SECURITY FOR TECH

FACE YOUR CYBERSECURITY CHALLENGES HEAD-ON

PROTECT SOURCE CODE AND IP FROM THEFT

Poor internal security controls can be an invitation for an unscrupulous insider or an attacker to take off with your source code and other IP without getting detected. This threat is most acute for early stage startups but remains a significant threat in later stages as well. Your secret sauce must always be protected.

CATCH SECURITY ISSUES AT DESIGN STAGE

Poor design choices, business logic mistakes and errors in handling sensitive data, authentication, access control and cryptography can be expensive to fix later and can threaten company survival if exploited by attackers. Build security into your dev cycle.

DON'T LOSE CUSTOMER OPPORTUNITIES

Startups in verticals such as fintech, biotech and healthcare and startups targeting large enterprise customers have to demonstrate robust security and satisfy relevant security compliance regimes. Startups that ignore this or address it too late risk losing major customer opportunities or incurring financial penalties due to non-compliance. Be proactive in addressing compliance.

CUSTOMERS BRING YOU IN SPOTLIGHT

As startups gain customers, they become attractive targets for cybercriminals interested in their valuable data, disrupting them for ransomware or attacking them for a host of other reasons.

BE INCIDENT-READY

Do you do more fire and earthquake drills than cybersecurity drills even though the latter may be more likely to occur? What will you do in the event of a successful attack? Whom would you call? Do they understand your environment beforehand? Does your environment lend itself to finding the attacker's trail? How will you ensure business continuity? How will you manage customer and public perception?

BE HARD TO ATTACK AND HARD TO DAMAGE

Minimize your attack surface so that you are very hard to attack as opposed to being a big target that is hard to defend. Create a security architecture that limits the damage from a successful attack as opposed to an architecture where a successful breach causes everything to fall apart.

MONITOR, DETECT & RESPOND TO ATTACKS

Who watches over your prized assets? Is it round the clock? Can they recognize a stealthy attack? Do they have the ability to respond to it and minimize damage?

DO YOU HAVE CYBERSECURITY EXPERTS?

The reality is that startup engineering and IT organizations typically lack security expertise and focus. Hence, it is dangerous to rely on their verdict and due diligence on cybersecurity. If you are exposed to the risks highlighted above, you should team up with cybersecurity experts.

EBRYX SOLVES TECH COMPANIES' SECURITY PROBLEMS COST-EFFECTIVELY

We have a unique solution for minimizing your attack surface and limiting damage. We help you with secure engineering, secure operations and compliance. We provide security assessment, penetration testing, continuous monitoring, incident readiness, detection and response services. We have a minimalistic approach and are sensitive to tight cybersecurity budgets.

Our goal is to be your long-term security partners from early stage to late stage and help you develop in-house capacity wherever needed along the way.