

Delivering Secure Observability Workflows in Zero Trust Architecture Environments

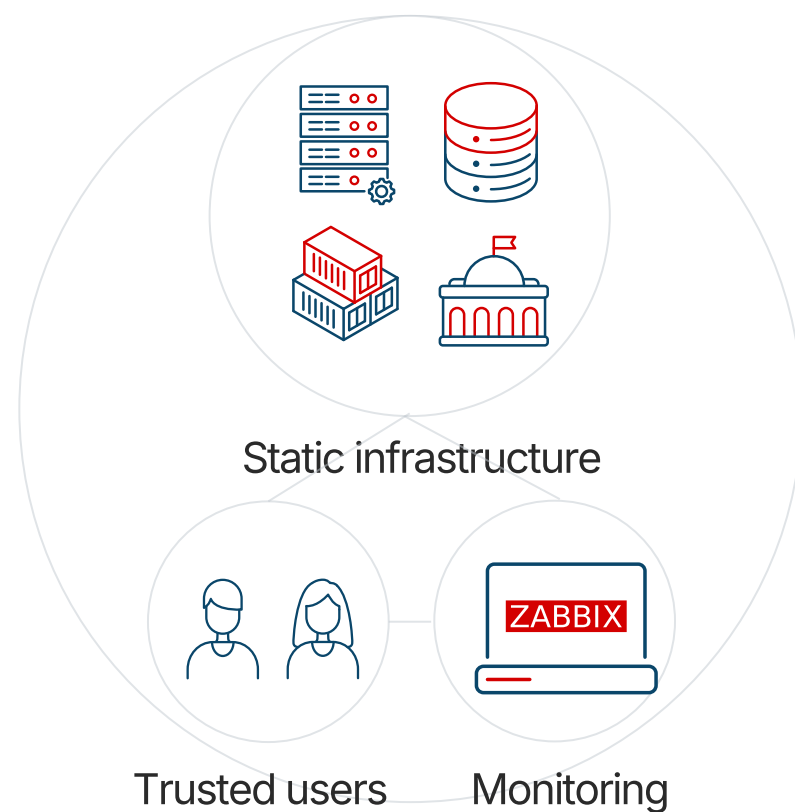
Aleksandrs Petrovs-Gavrilovs, Senior Trainer and Engineer, Zabbix SIA



