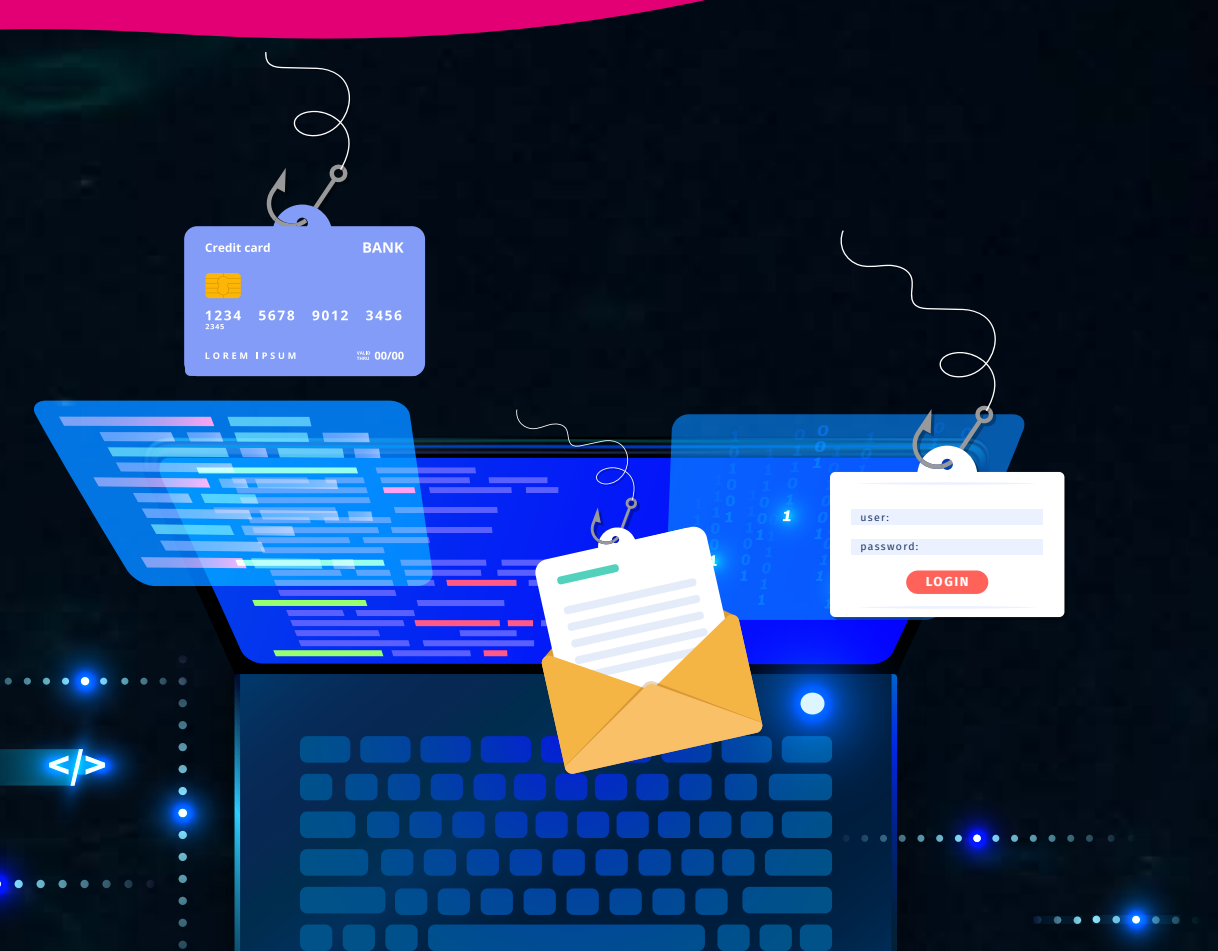
How to soften the blow of **ransomware attacks?**



1 The rising threat

Ransomware is now theft, extortion, disruption, not just data lockout. Some numbers depicting the threat landscape:

49%	of victims pay the ransom
$1M	= median payment
$1.5M +	= average recovery cost
$2.5M	total business impact
53%	fully recover within a week when controls are strong*

** Source: The State of Ransomware Report, 2025, Sophos

2 Why traditional defences fail

- Perimeter stops external-internal, not internal-internal network traffic
- Stolen credentials bypass firewalls
- Third-party supplier compromise is common
- Backups don't stop network-wide spread

3 An attack on a global retailer: M&S

- Attackers entered Marks & Spencer systems via a supplier help desk
- Moved laterally into core systems
- Resulted in major disruption + financial loss
- With microsegmentation security, the attack would have stopped in the supplier zone

4 What microsegmentation does

- Creates workload-level security zones
- Only approved traffic moves between systems
- Enforces least privilege at the network level

5 How it stops ransomware

- Blocks lateral movement
- Isolates infected systems instantly
- Containment = no domino effect
- Turns a major breach into a localized event

6 Key features

- Granular, policy-based traffic control
- Application-level visibility
- Real-time traffic mapping
- Identity-based enforcement
- Integrates with SIEM/XDR
- Agent-based or agentless deployment

7 Business benefits

- Limits blast radius and spread
- Cuts attack surface dramatically
- Faster isolation during incidents
- Supports PCI DSS, HIPAA, SOC 2
- Builds Zero Trust model by default

8 Bottom line

Microsegmentation is the decisive control that prevents ransomware from becoming an enterprise-wide outage.

To prevent ransomware attacks, get in touch with us today at:

cyber.security@t-systems.com

T Systems