

Taking a Zero Trust approach: Key takeaways from the DoD's latest roadmap



Debanjali Ghosh
Technical Evangelist
ManageEngine

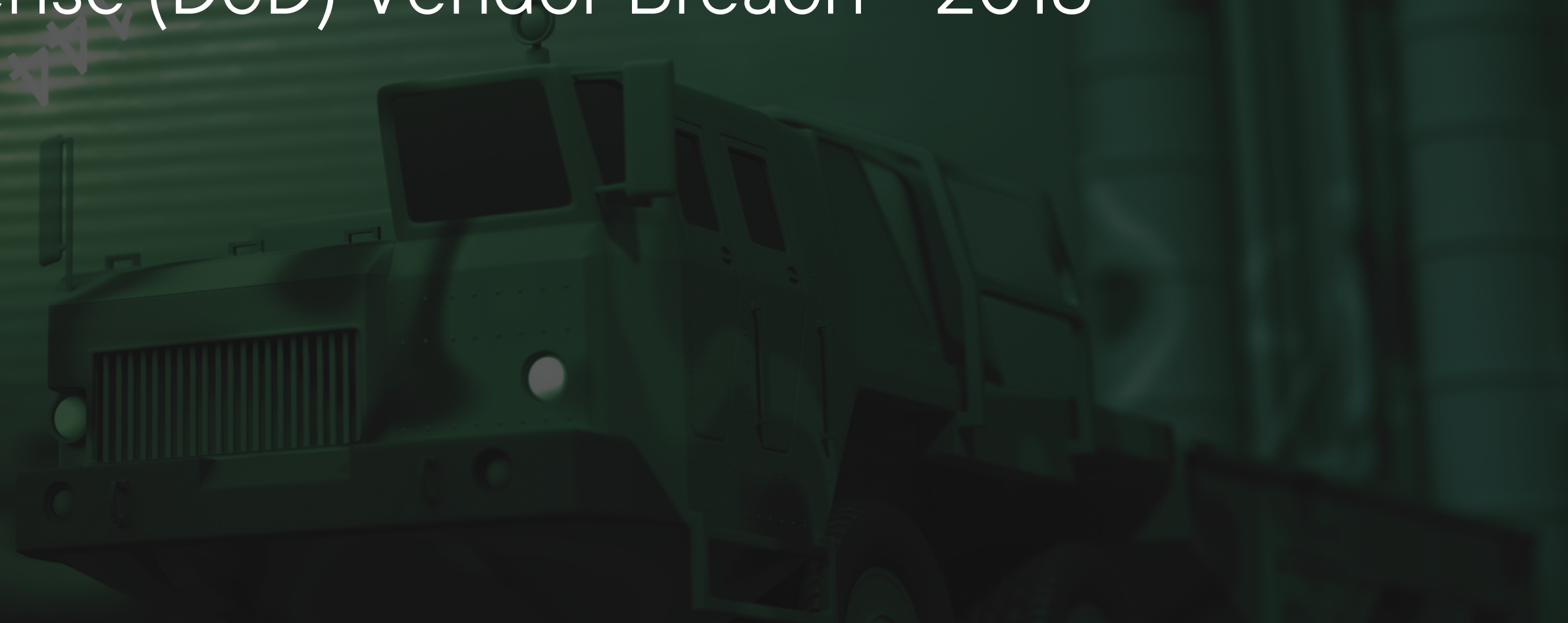
Agenda

- Increasing incidents of data leaks in the defense sector
- An overview of the DoD Zero Trust strategy
- Strategic goals, objectives, and pillars
- Implementing Zero Trust
- How ManageEngine can help

Increasing incidents of data breaches in the defense sector

Leaked Pentagon documents - 2023

Department of Defense (DoD) Vendor Breach - 2018



What is the DoD Zero Trust strategy?

The US Department of Defense (DoD) released the DoD Zero Trust strategy in October 2022.

Plans to implement it by FY 2027.

Integrates Zero Trust principles into five key cybersecurity functions: Identify, Protect, Detect, Respond, and Recover.