The Zero Trust Observability Challenge

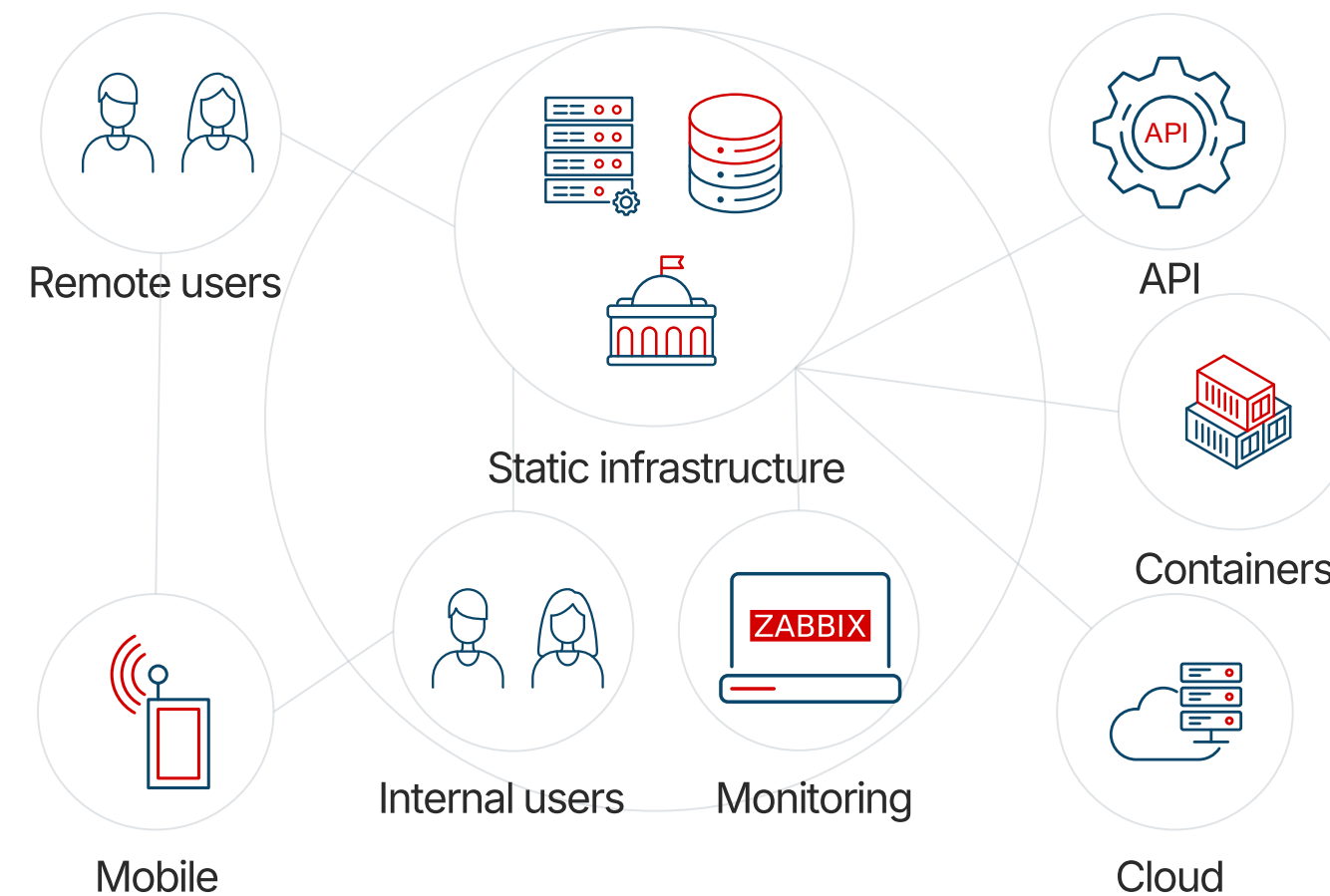


Observability changes with the times



Traditional environment

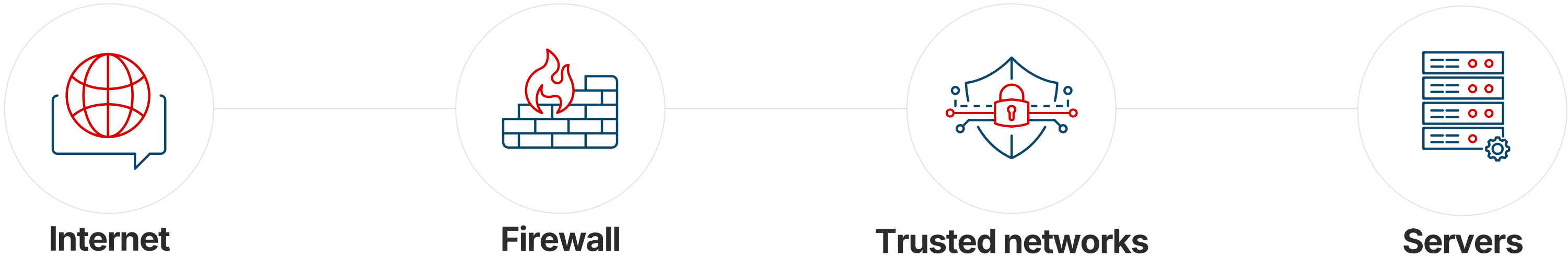
Everything is transparent and secluded



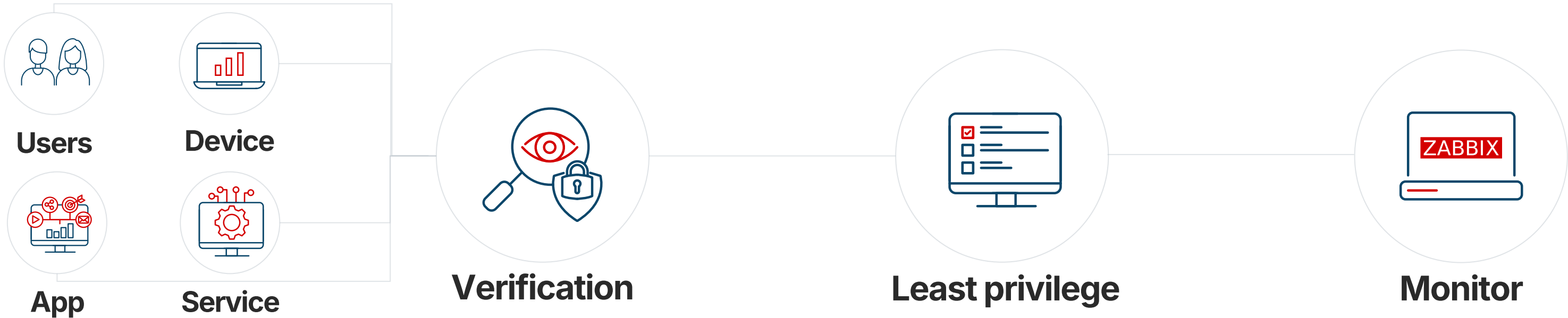
Modern environment

Varieties of different access types from different networks

From traditional



To Zero Trust



Using Zabbix to continuously observe, verify and respond



Infrastructure

Servers, networks, applications, cloud resources, and other systems being monitored.



Zabbix

Collects telemetry, detects issues, correlates events, and provides observability data.



Security/SOC

