RECAST SOFTWARE

The Bouncer at your Door

Embrace Zero Trust or Face Unnecessary Risk

In a time of constantly evolving cyber threats, organizations must work to protect their resources and data. Zero trust is a security concept that is quickly becoming a necessity for all organizations looking to protect their assets and data. At its core, zero trust is a security strategy that requires verification of all users and entities before granting access. Think of it as a virtual bouncer for your company's resources. No unauthorized access allowed! By requiring verification at every step, zero trust creates a strong foundation for your security posture.

Never Trust, Always Verify

The concept of zero trust is clear and compact: never trust, always verify. Place a bouncer at your door. Then all users, devices, and services must be verified before accessing the organization's resources. This also means that users must be continuously monitored and verified every time they attempt to access the organization's resources.

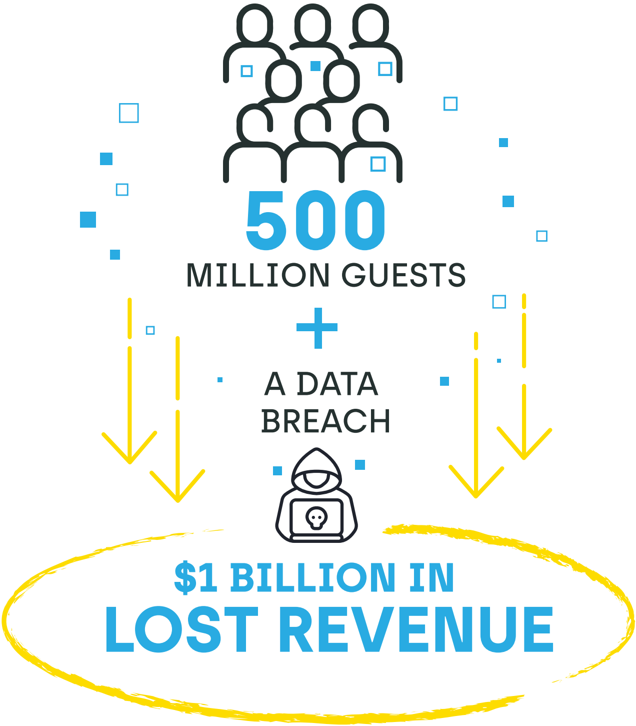
The goal of zero trust is to reduce the risk of malicious actors gaining access to the organization's resources. By verifying all users, devices, and services, organizations can best ensure that only authorized users and devices are allowed access.

Without Zero Trust the Gates are Open

Data Breaches Increase

If you're not implementing zero trust policies, you might as well be rolling out the welcome mat for malicious actors. Without zero trust policies, data breaches are nearly inevitable. Don't believe us? Just ask the companies who made headlines recently after learning the hard way.

- **2018:** The Marriott International data breach exposed the personal data of 500 million guests and cost the company an estimated $1 billion in lost revenue.*
- **2020:** SolarWinds suffered a major data breach due to a lack of zero trust policies. The breach led to the loss of sensitive data and cost U.S. businesses and government agencies an estimated $100 billion.**
- **2022:** LastPass suffered a series of breaches that compromised encrypted copies of users' password vaults and the cloud storage system. The reputational damage for LastPass was immense, and financial losses haven't yet been disclosed.***



500 MILLION GUESTS

+

A DATA BREACH

$1 BILLION IN LOST REVENUE

* Cyber Case Study: Marriott Data Breach

** SolarWinds Hack Recovery May Cost Upward of $100B

*** The LastPass Hack Somehow Gets Worse

Intellectual Property Theft Risk Rises

Valuable intellectual property is like your secret recipe for the best pizza in town. Without zero trust policies, your company's source code and trade secrets may be up for grabs to the highest bidder. Trust us, you don't want to see your secret sauce on the dark web.

Ransomware Attacks Abound

It's straight out of a Hollywood blockbuster. Your company's data is encrypted, and you're being held hostage for millions of dollars. Unfortunately, this drama has played out in real life with increasing frequency. The organizations below have already hit the "big screen" with their heist stories. Organizations that do not implement zero trust policies are more likely to be targeted by ransomware gangs, as these malicious actors can more easily access these organizations' resources and data.

2020:
a major data breach at AMD exposed source code and trade secrets. The hackers asked for

$100 million

on the open market for the source code.*

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

WITHOUT ZERO TRUST

2018:

a ransomware attack on the City of Atlanta encrypted the city's data and **forced the city to shut down several online services.**

2019:

the ransomware attack on the German-based steel producer ThyssenKrupp encrypted 40TB of stolen data. Attackers asked for **$50 million** for the data.*

* German industrial giant ThyssenKrupp under a cyberattack | Cybernews

2020:

a ransomware attack on the global aluminum manufacturer Norsk Hydro resulted 170 plants shutting down operations and **$71 million in financial losses.****

** Hackers hit Norsk Hydro with ransomware. The company responded with transparency - Source (microsoft.com)

Customer Confidence Declines

Trust is the foundation of any successful business relationship, a delicate dance that requires a company to lead with care. A misstep can have dire consequences. Confidence falls and the dance can quickly fall apart. Breaches enabled by a lack of zero trust policies erode confidence in the breached organization.

