WEBINAR

Zero Trust

End-to-end Protection and Policy Control for Sensitive Data

March 5, 2019

link by mobile:helix

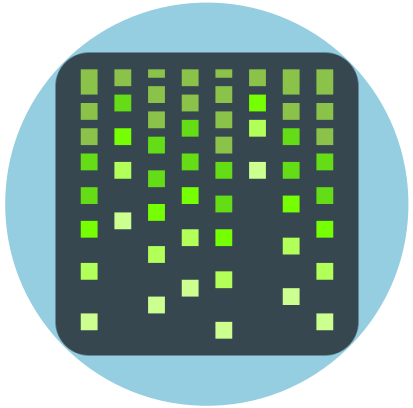
According to the World Economic Forum, a cyber attack is one of the top 5 greatest risks to our world in 2019

https://www.weforum.org/agenda/2019/01/these-are-the-biggest-risks-facing-our-world-in-2019/

Cyber Risk Paradigm Shift

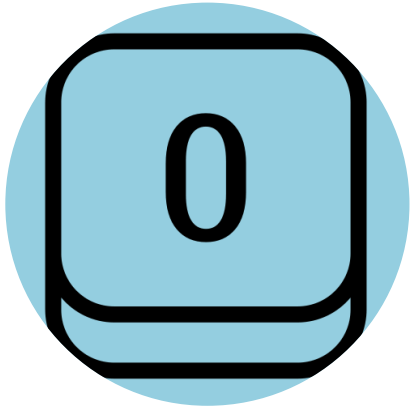
Network Centric

Protect the perimeter: the age of the firewall.



Data Centric

Protect the data: the age of encryption.



Zero Trust

Protect access: the age of ??.

Data protection in a zero-trust World

Data sanctuaries are designated repositories for sensitive data. These repositories must:

1. Implement pessimistic permissions
2. Provide a way to restrict client access

Data classification assigns policies and permissions to sensitive data. These policies must:

1. Be pessimistic – access on a need-to-know basis
2. Must travel with the data in some way

Data protection ensures that data policies are enforced uniformly, in all scenarios. It must:

1. Enable protected collaboration in your firm
2. Enable safe data sharing

What makes a secure data sanctuary?

1. Policies and permissions that match the sensitive of your documents
2. Controlled client access
3. A way to reference documents by link
4. A way to track activity and actor

What makes a data classification secure?

1. Pessimistic – i.e., permission is granted, not assumed
2. No loop holes (or at least minimal)
3. Applied at the group level, but allows for individualized exceptions

What makes data protection effective?

1. Leverages existing technology as much as possible (e.g., sending links not documents)
2. Protects data based on where it came from (because that is how you encode your classification!)
3. Has no loop holes – and email is a giant loop hole to close
4. Is driven by policy and workflow, not by user choice

The best is the enemy of the good

- Voltaire

Three steps to get started with 0-trust

Identify your most sensitive data. All data is not equal – start with the stuff you really care about:

1. Where is it stored?
2. How is it accessed?
3. Design a *better* path of least resistancee

Lock down your most sensitive data. If you you classify conservatively, you won't burn the house down.

1. Pick clients/matters that demand better protections
2. Be pessimistic ASAP

Find your biggest loop holes. Email and mobile are the top two on most lists.

1. Why aren't your users sending NRLs/links?
2. Make mobile the safe haven, not the back door

Key takeaways and pitfalls to avoid

Protect your sanctuaries. In particular, remember that most successful attacks these days are email-born, not hackers breaking into your firewall. Client protection is as critical as server protection.

Pessimistic permissions are essential. There must be a stake in the ground. However, superusers, email attachments, and file sharing services de-classify data. Provide a better way for attorneys and IT to work.

Data protection must operate end-to-end. Protecting data in DMS is ineffective if attorneys are sharing documents internally and externally without protection.

How we can help.

Link extends your data protection to mobile:

- We make it easy to consume and send document links
- We lock down the mobile client
- We integrate with IRM to safely share documents
- Mobile DLP and metadata scrubbing
- And stay tuned … we are moving beyond mobile in 2019!

Have questions?

contact@mobilehelix.com

347.508.0967