can steal sensitive files almost at will.**

Infostealing malware has surged 3x in 2025. Ransomware gangs now prefer "double extortion," stealing data and threatening to leak it instead of just encrypting systems.

3X

Every major breach ends with data **leaving the network**. DPRM makes that data **valueless to attackers**.

Passwords and Identity Tools Are Failing

Almost half of organizations tested had at least one cracked password.

25% of malware samples target password managers and stored credentials, giving attackers immediate access.

Relying on identity tools like MFA and SSO is no longer enough; once a login is stolen, the attacker is inside.

Identity, detection, and firewalls **can be beaten**. DPRM ensures the data **remains secure**, no matter what fails.

Detection Doesn't Stop Attacks

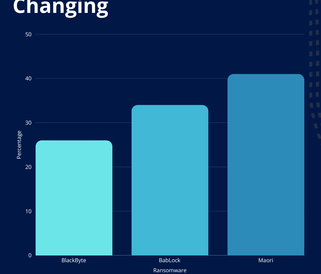
54% of attacker actions aren't even logged. If it's not logged, it can't be detected.

86% of attacks fly under the radar.

Prevention effectiveness is still dropping, proving detection tools alone can't keep up.

Legacy tools won't save you. It's time to protect the crown jewels - **the data** - not just the perimeter.

Ransomware Tactics Are Changing



- **BlackByte ransomware remains the hardest strain to stop, with only 26% prevention effectiveness.**
- **Other strains like BabLock (34%) and Maori (41%) are still slipping past defenses.**
- **Attackers are shifting to "encryptionless extortion," stealing data and threatening to release it instead of locking systems.**

Backups don't prevent criminals from leaking your data. DPRM prevents extortion by making stolen files unusable.

***Stats from Picus Blue Report, 2025**

CERTES DPRM: CLOSING THE GAP

Your perimeter will be breached. Your credentials will be stolen. Your backups will be bypassed. The only question is whether the data remains usable once it's out of your hands.

Certes DPRM ensures the answer is no.

Compliant with CJIS, GDPR, DORA, NIS2

Post-Quantum security that's already in place

Secures data in transit, even if the network is compromised

Built for resilience, so attackers can't use what they steal

Take away the value of data, and you remove the reason to attack in the first place. DPRM makes stolen data valueless.

Keep your data Secret. Keep your data Certes.

Booka meeting with us and find out more about how Certes can help safeguard your business.

www.certes.ai