Analyzes security-related events, investigates incidents, and coordinates security response.



Operators

Use alerts and dashboards to monitor the environment, investigate problems, take action.

The Zero Trust Principles

Zabbix isn't an identity provider or a firewall,
but observability supports Zero Trust by providing visibility into the state and behavior of monitored environment.

VERIFY EXPLICITLY

Identity, device, application and context

LEAST PRIVILEGE

Provide only the access required

ASSUME BREACH

Continuously monitor and limit impact when
required

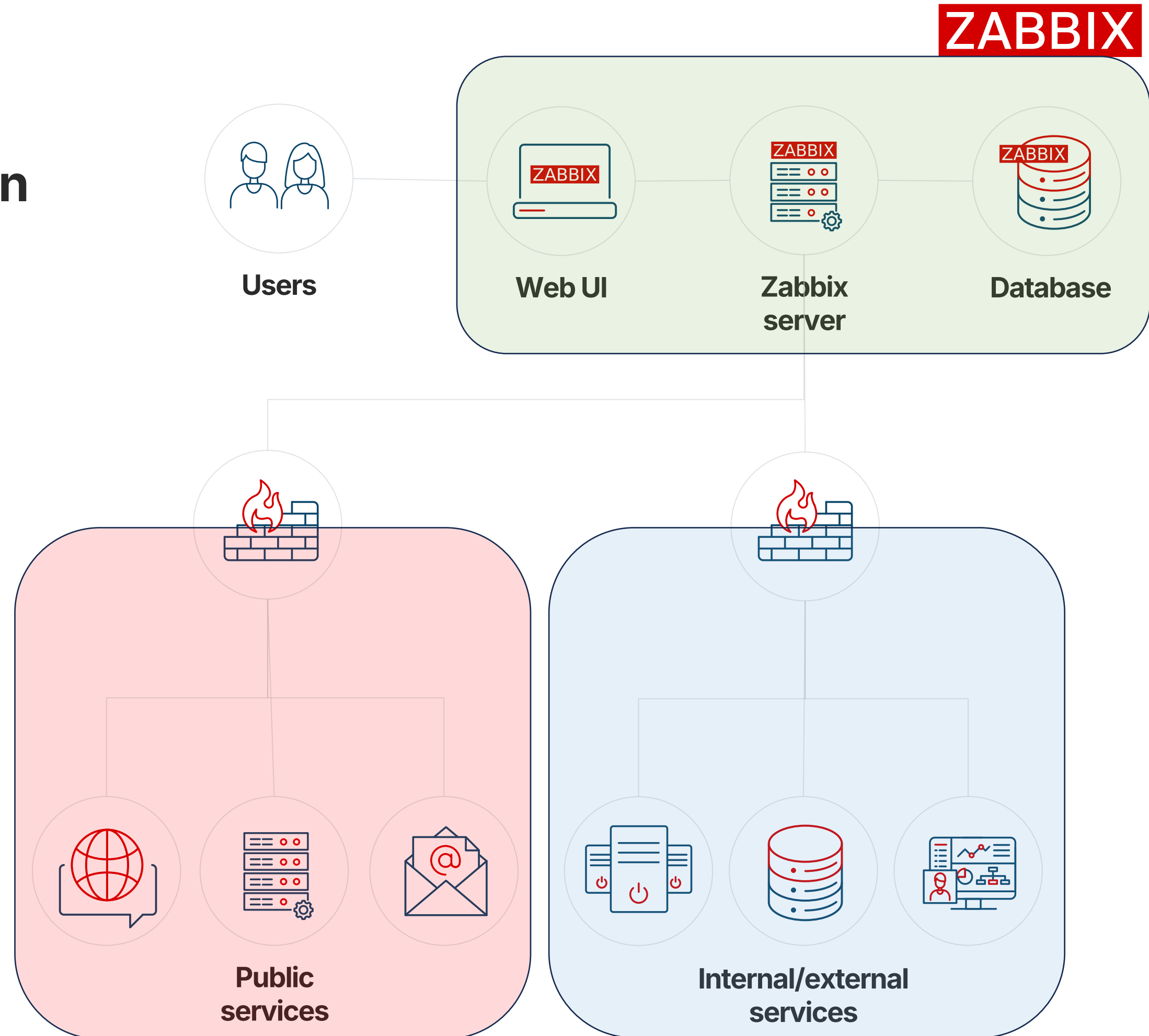
Building a Secure Observability Foundation