Plan of action

7 pillars

4 strategic goals

45 capabilities



Pillars of Zero Trust



User



Devices



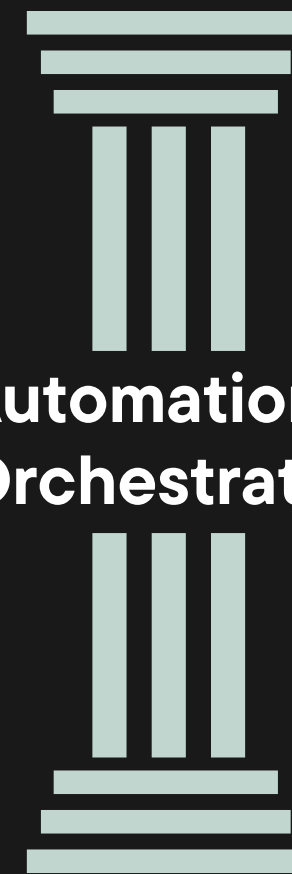
**Applications &
Workloads**



Data



**Network &
Environment**



**Automation &
Orchestration**



**Visibility &
Analytics**

Strategic Goals

**Zero Trust
Cultural Adoption**

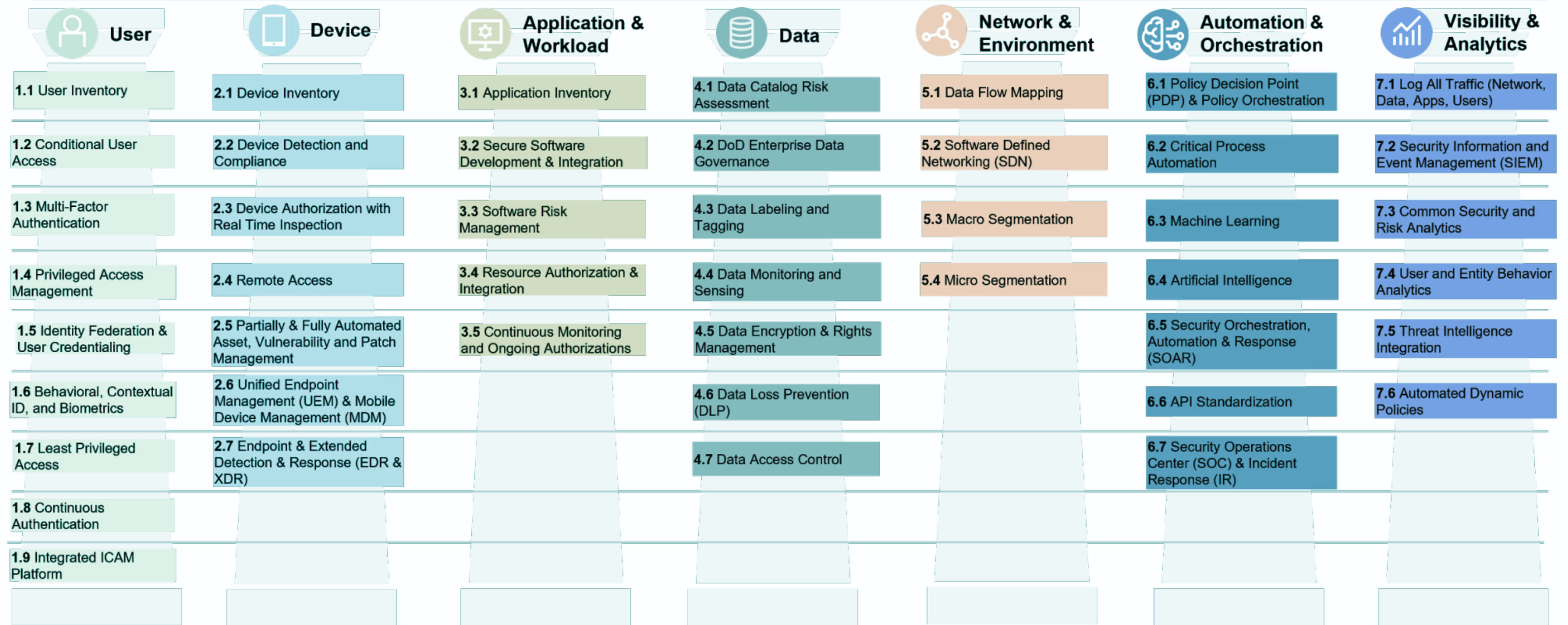
**DoD Information
Systems Secured
and Defended**

