ManageEngine

Reimagine cybersecurity with Zero Trust

Begin your Zero Trust journey or plug the gaps in your existing approach with ManageEngine's cybersecurity solutions.

manageengine.com/zerotrust

Your cybersecurity approach needs an upgrade

Your attack surface is expanding

With 83% of organizations increasing their reliance on the cloud,[1] the days of a well-defined network perimeter are gone. Additionally, organization attack surfaces have been expanding with the introduction of IoT devices, hybrid work, BYOD policies, and more.

Your perimeter alone can't keep the bad guys out

The traditional perimeter-based or implicit trust models rely on firewalls and VPNs to separate legitimate users from adversaries. People within the network, whether working on-premises or connected via VPN, are trusted.

However, this approach fails to account for:

- Credential theft - The second most common cause of data breaches, credential theft also takes the longest to identify and costs organizations an average of USD 4.62 million per incident.[2]

- Insider threats - Malicious insiders make up a smaller portion of the cyberthreat pie (83% of breaches involve external actors[3]) but can still cost organizations an average of USD 4.9 million per incident.[2]

[1] Source: The 2021 Digital Readiness Survey, ManageEngine

[2] Source: Cost of a Data Breach Report 2023, IBM Security

[3] Source: 2023 Data Breach Investigations Report, Verizon

Why adopt a Zero Trust approach to security?

Zero Trust complements and enhances traditional perimeter-based security. It helps protect organizations against threats that implicit trust models can't defend against, such as credential-based attacks and malicious insiders.

Zero Trust security can also help your organization and its workforce:

- Securely work from anywhere, anytime.
- Strengthen its security posture and defend against data breaches.
- Defend against credential theft, insider threats, and other risks.
- Comply with government and industry mandates.

The Zero Trust ecosystem

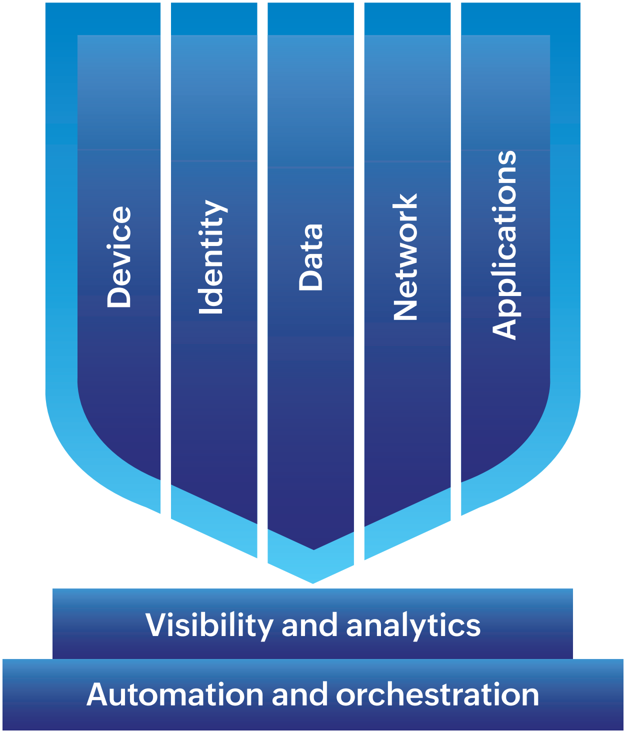
To ensure complete security you need to have processes and technology in place to secure, monitor, and manage your identities, data, endpoints, network, and applications.

Additionally, to complete your Zero Trust implementation, you also need to implement:

- Visibility and analytics solutions to get complete visibility into the network and detect potential and active threats.

- Security automation and orchestration to ensure swifter response times and ensure 24x7 protection.

The Zero Trust eXtended ecosystem and the five pillars of Zero Trust security


Device

Identity

Data

Network

Applications

Visibility and analytics

Automation and orchestration

Implementing Zero Trust with ManageEngine

Zero Trust security can be implemented in many ways.

