RECAST SOFTWARE

Security at the Gates
Zero Trust Strategy

Never Trust, Always Verify

Place a bouncer at your door. Then verify all users, devices, and services before they access the organization's resources. Repeat every time.

Without Zero Trust the Gates are Open

Data Breaches Increase

Intellectual Property Theft Risk Rises

Ransomware Attacks Abound

- **2019: ThyssenKrupp attacked.** 40TB of stolen data encrypted. **$50 million** ransom requested.[1]
- **2020: AMD breached.** Source code and trade secrets stolen.[2]
- **2020: Norsk Hydro attacked.** 170 plants shut down resulting in **$71 million** in financial losses.[3]
- **2020: SolarWinds breached**. Sensitive data revealed costing U.S. businesses and government agencies an estimated **$100 billion**.[4]
- **2022: LastPass breached.** Compromised encrypted copies of users' password vaults and the cloud storage system.[5]

1 German industrial giant ThyssenKrupp under a cyberattack (Cybernews)

2 A hacker stole and leaked the Xbox Series X graphics code (engadget.com)

3 Hackers hit Norsk Hydro with ransomware. The company responded with transparency (microsoft.com)

4 SolarWinds Hack Recovery May Cost Upward of $100B (govtech.com)

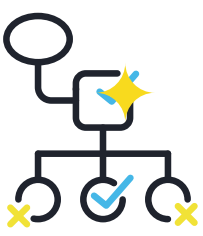
5 The LastPass Hack Somehow Gets Worse (wired.com)

YOUR POWERFUL BOUNCER
The Principle of Least Privilege

Data from Microsoft going back to 2013 revealed that **92% of all "critical" vulnerabilities were mitigated** by removing admin rights.*

* 2013 Microsoft Vulnerabilities Study: Mitigating Risk by Removing User Privileges

A Brief Guide to Securing Your Systems

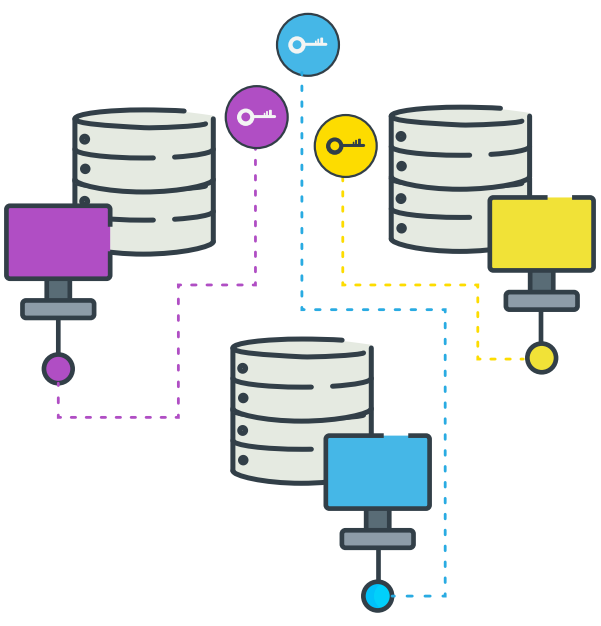


Role-Based Access Control (RBAC)
Grants users access to resources based on their job roles.

Access Control Lists (ACL)
A list of users and groups that identifies the resources they can access.

Multifactor Authentication (MFA)
Requires users to provide multiple forms of verification to access a system or resource.

Single Sign-On (SSO)
Allows users to log in to multiple applications with a single username and password.



Endpoint Architecture for a World of Risks

Organizations must invest in a security architecture that supports zero trust. This can include a micro-segmentation approach, which isolates critical resources and limits the scope of a potential attack.

VIP Lists and Security at Every Entry

Adding a skilled zero trust bouncer at your organization's door is the best way to keep up with ever-evolving cyber threats. Embrace zero trust or face unnecessary risk.

Learn more about RECAST SOFTWARE here.

RECAST SOFTWARE

About Recast Software

Recast Software is a crucial part of how teams create secure and compliant environments in an ever-changing IT landscape. Our software does this by seamlessly integrating with existing IT infrastructure to quickly remediate issues, ensure compliance, enhance security, and maintain clear visibility across all devices.