Once trust is lost, the negative impact extends far beyond the affected customers. As news of a data breach spreads, potential customers start hesitating to engage with the hacked company, and existing customers may choose to take their business elsewhere. This ripple effect hinders a company's ability to attract new customers and retain existing ones.

A Saving Grace

The Principle of Least Privilege

The principle of least privilege is a cybersecurity approach where users gain access to only the data and resources they require to perform their job, and only for the duration necessary to complete that task. Users should only be granted the minimum level of access necessary to complete their tasks, and that access should be revoked as soon as it is no longer needed.

Data from Microsoft going back to 2013 revealed that 92% of all "critical" vulnerabilities were mitigated by removing admin rights.* Restricting admin rights and implementing the principle of least privilege forms the bedrock of zero trust security. By granting users only the minimum level of access they need, organizations can prevent most security breaches.

92%

of all "critical" vulnerabilities were mitigated by removing admin rights

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

The Power of Least Privilege

A Brief Guide to Securing Your Systems

Role-Based Access Control (RBAC)

A method of granting users access to resources based on their job roles. Just like you wouldn't let the drummer play the piano at your band's upcoming gig, you shouldn't give an employee in the marketing department access to the company's financial systems.

Access Control Lists (ACL)

ACLs are like a VIP list for your company's resources. You maintain lists of users and groups and the resources they can access. Then your zero trust nightclub bouncer only lets in the people on the list.

For example, an ACL might list all of the employees who have access to the company's file server. Only those on the list can gain access.

Multifactor Authentication (MFA)

A security measure that requires users to provide multiple forms of verification to access a system or resource. MFA combines something the user knows (e.g., a password), something the user has (e.g., a security token or mobile device), and/or something the user is (e.g., biometric data like a fingerprint). This added layer of security creates a secret handshake for each employee that helps ensure unauthorized access is prevented, even if a user's credentials are compromised.

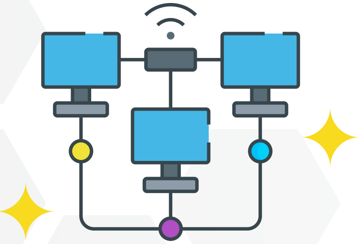
Single Sign-On (SSO)

A system that allows users to log in to multiple applications with a single username and password. This streamlines the login process, reduces the need to remember multiple passwords, and encourages the use of a single, strong password. As a result, SSO enhances security by impeding unauthorized access to sensitive data.

These four methods combined ensure that users only have access to resources necessary for their job roles, maintain clear records of authorized access, and provide robust security through multiple verification or simplified login processes across multiple applications. Leveraging these strategies minimizes the risk of unauthorized access, protects sensitive data, and helps maintain a strong security posture.

Always On

Organizations must embrace zero trust in order to protect their resources and data from malicious actors. Zero trust is not a one-time solution, but rather needs to be implemented and then constantly improved in order to be effective. Organizations will face cyber threats that evolve rapidly, and zero trust is the best practice for keeping up with these ever-evolving threats.



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. The micro-segmentation approach is a security architecture that divides a company's network into smaller segments, or "micro-segments", in order to isolate critical resources and limit the scope of a potential attack.

> "For most, this won't be a one-shot upgrade; legacy systems and zero-trust environments will take time to coexist. Since zero-trust technology is still maturing, it's important to understand the technology and solution to better protect investments over the long term."
>
> - TIM LIU OF HILLSTONE NETWORKS, FORBES

16 Essential Early Steps In Creating An Effective Zero-Trust Environment

Conclusion

You Need a Bouncer at your Door

Embracing zero trust is the best way to keep up with ever-evolving cyber threats. Organizations must invest in strong authentication methods, user and device monitoring, and a security architecture that supports zero trust. By doing so, organizations can reduce their risk of a malicious actor gaining access to their resources and data. Embrace zero trust or face unnecessary risk.

Embrace zero trust or face unnecessary risk

Who We Are

Learn more about Recast Software here.
recastsoftware.com

We're obsessed with information technology and how to better manage it.

We are a dedicated group of Systems Administrators and tech-savvy product experts that love what we do and the IT community we do it with.

We empower organizations to better manage and support users and devices.

We are a rapidly growing software company with our solutions being used by thousands of enterprise organizations in more than 125 countries, impacting millions of devices and (more importantly) the people who use them. With our growing portfolio of tools, we empower IT departments at every single endpoint to do their best work.