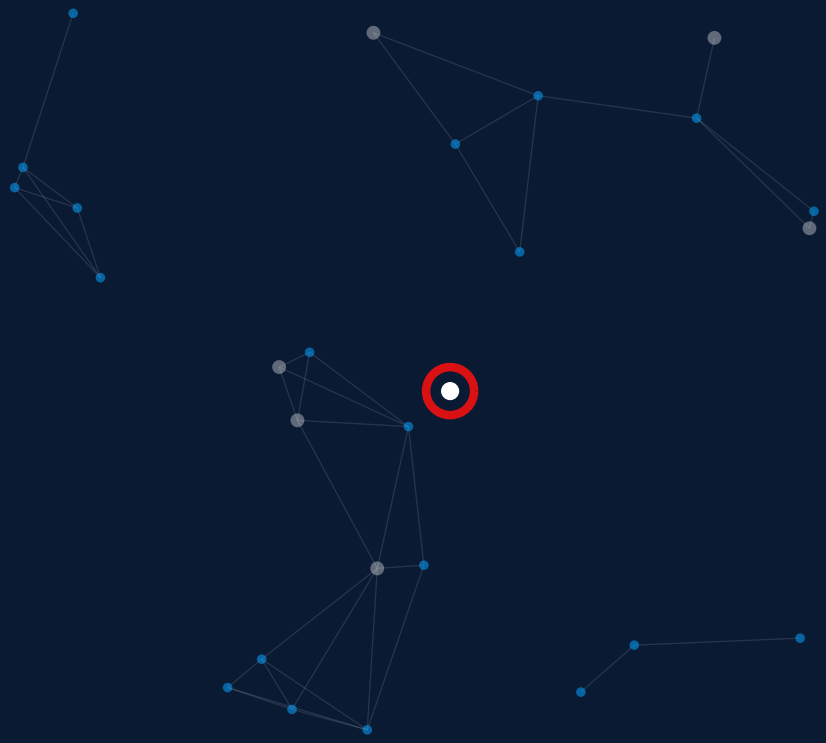
KRYNTHNODE



Cybersecurity and digital risk | Report

Zero trust beyond the perimeter

A maturity path for mid-size enterprises

Published 4 August 2026
Krynthnode Research and Advisory LLP | krynthnode.com

Research that shows its working.

Executive summary

Zero trust has moved from a slogan to the expected security model for organisations of every size. Yet most published guidance assumes the resources of a large enterprise or government agency: dedicated architecture teams, multi-year budgets and a mature identity platform. Mid-size enterprises in India, typically with a security team of fewer than ten people, need a different path.

This report sets out a four-stage maturity path that starts with the controls that reduce the most risk for the least cost, and defers the expensive, complex work of network micro-segmentation until the foundations are in place. It aligns with NIST Special Publication 800-207 and the CISA Zero Trust Maturity Model, and maps each stage to obligations Indian organisations already carry under CERT-In's 2022 directions and the Digital Personal Data Protection Act.

Key findings	Confidence
Identity is the most effective starting point. Consolidating identity providers and enforcing strong multi-factor authentication addresses the credential-based attacks behind a large share of breaches, at lower cost and disruption than network redesign.	High confidence
Asset and device inventories are usually less complete than organisations believe, and access decisions based on device health are only as reliable as that inventory.	Moderate confidence
Managed detection and response services can close the skills gap for smaller security teams, but only when escalation ownership and permitted actions are agreed in advance.	High confidence
Organisations that treat zero trust as a single product purchase rarely reach the later maturity stages.	Moderate confidence

Each finding is graded in the Krynthnode confidence ledger. See the methodology at the end of this report.

What we recommend

1. Consolidate to one authoritative identity provider and require phishing-resistant multi-factor authentication for administrators and remote access first.
2. Reconcile your device inventory against network and endpoint data before using device posture in access decisions.
3. Put application-level access controls in front of your most critical systems before attempting network micro-segmentation.
4. Define measurable exit criteria for each maturity stage and report progress to the board twice a year.

© 2026 Krynthnode Research and Advisory LLP. All rights reserved.

Why the perimeter no longer protects you

Traditional network security assumed a trusted inside and an untrusted outside. Hybrid work, software-as-a-service applications, cloud infrastructure and third-party access have dissolved that boundary. Users connect from anywhere, data lives in many places, and suppliers hold credentials to internal systems.

Zero trust replaces location-based trust with continuous verification. NIST SP 800-207 describes it as a set of principles in which no implicit trust is granted to assets or user accounts based solely on their physical or network location. Every access request is evaluated on the identity of the requester, the health of the device, and the sensitivity of the resource.

For a mid-size organisation, the practical question is not whether to adopt zero trust, but in what order to build it so that each step delivers measurable risk reduction.

The four-stage maturity path

The path below adapts the five pillars of the CISA Zero Trust Maturity Model (identity, devices, networks, applications and workloads, and data) into a sequence that fits the budgets and staffing of mid-size enterprises.

