stratascale
CYBERSECURITY DIVISION OF SHI

Zero Trust Guide

Context is Key in Zero Trust

Applying the Kipling Method to gather crucial context to strategically inform security decisions

Table of Contents

Embracing Zero Trust

In an era where cyber threats are increasingly sophisticated, traditional perimeter-based security models are struggling to keep pace. **Enter Zero Trust security**—an approach that challenges the notion of inherent trust, both within and outside an organization.

Zero Trust eliminates implicit trust and continuously validates every stage of digital interaction. Guided by the principle of **"never trust, always verify",** it employs identity verification and microsegmentation to minimize breach impact and improve security posture.

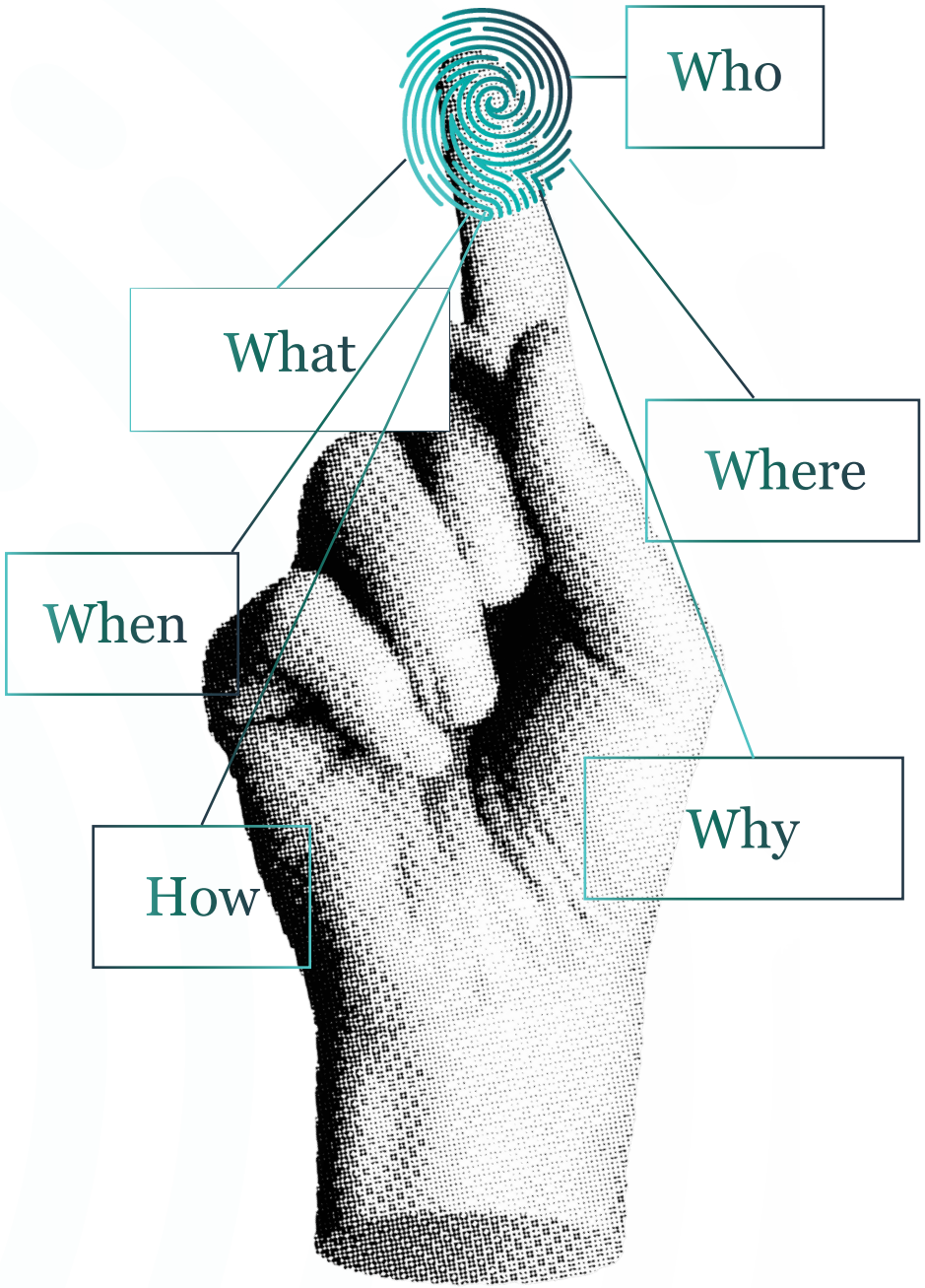
Organizations are increasingly adopting Zero Trust models to combat challenges surfaced by remote work, the rise of cloud-based services, and the proliferation of sophisticated cyberattacks. By embracing Zero Trust, companies can protect their assets in an environment where conventional network perimeters are becoming obsolete.

The benefits of a well-implemented Zero Trust model—including improved security posture, reduced breach impact, and better regulatory compliance—make it an increasingly essential approach in today's dynamic threat landscape.