At ManageEngine, we recommend taking an identity-centric approach. Enterprises that focus on identity and device security seem to reduce security risks more quickly as per Forrester's "A Practical Guide To A Zero Trust Implementation."

Whichever approach you choose, our solutions can provide the technological foundation for your Zero Trust security model or can fill in the security gaps in your existing approach.

Our offerings

Identity security: Gain visibility into all your identities across your on-premises and cloud applications. Secure your identities with MFA, least privilege, and implement trust scoring and policy-based access controls (PBAC) for real-time threat mitigation.

Our identity security offerings:

AD360: Manage user identities and access, deploy adaptive MFA, protect privileged accounts with UBA, and ensure regulatory compliance for hybrid environments. **(On-premises)**

Identity Manager Plus: Provide users with secure, one-click access to on-premises and enterprise SaaS applications. **(Cloud)**

PAM360: Establish strict governance over privileged access pathways and prevent security risks using real-time trust scoring and policy-based access controls. **(On-premises | MSP)**

Device trust: Monitor and track the health, availability, and security status of all endpoints accessing the enterprise network. Detect and patch vulnerabilities across OSs and applications to reduce your attack surface, and remotely lock, quarantine, or wipe devices as needed.

Our endpoint security offerings:

Endpoint Central: Protect your IT infrastructure with automated patching, attack surface management, ransomware protection, and more from a single console. **(On-premises | Cloud | MSP)**

Mobile Device Manager Plus: Securely manage corporate and personally owned devices running Apple OSs, Android, Windows, and Chrome OS. **(On-premises | Cloud | MSP)**

Data security: Locate, identify, and classify sensitive files and vulnerable data across your network. Monitor all file activities in real time, prevent unauthorized actions on sensitive data, and detect and shutdown ransomware attacks with automated threat responses.

Our data security offerings:

DataSecurity Plus: Audit file changes, analyze file storage and security, discover and classify sensitive data, monitor web traffic, and prevent data leaks. **(On-premises)**

Endpoint DLP Plus: Automate the discovery and classification of sensitive endpoint data and enforce rules for secure usage and transfer. **(On-premises)**

Network security: Monitor your network and servers in real time to detect rogue devices and network misconfigurations. Carry out network forensic analysis to detect threats or attacks, and back up network configurations for quick disaster recovery.

Our network security offerings:

OpManager Plus: Manage and monitor your network devices, servers, storage, and applications and optimize network performance from a single console. (On-premises)

NetFlow Analyzer: Get holistic visibility into your network traffic and bandwidth utilization, perform network forensics, and secure your network with advanced security analytics. (On-premises)

Network Configuration Manager: Take full control over your network configurations and automate configuration backups. (On-premises)

Security analytics and automation (SIEM and SOAR): Analyze network activity and sync data from threat intelligence services to detect and mitigate cyberattacks. Use AI-based user and entity behavior analytics to detect insider threats and account compromise, and automate your incident response with predefined and custom workflows.

Our SIEM and SOAR solutions:

Log360: Equip your SOC with deeper visibility into security events, accelerate threat detection and response, enhance your network security posture, and ensure compliance. (On-premises | Cloud | MSSP)

Cloud Security Plus: Spot and neutralize threats across AWS, Azure, GCP, and other IaaS, SaaS, and PaaS solutions. (On-premises)

About ManageEngine

ManageEngine crafts the industry’s broadest suite of IT management software. We have everything you need—over 60 products—to manage all of your IT operations, from networks and servers to applications, service desk, Active Directory, security, desktops, and mobile devices.

Since 2002, IT teams like yours have turned to us for affordable, feature-rich software that’s easy to use.

As you prepare for the IT management challenges ahead, we’ll lead the way with new solutions, contextual integrations, and other advances that can only come from a company singularly dedicated to its customers. And as a division of Zoho Corporation, we’ll continue pushing for the tight business-IT alignment you’ll need to seize opportunities in the future.

Scan this QR code to learn more about securing your business with Zero Trust security

ManageEngine
a division of **Zoho** Corp.