BEYOND IDENTITY

Zero Trust Authentication and Remote Access: Strengthening Security

Secure remote access to your networks and resources used to be a nice option, now it's a necessity. Your employees need to access applications that are stored on your cloud. A contractor needs to access company resources on their BYOD device. Your network administrator wants to update software in the middle of the night at home with less disruption.

According to Gartner, 39% of knowledge workers will be hybrid by the end of 2023. With the increase in remote work, the ability to access an organization's data, apps, and infrastructure from anywhere, at any time, on any device is now a business requirement.

Employees with location flexibility often experience better work-life balance and greater job satisfaction. Additionally, employees who can choose the best work location for their specific tasks are often more productive. Remote access also improves business continuity in the event of a natural disaster, as employees can work from other locations. The flexibility is beneficial, but how do you make sure your resources remain secure?

Security concerns with remote access

While remote access provides many benefits, it also can increase cybersecurity risk without proper access control.

With the in-office model, cybersecurity professionals used to focus on protecting the perimeter, which is the physical building and network. Remote access changes that. Instead of protecting a finite number of endpoints (places where employees access the network), cybersecurity professionals often have to protect a surface area that spans the entire globe.

Remote access increases multiple security concerns, including:

- **Increased cost of a breach.** The IBM 2023 Cost of a Data Breach report found that a remote workforce increased the cost of a breach by an average of $173,074. Breaches that happen through remote access often take longer to detect, which increases the damage caused.
- **Numerous specific threats targeting remote access.** Because stealing credentials is often easier with remote access, many cybercriminals target users remotely accessing a network. With those credentials, threat actors can then perform an account takeover with access control, where they gain full access to the account. They often change the password, so the authorized user no longer has access. Cybercriminals are then able to use the account to make purchases, access data, and even gain access to more accounts.
- **Increased use of BYOD devices.** It's easier to check work email on a personal device if it's the one closest to you, even if it's against company policy. Employees accessing the network remotely may use devices that do not meet the organization's security standards.
- **Risk varies based on the employee.** With remote access, each employee handles their own cybersecurity.

Because there is less oversight, some employees follow the processes, but there are likely those who don't always do so, which means higher risk. While IT leaders can provide training and tools, the actual follow-through is largely in each employee's hands.

- **Stolen or compromised credential breaches are challenging to resolve.** When employees use remote access, the risk of compromise through stolen or compromised credentials increases. The IBM 2023 Cost of a Data Breach found that this type of attack took the longest to resolve—an average of 328 days.

Reducing risk with Zero Trust Authentication

Reducing the risk caused by remote access requires a shift in strategy. Organizations are now turning to zero trust architectures built on a foundation of Zero Trust Authentication to protect their environment.

Instead of protecting endpoints and a now non-existent perimeter, zero trust focuses on authentication by assuming that every app, user, and device requesting access is unauthorized. With the default being to trust no source, all requests—both external and internal—are continually authenticated during the user session.

The process of implementing zero trust isn't a single technology or approach. It's a framework with numerous principles that you implement throughout your organization. A zero trust architecture coordinates communication between multiple systems to monitor, evaluate, and respond to user and device security threats. Implementing Zero Trust Authentication facilitates that communication during the authentication process and throughout the user session.

With proper implementation, Zero Trust Authentication creates a user experience that empowers employees while also reducing cybersecurity risk.

Zero Trust Authentication consists of seven key elements:

- **Passwordless authentication:** Because passwords rely on human behavior, they offer a weak link to access an organization's sensitive data. By moving to a passwordless model, often through FIDO2-compliant authentication, you eliminate significant risk.
- **Phishing resistance:** By eliminating phishable factors, Zero Trust Authentication makes sure only authorized users access critical resources.
- **Device validation and authorization (Device Trust):** Zero Trust Authentication requires authentication of every device to ensure only trusted devices are granted authorization.
- **Device security posture assessment:** A device that was previously granted access may have become infected or no longer meet security policies. By verifying each device's settings and security controls every time, you ensure all devices are clean and meet standards.
- **Multi-dimensional risk signal analysis:** Cyberattacks and breaches start in different ways. By using the full security ecosystem to analyze risk signals from multiple sources, such as endpoints and IT management tools, you can make the best possible risk-based decision.
- **Continuous risk assessment:** Traditional security practices focus on authentication—once. Zero Trust Authentication monitors and evaluates risk throughout a session for behavior changes that might indicate an account takeover or internal threat.
- **Integration with security infrastructure:** When you use a variety of security tools, you improve detection and response to a possible cybersecurity incident.

Zero Trust Authentication improves remote access security

Organizations using Zero Trust Authentication see improved security during remote access user sessions, which results in increased response time and employee satisfaction.

How would your organization benefit?

1. **Enhanced protection:** With Zero Trust Authentication, your data and infrastructure have a much higher level of protection against unauthorized access attempts than with traditional security methods.
2. **Strengthened device security and compliance adherence:** By using Zero Trust Authentication, you can reduce compliance issues, which typically involve expensive fines and reputation damage due to cybersecurity concerns.
3. **Improved risk detection and response capabilities:** Instead of waiting for an incident to occur, Zero Trust Authentication allows you to proactively detect and either stop or mitigate attacks by quarantining devices or completely removing network access for that user.
4. **Decreased BYOD and specific security needs:** Each unmanaged device adds complexity and risk to the environment. Through granular access controls, Zero Trust Authentication eliminates additional management and risk.
5. **Device trust:** By focusing on device trust, Zero Trust Authentication provides peace of mind that every device accessing the data, apps, and infrastructure is authorized.

Conclusion

As your company expands or continues to utilize remote access, Zero Trust Authentication is key to keeping your organization protected from cyberattacks. Because the framework focuses on providing a positive user experience, your employees can get the access they need to do their jobs effectively while the organization stays protected.

When you adopt Zero Trust Authentication, you protect your organization's investments and enhance your ability to serve customers.

The need for remote access in the future will only increase. Give your employees the ability to work wherever they need to, and you are setting up your organization for success both today and in the future. Experience Zero Trust Authentication in action. Book a demo today.