Why Data Security is More Important Than Network Security

Your Network Can Be Breached, But Your Data Doesn't Have to Be

The realisation that data security is the most critical aspect of cybersecurity is now a staple - it's now far more important than traditional network security. While network security plays a role in protecting the infrastructure, it is ultimately data that cybercriminals, insider threats, and nation-state actors are after. Securing the network without securing the data is like locking the doors but leaving the valuables unguarded. Here's why data security should take priority:

Data is the Ultimate Target of Every Cyberattack

- Hackers don't **steal networks** - they steal **data**.
- **Financial records, customer information, intellectual property, the trade secrets** are the assets that fuel cybercrime.
- **Example:** The **Equifax breach (2017)** compromised **147 million records**, leading to **$700M in legal settlements** - yet the network remained intact.

Reality: **Protecting the data itself is far more critical than just securing the network it travels through.**

> **Cybercriminals target data, not networks. Financial records, customer details, and intellectual property are the real assets at risk, making data protection the top cybersecurity priority.**
>
> *Paul German – CEO, Certes*

Data is More Valuable Than Infrastructure

- Businesses today are driven by data analytics, customer insights, and proprietary algorithms.
- **Losing access to data means lost revenue, legal liabilities, and reputational damage** - even if the network remains secure.
- **Example:** The **Equifax breach (2017)** compromised **147 million records**, leading to **$700M in legal settlements** - yet the network remained intact.

Reality: **A business can recover from a network outage, but data loss or exposure can be irreversible.**

Insider Threats Make Network Security Less Effective

- Many breaches happen from inside the organization - not through external network attacks.
- Employees, contractors, and third-party vendors often have legitimate access to networks, meaning traditional firewalls and perimeter security fail to stop them.
- **Example:** Tesla faced an insider data theft case where an employee leaked confidential business information, bypassing network security altogether.

Reality: **Data security focuses on encryption, access controls, and data loss prevention - stopping both external and internal threats.**

Cloud Computing & Remote Work Make Network Boundaries Obsolete

- With cloud storage, SaaS applications, and remote work, corporate data no longer stays within a single network.
- Traditional firewalls and VPNs don't protect data stored in cloud apps like Google Drive, Dropbox, or Microsoft 365.

- **Example:** The Capital One breach (2019) involved a misconfigured Amazon S3 bucket, exposing 100M+ customer records, despite having strong network security.

Reality: Network perimeters are disappearing—securing data itself is the only reliable defence.

> **Data breaches have lasting consequences.**
>
> **While networks can be restored, exposed or stolen data can lead to severe financial losses, legal repercussions, and long-term reputational damage.**
>
> *Simon Pamplin – CTO, Certes*

Ransomware Attacks Focus on Data, Not Networks

- Modern cyberattacks - especially ransomware - do not target networks; they encrypt critical data and demand payment.
- **Example:** The Colonial Pipeline ransomware attack (2021) disrupted fuel supplies across the U.S. because data access was lost, even though the network was functional.
- Data-centric security (encryption, backups, and zero-trust policies) is the best way to mitigate ransomware damage.

Reality: **Securing the network does nothing if attackers can access and encrypt business-critical data.**

Regulatory & Legal Consequences Focus on Data Protection

- Governments and regulators do not penalize companies for network breaches—they penalize them for data exposure.
- Laws like GDPR, CCPA, and HIPAA impose massive fines for failing to protect personal and sensitive data.

Zero Trust & Data-Centric Security is the Future

- "Trust no one, verify everything" is the foundation of modern security.
- However, the third tier of Zero Trust is "Assume Breach" – your network will be breached so focus on protecting the target of the attack with Data centric DPRM protection.
- Businesses must encrypt sensitive data, limit access, and monitor usage—regardless of network security measures.
- Example: Google's BeyondCorp model eliminates reliance on network security, focusing instead on data access controls.

Reality: **The future of cybersecurity is data-driven, not network-driven.**

Conclusion

- Hackers want data, not networks.
- Insider threats bypass firewalls but can be stopped with data loss prevention (DLP) tools.
- Data exfiltration / Ransomware exploit CVE and Zero-Day vulnerabilities in Firewalls and monitoring tools but can be defeated by Data Protection and Risk Mitigation tools (DPRM).
- Cloud and remote work render network-based security ineffective, data centric tools like DPRM abstract data protection from infrastructure so the data remains protected no matter what network it travels over.
- Legal and financial damages stem from data breaches, not network intrusions.

Protecting data—not just networks—is the key to modern cybersecurity.

Contact Certes

300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108

1 (888) 833-1142

sales@certes.ai