**Technology
Acceleration**

**Zero Trust
Enablement**

Capabilities

DoD Zero Trust Capabilities



EXECUTION ENABLERS



Doctrine



Organization



Training



material



Leadership



Personnel



Facilities

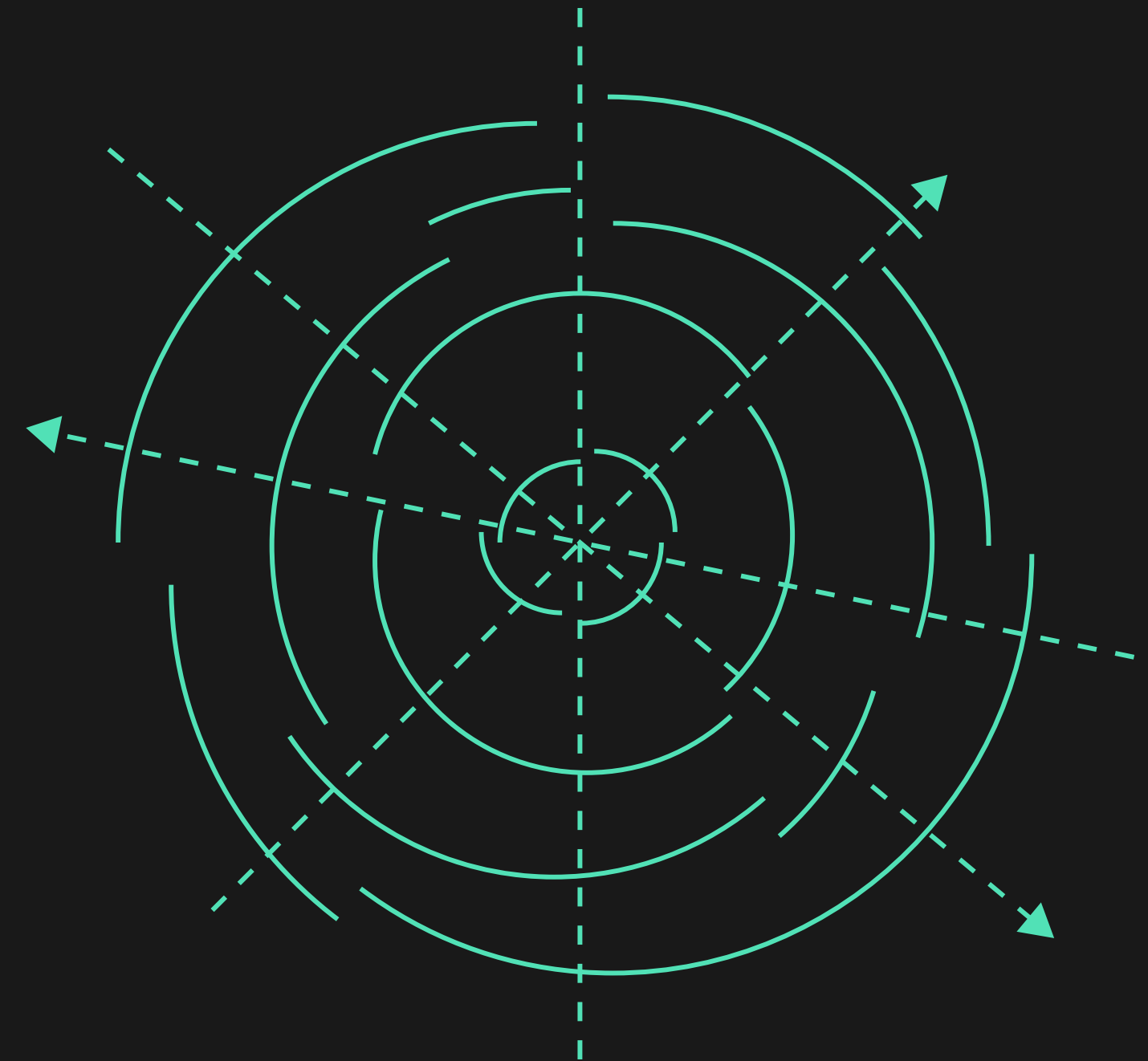


Policy

Zero Trust: never trust, always verify.

Prevent unauthorized access to data, services, and applications.

Make access control and security decisions as granular as possible to ensure least privilege.