At the heart of the Zero Trust model lies a fundamental principle: **context is crucial.**

To explore this concept, we turn to Rudyard Kipling's poem "The Elephant's Child," which introduces the idea of the *Six Honest Serving Men:*

> I keep six honest serving-men (they taught me all I know); their names are:



These six questions—Who, What, Where, When, Why, and How—provide a robust framework for gathering information and understanding context. In the realm of Zero Trust, these questions serve as a strong guide for evaluating and making informed access decisions.

By applying the Kipling Method to Zero Trust, organizations can better understand how context informs our security decisions:

- **Who** is attempting to access resources?
- **What** are they trying to access?
- **Where** is the access request originating from?
- **When** is the access attempt being made?
- **Why** is this access necessary?
- **How** are they connecting to the resource?

Each question adds a layer of context that, when combined, offers a comprehensive perspective on access requests. This holistic view enables organizations to make more informed, nuanced decisions about granting or denying access, ultimately enhancing their security posture.

> In the following sections, we'll explore each of these questions in detail, examining how they contribute to the implementation of a robust Zero Trust security model.

Who?

Identities Human/Non-Human

The question of "Who?" is central to the Zero Trust framework, emphasizing the importance of identity verification. In this context, understanding the identity of a user—whether human (carbon-based) or non-human (non-carbon-based)—is paramount. The broad definition of "user" includes not only human employees and customers but also devices, applications, services, and automated processes that may request access to resources.

Organizations must implement robust authentication measures for all types of users:

Human Users

- Multi-factor authentication (MFA)
- Biometric verification (e.g., fingerprint, facial recognition)
- Knowledge-based authentication

Non-Human Users

- API keys and secrets
- Digital certificates
- OAuth tokens
- Device certificates and identifiers

Unlike traditional methods of one-time authentication, continuous verification is crucial in preventing session hijacking or the misuse of compromised credentials, regardless of the user type. This approach ensures that trust is continuously evaluated throughout a session, adapting to changes in user behavior or system state.

By thoroughly verifying identity for all user types, organizations can establish a foundational layer of trust, albeit a conditional one. This comprehensive approach to identity is crucial in modern environments where machine-to-machine communications and automated processes are as common as human-initiated access requests.

Emerging authentication technologies are enhancing this aspect of Zero Trust for both human and non-human users:

Biometrics for humans
Facial recognition, fingerprint scans, and even behavioral biometrics (such as typing patterns) provide stronger identity verification.

Behavioral analysis
AI-driven systems can learn typical behavior patterns for both human and non-human users, detecting anomalies that might indicate a compromised account or system.

Device fingerprinting
For non-human users, advanced techniques can create unique “fingerprints” based on hardware and software configurations, adding an extra layer of identity verification.

Quantum-resistant cryptography
As quantum computing progresses, new cryptographic methods are being developed to secure identity verification for all user types against future threats.

This holistic approach to identity verification within the “Who” aspect of Zero Trust ensures that all entities accessing resources—whether human operators, IoT devices, or cloud services—undergo rigorous verification processes. This significantly reduces the attack surface and enhances overall the security posture.

What?

Resource Identification

Next, we ask, "What?" This question focuses on understanding what resources or applications the user is attempting to access. In a Zero Trust model, the principle of least privilege comes into play—users should only have access to the information necessary for their specific roles.

Organizations can further limit access through microsegmentation, which involves breaking down the network into smaller segments and limiting access even within a specific resource.

For instance, in a healthcare setting, microsegmentation might allow a doctor to access patient medical records while restricting access to billing information, despite being part of the same patient management system.

By clearly defining access levels and segmenting resources, organizations can minimize the risk of data breaches and ensure that sensitive information is protected from unnecessary exposure.

Where?
Access Location

The third question of "Where?" addresses the context of the access request's origin. Is the request coming from a trusted internal network, a remote location, or a potentially compromised public Wi-Fi? Understanding the location of the user adds an important layer of context.

Organizations can implement geo-fencing or conditional access policies that automatically block or restrict access from unrecognized or high-risk locations. If an employee attempts to access sensitive resources from an unrecognized network, additional security measures—such as adaptive authentication or access restrictions—may be warranted to mitigate potential risks.

Zero Trust Network Access:
The Modern Alternative to VPNs

Zero Trust Network Access (ZTNA) plays a crucial role in addressing the "Where" component of a Zero Trust architecture. Traditionally, Virtual Private Networks (VPNs) extended the trusted network perimeter, inadvertently creating an implicit trust boundary. In contrast, ZTNA has become the favored approach in a genuine Zero Trust model due to its transformative approach to granting access.

Unlike VPNs, which provide broad network access after authentication, ZTNA adheres to the principle of least-privilege access, characterized by:

- Applications and resources being concealed from discovery, with access granted on a per-session basis.
- Connections established only after verifying identity, context, and policy adherence.
- Access restricted to specific applications instead of entire network segments.
- Continuous verification throughout the session, not just at the initial connection.