Zero trust network segmentation

Zero Trust network segmentation is a cybersecurity strategy that divides a network into smaller, isolated zones and applies strict, identity-driven controls over who or what can move between them.

By containing threats to a single segment, it prevents attackers from moving laterally across the entire environment if a breach occurs.



Zabbix proxies for segmentation

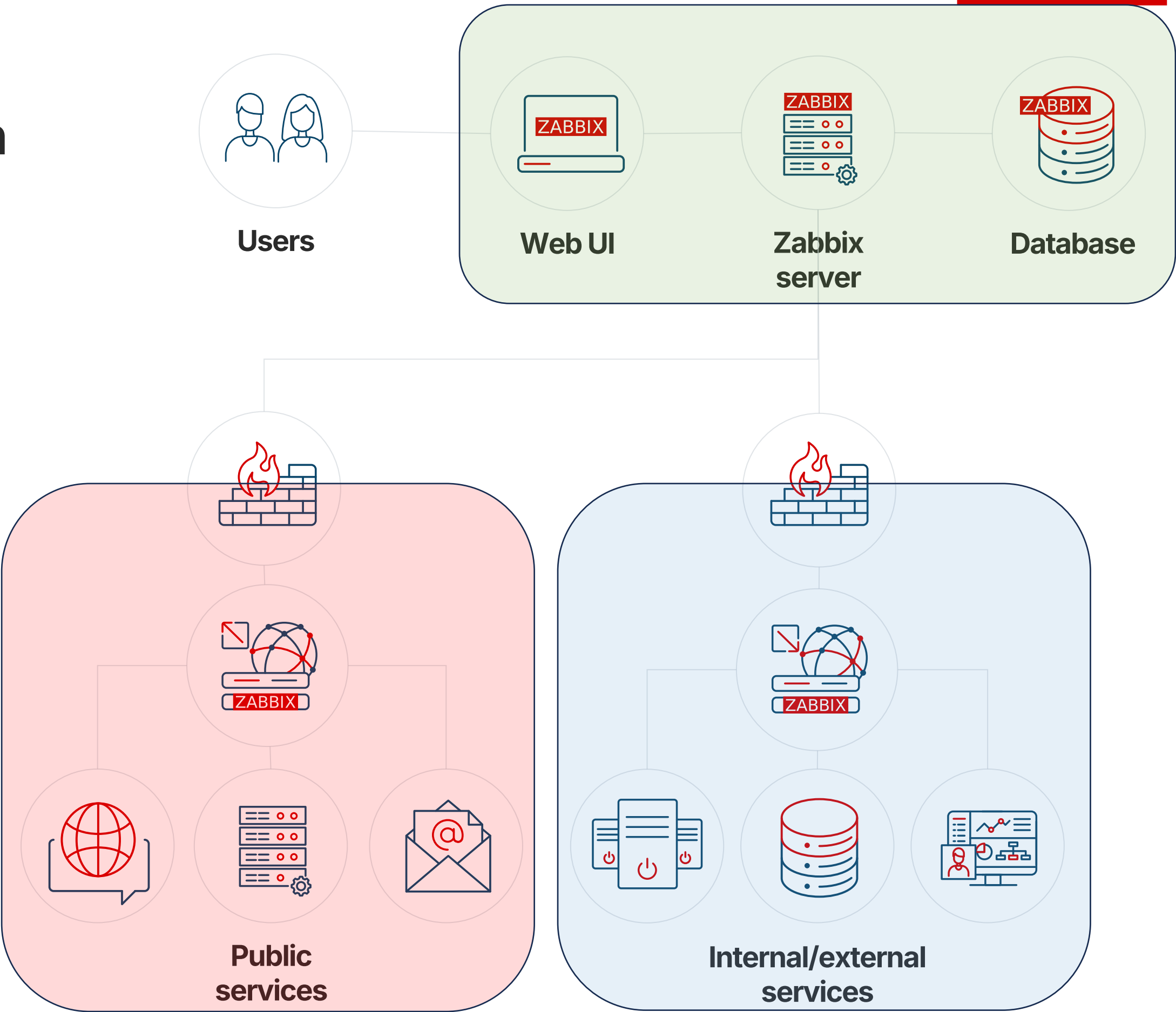
Zabbix proxies can collect monitoring data from different network segments without requiring the Zabbix server to directly connect to every monitored device.