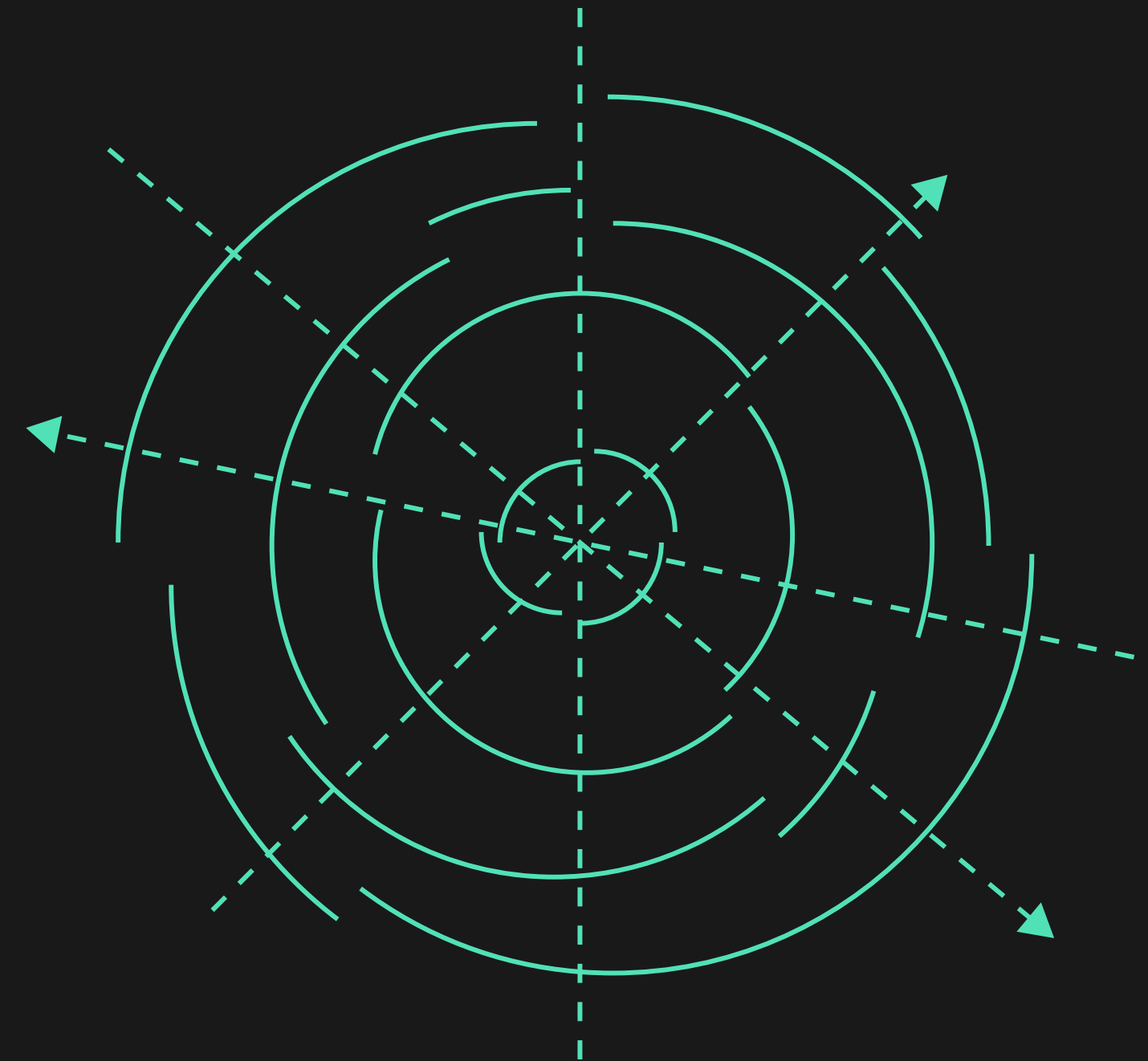
Why Zero Trust?

Secures hybrid ecosystems

Finegrained visibility

Timely incident response

Minimizing privileged credential abuse



Implementing Zero Trust

Microsegmentation

Least privileged access

Multi-factor
Authentication

Continuous monitoring

How ManageEngine can help

Multi-factor authentication

Least privileged access

Data loss prevention (DLP)

Security information and event management (SIEM)

User entity and behavior analytics (UEBA)

Threat intelligence integration

Adaptive authentication

AD360 performs risk-based adaptive authentication for tighter security and access control.

Employs multi-factor authentication (MFA) to provide an additional layer of security.

Provides single sign-on (SSO), which helps reduce the attack surface.

Least privileged access

AD360 provides role-based access control, which uses the principle of least privilege to enforce granular control.

Empowers users to perform any combination of administrative tasks with custom roles.

Allows organizations to restrict employees from performing actions beyond their scope.