Stage	Focus	Typical duration	Exit criteria
1. Foundation	Single identity provider; MFA for all users; privileged accounts vaulted	3 to 6 months	No shared admin accounts; MFA coverage above 95% of users
2. Visibility	Device inventory; endpoint detection on all managed devices; central logging	3 to 6 months	Inventory reconciled; logs retained 180 days in India
3. Access	Application-level access for critical systems; device posture checks	6 to 9 months	Critical apps reachable only through policy-based access
4. Segmentation	Network micro-segmentation; data classification driving access	9 to 18 months	Lateral movement paths tested and closed

The durations are indicative. Organisations with existing identity consolidation can move faster through the first stage, while those with extensive legacy operational technology will need longer in the third and fourth.

© 2026 Krynthnode Research and Advisory LLP. All rights reserved.

Stage one: identity first

Identity delivers the fastest return because it addresses the most common attack path. Stolen or weak credentials remain a leading initial access vector in public incident reporting, and multi-factor authentication blocks the majority of automated credential attacks.

Not all multi-factor authentication is equal. CISA guidance recommends phishing-resistant methods, such as FIDO2 security keys or platform authenticators, for high-value accounts, because one-time codes sent by SMS or approved by push notification can be intercepted or socially engineered.

- Consolidate identity providers so that joiners, movers and leavers are handled in one place.
- Enforce multi-factor authentication for all users, and phishing-resistant methods for administrators, finance and remote access.
- Remove shared administrator accounts; vault privileged credentials and grant them only when needed.
- Review access rights for systems that hold personal data, since this supports DPDP Act obligations to protect that data.

Stage two: know what you are protecting

Access decisions based on device health are only as good as the inventory behind them. In practice, inventories drift: unmanaged personal devices, forgotten virtual machines and shadow cloud accounts accumulate. Before relying on device posture, reconcile the inventory against what the network and endpoint tools actually observe.

This stage also builds the logging foundation that CERT-In's 2022 directions require: logs of ICT systems maintained securely for a rolling 180 days within Indian jurisdiction, and system clocks synchronised with the time sources specified by CERT-In. Treating these as zero trust building blocks, rather than separate compliance tasks, avoids paying for the same work twice.

Stages three and four: controlling access and movement

Once identity and visibility are reliable, place application-level access controls in front of the most critical systems. Zero trust network access and secure access service edge products can replace broad VPN access with per-application policies that consider identity and device health.

Network micro-segmentation, which limits how far an attacker can move after compromising one system, is valuable but complex. It depends on understanding application dependencies, and done too early it breaks business processes. We recommend it as the final stage, informed by the visibility built in stage two.

© 2026 Krynthnode Research and Advisory LLP. All rights reserved.

Making the programme sustainable

Small teams sustain zero trust programmes by being deliberate about what they run themselves. Managed detection and response services can provide round-the-clock monitoring, but contracts must specify exactly which containment actions the provider may take without approval, who is called at night, and how quickly.

Finally, report progress in business terms. Boards respond to statements such as the proportion of critical applications protected by policy-based access, or the time to revoke a departing employee's access, far more than to lists of tools deployed.

Methodology and the confidence ledger

This report draws on the public frameworks and regulations listed in the references, applied to the operating constraints of mid-size enterprises. Findings are graded in the Krynthnode confidence ledger according to how consistently they are supported across these sources and established security practice.

Grade	What it means	How to use it
High confidence	Consistent across several independent sources and established practice.	Suitable for committing budget.
Moderate confidence	Supported, with some gaps or variation between contexts.	Suitable for a pilot with a review date.
Emerging evidence	Limited or recent evidence.	Worth monitoring before acting.

References

1. National Institute of Standards and Technology. SP 800-207, Zero Trust Architecture. August 2020.
2. Cybersecurity and Infrastructure Security Agency. Zero Trust Maturity Model, Version 2.0. April 2023.
3. Cybersecurity and Infrastructure Security Agency. Implementing Phishing-Resistant MFA (fact sheet). October 2022.
4. National Institute of Standards and Technology. SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management.
5. Indian Computer Emergency Response Team (CERT-In). Directions under sub-section (6) of section 70B of the Information Technology Act, 2000. 28 April 2022.
6. International Organization for Standardization. ISO/IEC 27001:2022, Information security management systems.

© 2026 Krynthnode Research and Advisory LLP. All rights reserved.

About Krynthnode

Krynthnode Research and Advisory LLP is an independent technology and cybersecurity research and advisory firm. We help leaders make decisions they can defend: every finding we publish carries its evidence, its sources and an honest rating of how sure we are. We do not sell technology, take referral fees or accept payment for ratings.

To discuss this research with the analyst team, visit krynthnode.com/contact or email hello@krynthnode.com.

This publication reflects the views of Krynthnode analysts based on the sources available at the time of writing. It is provided for information and is not legal, regulatory, financial or investment advice. Mention of any organisation, product or standard is not an endorsement. Trademarks belong to their respective owners. No part of this publication may be reproduced or redistributed without written permission, except for short quotations with attribution.

© 2026 Krynthnode Research and Advisory LLP. All rights reserved.