Recorded Future®

SOLUTION BRIEF

Zero Trust Security

There Is No “Zero Trust” Without Intelligence

Challenges Today

For years, security practices were structured around protecting a company’s critical infrastructure and assets by working to secure the perimeter. The assumption was that if you prevented someone from accessing your network with robust controls, then you could trust the people on the network to perform privileged actions.

This was the model of a castle - where you construct a moat and strong walls - but this model does not scale to the distributed and often cloud-based applications that are used within enterprises today. Now, instead of walls, organizations need watchtowers that allow them to continuously monitor their internal and external threat landscape for compromised identities.

Zero Trust is Just the Beginning

Organizations must now secure every authentication and action request that is being made, regardless of whether the user is on the network or remote. To accomplish this, many organizations are moving towards a Zero Trust model, as it allows for zero implicit trust based on the location or previous authentication grants of the user.

Establishing user trust and ensuring that only authorized users are attempting to access resources can be achieved in a number of ways. Multi-factor authentication (MFA) and passwordless authentication are both common options today, but neither are perfect solutions that eliminate identity-related risks for organizations.

Many MFA solutions, especially for consumer services, rely on SMS messages to send a code to the user which unfortunately can be hacked or spoofed. Additionally, there will inevitably be some legacy systems that don’t support MFA, leaving a door open to threat actors. And in regards to passwordless authentication, credentials are used to authenticate the system on the backend, meaning password security and the user’s identity are still potential avenues for compromise.

So while MFA and passwordless authentication solutions provide more secure solutions for accessing business-critical applications and infrastructure, they don’t solve for the fundamental issue of a Zero Trust model, which still inherently relies on one thing - a user’s identity.

As organizations remove implicit trust based on a device or network segment, they place more importance on the authenticity and security of a user’s identity. Therefore, to ensure their access and security management is effective, organizations must also increase the data-driven insights for an identity. Identity Intelligence provides the critical insights for a Zero Trust approach, by enabling organizations to automatically identify identity compromises and be able to respond confidently — all without any manual effort.

Identity Intelligence for a Zero Trust Model

The Identity Intelligence module by Recorded Future automates the collection, analysis, and production of intelligence from a vast range of open source, dark web, and technical sources, offering an unmatched source of truth for identity authenticity that can be automatically integrated into a Zero Trust based environment to dramatically reduce the amount of time it takes to detect, investigate, and respond to real risks to the organization. Identity Intelligence enables organizations to:

- **Identify the Riskiest Users and Enforce More Robust Security Controls:** Continuously measure user risk based on their security posture and exposure trends to target more robust controls. Users with high compromises should be required to reset passwords more frequently, use stronger passwords, or use MFA for every login attempt.
- **Proactively Reset Compromised Identities with Confidence:** Utilize real-time intelligence to trigger automatic actions such as restricting access on a compromised account or requiring multi-factor authentication, since many systems only require MFA every few days or weeks by default.
- **Investigate and Determine Root-Case for Security Incidents:** Understand the context of security incidents to increase the speed and quality of the root-case analysis.

This intelligence-driven approach to Zero Trust security empowers organizations to disrupt adversaries before damage to the business can be done. With relevant insights, updated in real-time, from Recorded Future's Identity Intelligence module, organizations can effectively prevent identity fraud and reduce risk.