Security information and event management (SIEM)

Log360 collects log data from various sources across the network.

Tracks the changes made by privileged users and detects suspicious or anomalous behavior.

Performs real-time change auditing of activities across the network.

User entity and behavior analytics (UEBA)

Leverages machine learning algorithms to create a baseline of normal behavior of humans and other entities.

A deviation from this baseline denotes an anomaly.

Employs score-based risk assessment to flag high risk events.

Data loss prevention (DLP)

Monitor access to sensitive information stored in your network and ensure data protection.

Log360 monitors access to sensitive information and provides real time alerts whenever an unauthorized access request is raised.

Helps store critical files and ensures the integrity of stored files.

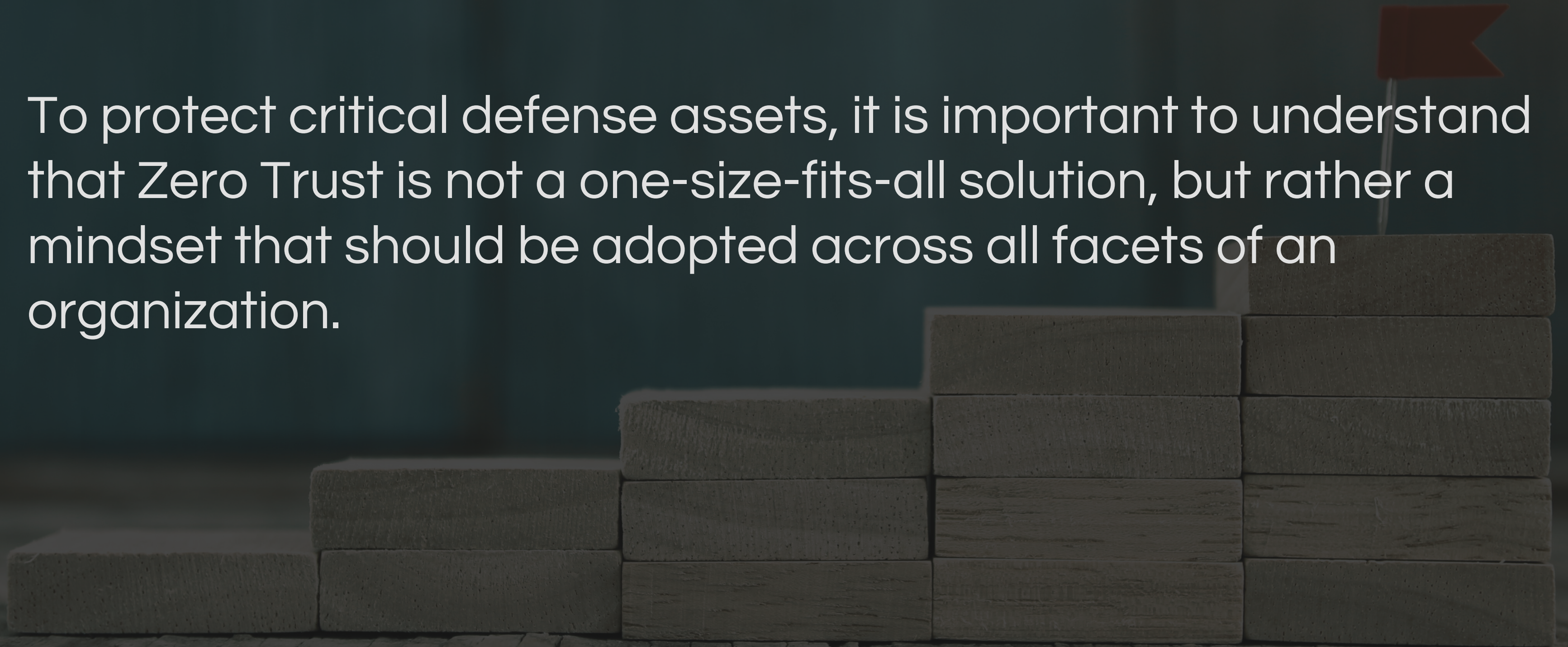
Threat intelligence integration

Log360 leverages advanced threat analytics to detect communications with external malicious sources.

Correlates data from external threat feeds to flag suspicious sources.

Helps automate incident response to threats.

To protect critical defense assets, it is important to understand that Zero Trust is not a one-size-fits-all solution, but rather a mindset that should be adopted across all facets of an organization.



Thank you.

Write to me for a consultation.

 debs@manageengine.com