Active Proxy

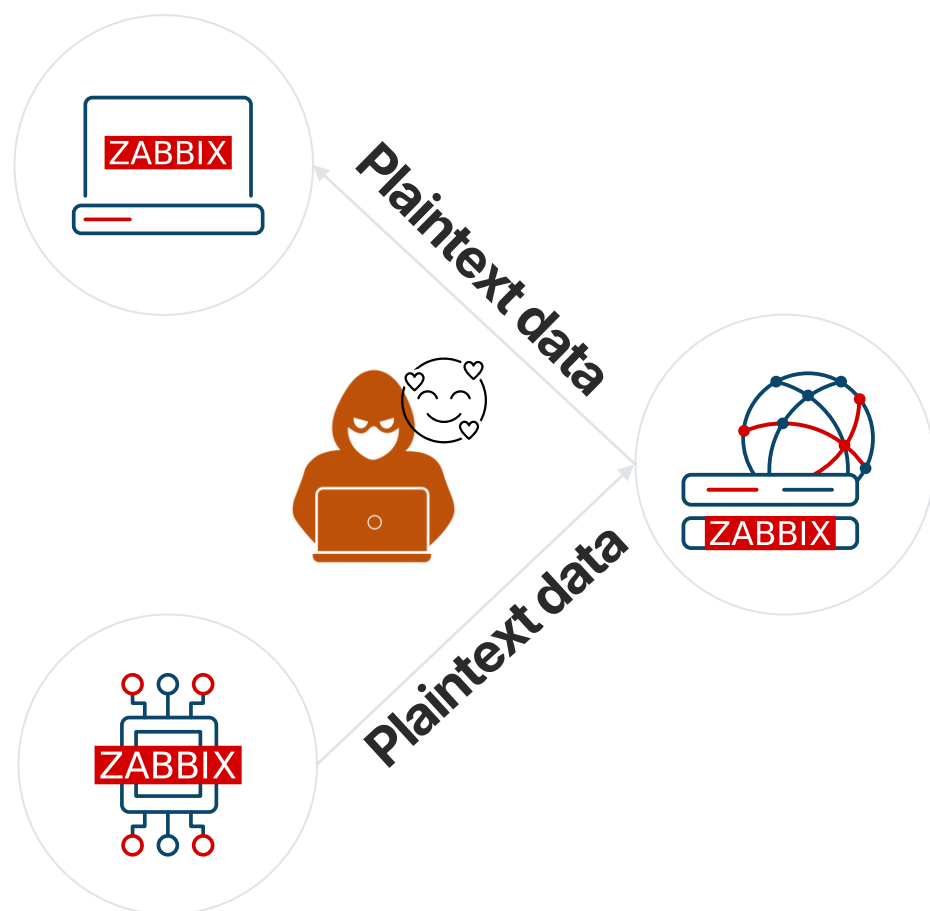
No inbound access — smaller attack surface.
 Firewall-friendly — outbound connection only.

Passive Proxy

No outbound connection — useful when restricted.
 More firewall exposure — server must reach the proxy.

