Take the Risk out of Digital Transformation

By providing the adversarial view, XM Cyber's hybrid Attack Path Management Platform helps organizations rise to the challenge of de-risking Digital Transformation initiatives

Digital transformation has become a competitive imperative in most industries. Organizations that fail to make this shift successfully – or in a timely fashion – are at risk of falling behind their competitors. Yet a change of this magnitude requires diligent preparation and careful execution.

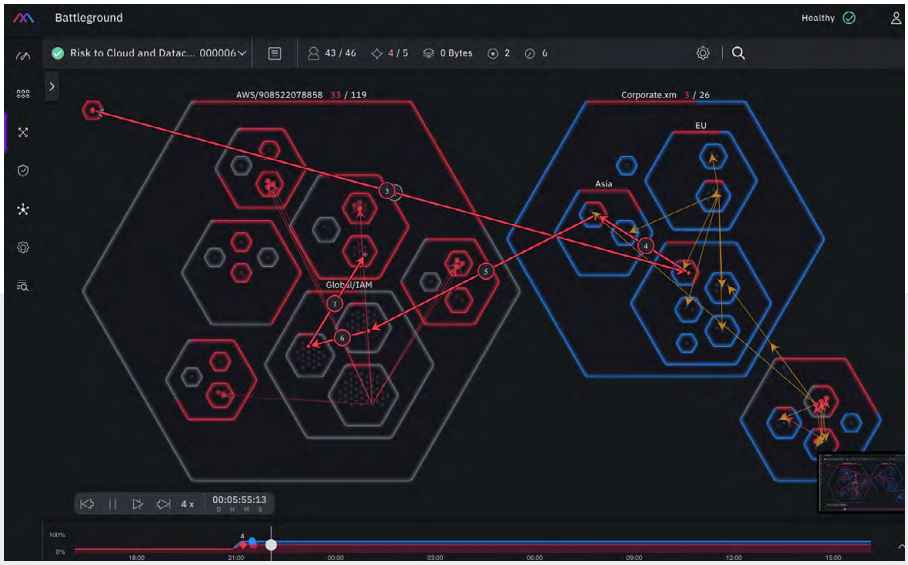
Cybersecurity is one area that is often overlooked in the race to transform, and the consequences of this omission can be ruinous, both financially and reputationally.

82% of IT leaders told the Ponemon Institute that their digital transformation initiatives were responsible for at least one data breach

The Security Challenges with Digital Transformation

As digital transformation initiatives are fast-tracked, security standards have often fallen by the wayside. A surprising 82% of IT leaders told the Ponemon Institute that their digital transformation initiatives were responsible for at least one data breach, while roughly 63% of IT leaders told the Ponemon Institute that they are not confident in their ability to operate securely in such a dynamic context. One reason for this is that digital transformation has lots of uncontrolled change.

While an 82% breach rate may be understandable to some degree given the complexity of such large-scale shifts, it is also unacceptably risky. Even the most innovative new processes and technologies don't mean much if a company cannot protect its business-critical assets.



See attack paths across on-premises and cloud networks to reduce cyber exposures

Let's take a closer look at some of the core challenges with digital transformation:

- **Complexity and scale of environments is increasing**
  Hybrid cloud and multi-cloud networks create heightened complexity, which in turn can create environment-specific silos that attackers will exploit to move laterally. The dynamic nature of cloud computing -- and the amount of fast-paced change needed to execute business strategy -- puts the attack surface in flux and makes it difficult to manage.

- **Operational security processes become split**
  Separate processes and personnel (IT teams vs. DevOps/SecOps) are often set up to manage cloud environments, thus fragmenting the security of organizations.

- **Unnecessary high level of permission**
  The cloud's permission models make it harder for teams to keep track of who has access or permissions to given resources or services. Identities with an unnecessarily high level of permission or permissions beyond the lowest privilege requirement can put your entire network at risk if not detected, monitored and fixed constantly.

- **Traditional penetration testing and red teaming will not scale**
  In order to meet the modern needs of a hybrid organization, a continuous and comprehensive understanding of the attack surface is crucial.

- **Most importantly, the adversarial view is missing**
  Defenders lack insight into the ways that cloud environments can be compromised, as well as the mechanics and risks of lateral movement. Attackers don't think in terms of compliance and controls. They will use all available technical weaknesses to exploit critical assets.

Securing Your Journey to the Cloud

XM Cyber provides continuous and safe attack modeling across on-premises and cloud networks. It highlights all exploitable attack paths and illuminates lateral movement opportunities between cloud and on-premises environments.

Integration of XM Cyber's attack path management platform with your operational and technology ecosystem will provide game changing benefits across the security stack.

- Illuminate attack paths to your critical assets across on-premises and multi-cloud environments
- Achieve better control over the true risk of compromise within hybrid environments and enable a more proactive approach, allowing security teams to close exposures as they appear.
- Red team effectiveness will increase due to expanding capacity and coverage, and security operations will improve because of the reduced detection and response times.
- Gain insight to drive cost-effective, prioritized risk mitigation. Adversarial-focused risk reporting for corporate boards helps provide much needed quantification, resolving the disconnect that is sometimes present between CISOs and the business side of the organization.

Successful digital transformation requires buy-in from leaders and their teams, support from the C-suite, and a careful and well-thought-out plan. Having the adversarial perspective of the hybrid environment empowers business leaders to understand and manage exploitable risks caused by attack paths. This provides organizations with the confidence to accelerate transformation and gives security teams the insight needed to dramatically reduce the chances of compromise.

Tel Aviv +972 3 978 6668
New York +1 866 598 6170
London +44 203 322 3031
Munich +49 163 6288041
info@xmcyber.com