The transition from VPNs to ZTNA marks a shift from perimeter-based security to application-level security. In ZTNA, the connection itself is never inherently trusted; users and devices must undergo rigorous authentication and authorization for each access request, regardless of location.

By employing ZTNA along with advanced measures like geo-fencing, adaptive authentication, and continuous authorization, organizations can effectively manage and secure access based on location while maintaining a robust security posture that aligns with Zero Trust principles.

When?

Time of Access

The fourth question, "When?" considers the timing of the access request. Unusual access times can serve as a red flag, indicating potentially unauthorized attempts to access resources. For instance, if an employee who typically accesses data during business hours suddenly attempts to log in at midnight, this anomaly could trigger alerts and warrant further investigation.

Incorporating time as a contextual factor enhances an organization's ability to detect and respond to suspicious activities. Anomaly detection systems can automate responses to abnormal behavior, allowing for quicker identification and remediation of potential threats.

Machine learning plays a crucial role in establishing and monitoring normal access patterns:

Baseline Patterns
ML algorithms analyze historical access data to establish baseline patterns for individual users or groups.

Detecting Anomalies
These systems can detect subtle anomalies that might not be apparent to human observers, such as slight shifts in access times or unusual sequences of resource access.

Automated Responses
Upon detecting anomalies, the system can trigger additional authentication steps or alert security teams for manual review.

By leveraging time as a key contextual factor and utilizing machine learning to monitor access patterns, organizations can proactively identify and address potential security threats, thereby strengthening their security posture.

Why?

Purpose of Access

The fifth question, "Why?" dives into the intent behind the access request.

Understanding the purpose of access can provide critical insights into the legitimacy of a request. Is the user accessing data for a legitimate business need, or are they attempting to exploit vulnerabilities?

Behavior analytics can help organizations analyze patterns of user activity, providing insight into the purpose behind access requests. By evaluating the rationale behind access requests, organizations can better assess the risk involved and determine appropriate responses, whether that means approving the request or denying it.

Implementing effective behavior analytics involves key steps:

1. **Data Collection:** Gather comprehensive logs of user activities, including login times, accessed resources, and performed actions.
2. **Pattern Establishment:** Use machine learning algorithms to establish baseline behavior patterns for individual users or user groups.
3. **Real-time Analysis:** Continuously monitor user activities and compare them against established baselines.
4. **Risk Scoring:** Assign risk scores to activities based on their deviation from normal patterns.
5. **Automated Response:** Implement automated responses for different risk levels, such as requiring additional authentication or alerting security teams.
6. **Continuous Learning:** Regularly update the behavior models to account for legitimate changes in user behavior over time.

> By focusing on the “Why” and leveraging behavior analytics, organizations can gain deeper insights into user intent, allowing for more informed access control decisions and enhancing overall security.

How?

Method of Access

Finally, we consider "How?". This question examines the method by which access is being requested. Users need to be connected using a VPN/ZTNA but if their device is compromised, the attacker can ride the secure network into the environment. By analyzing the access method, organizations can enforce security policies that adapt based on device compliance and connection security.

Endpoint Detection and Response (EDR) solutions can be used to check if a device is up-to-date on patches, antivirus status, or other security measures. Devices that fail these security checks might be denied access or redirected to a remediation process, ensuring that both the user and their device meet security requirements before granting access.

Encryption is essential in securing access methods:

Data Encryption
All data in transit should be encrypted using strong protocols (e.g., TLS 1.3) to protect against interception.

End-to-End Encryption
Implement end-to-end encryption for highly sensitive data to ensure it remains encrypted even during processing on servers.

Encryption Key Management
Proper management of encryption keys is vital to maintaining the integrity and security of encrypted data.

By looking over the "How" of access requests and employing technologies like EDR and encryption, organizations can ensure that access methods are secure, further reducing vulnerabilities and enhancing their overall security posture.

The Power of Context in Zero Trust

In the Zero Trust security model, context is not just an important consideration—it is essential for making informed, effective security decisions.

By applying the concept of **the Kipling method**, organizations can systematically evaluate access requests, enhancing their security posture and reducing risk. The interplay of who, what, where, when, why, and how creates a comprehensive understanding of each request, enabling a nuanced approach to security that is proactive rather than reactive.

By embracing the contextual, adaptive security approach of Zero Trust, organizations can better protect their assets, empower their workforce, and confidently navigate the complexities of the modern digital landscape.

To learn more about implementing Zero Trust, explore additional insights and reach out to the Stratascale team.

stratascale

CYBERSECURITY DIVISION OF SHI

You Partner in Success

Stratascale is a purpose-built cybersecurity services company delivering strategy and solutions to the Fortune 1000, and beyond. Using deep domain expertise and a results-oriented approach, we partner with ambitious security leaders to fortify their defenses and increase cyber resiliency.

stratascale.com