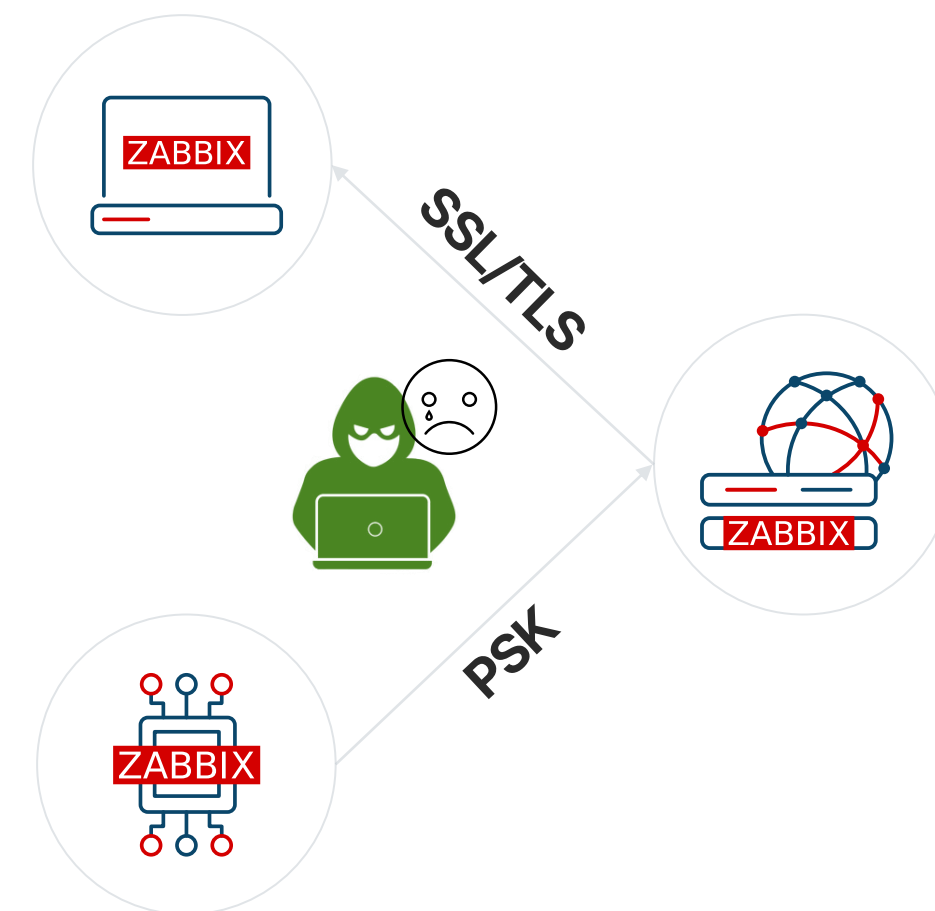


Securing the Monitoring Channel



Exchanging data as-is

Very simple to configure, easy to share with everyone, even if not willing



Encrypting data between components

Still easy to configure, data stays secure, shared between trusted members

Multiple ways to encrypt data with Zabbix

Pre-shared keys

Symmetrical. If both parties share the same PSK identity and value, the connection will proceed

SSL/TLS Certificates

Asymmetrical. Identity is verified through certificates and a trusted CA.

Mixed

Depending on environment, both PSK and SSL/TLS can be utilized

Zero trust verification principle

Zabbix components support all three wait of encryption, but SSL/TLS option allow us to verify the certificate Issuer and the Subject of components

Frontend/Server – Database

Allow encrypted only, verify issuer and subject

Frontend – Server

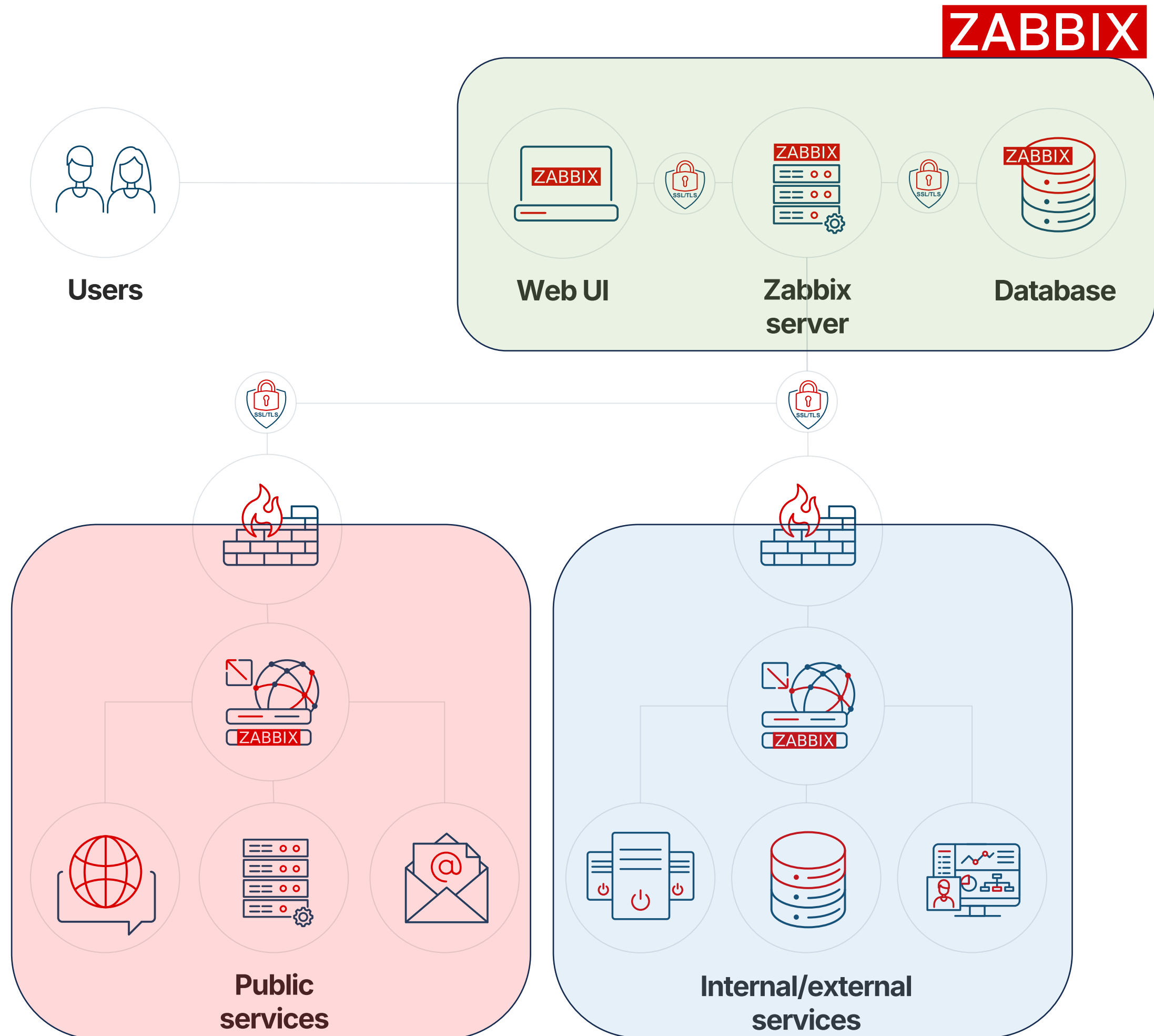
Allow encrypted only, verify issuer and subject

Server – Proxies

Allow encrypted only, verify issuer and subject

Server/Proxy – Agents

PSK can be used as well, but in that case unique PSK identities and keys should be used as much as possible



User verification

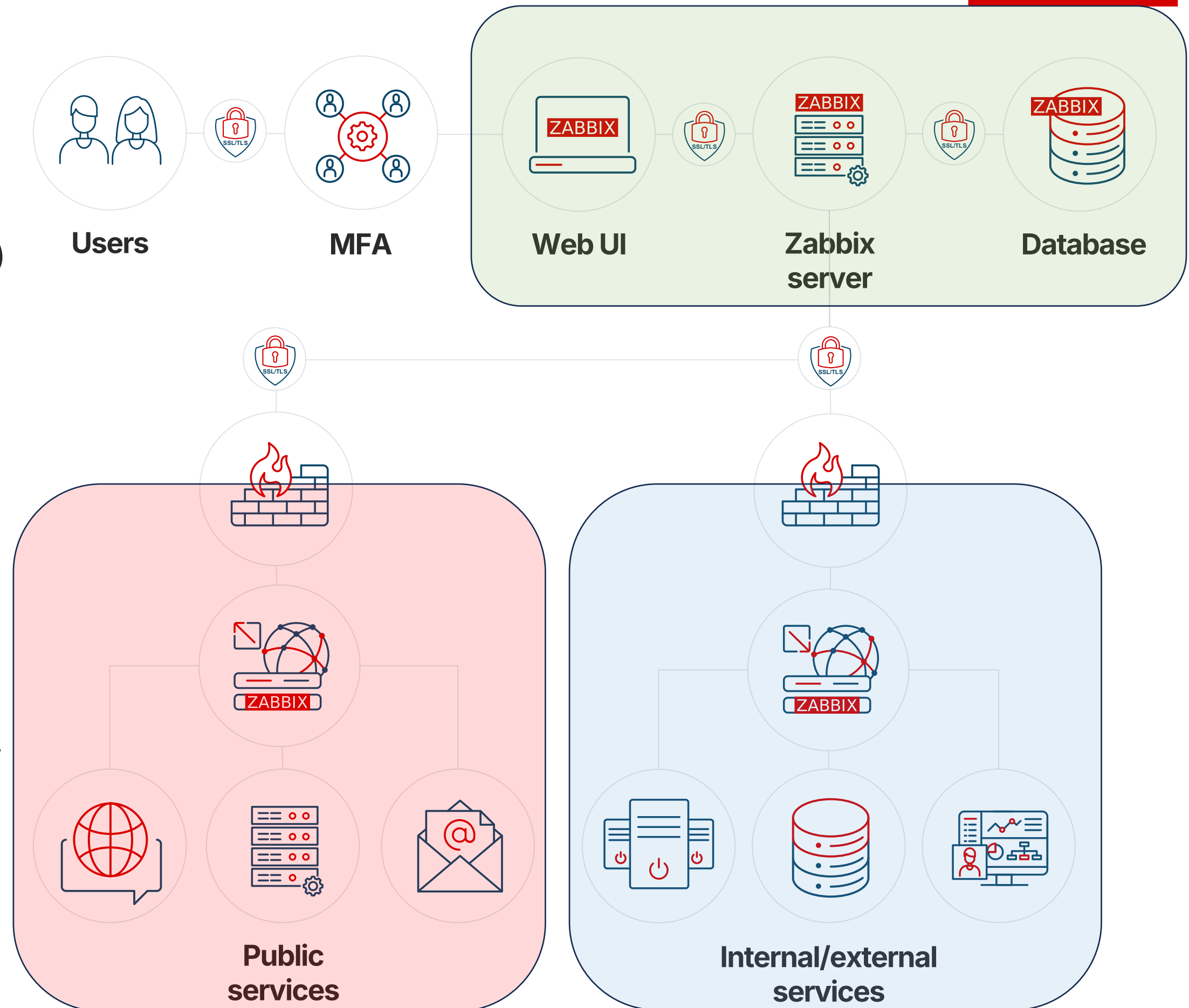
In a Zero Trust architecture, LDAP or SAML combined with Multi-Factor Authentication (MFA) are necessary to replace the traditional network security as the primary line of defense. Zabbix provides all the required options:

SAML/LDAP

Centralize identity and access policies, while SAML enables secure SSO.

MFA

Strengthens Zero Trust by requiring multiple forms of authentication before access is granted.





NOC teams

User group

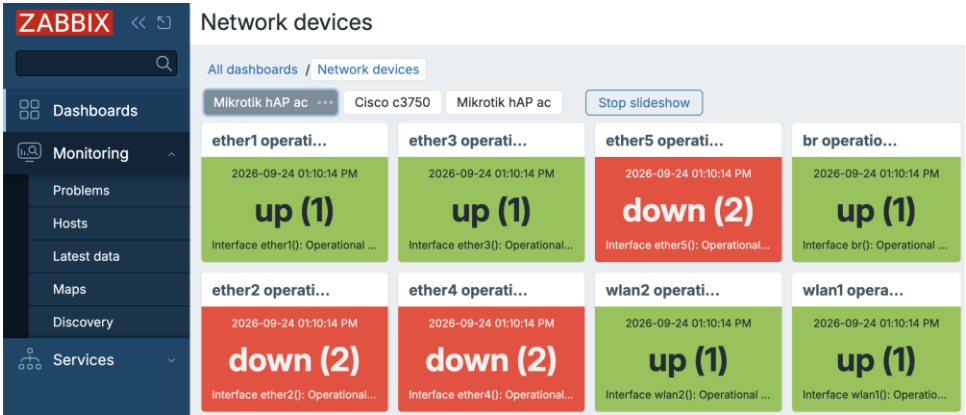
Operators

User role

User based

Access in Zabbix

- View dashboards
- Acknowledge problems
- No configuration access



Template team

User group

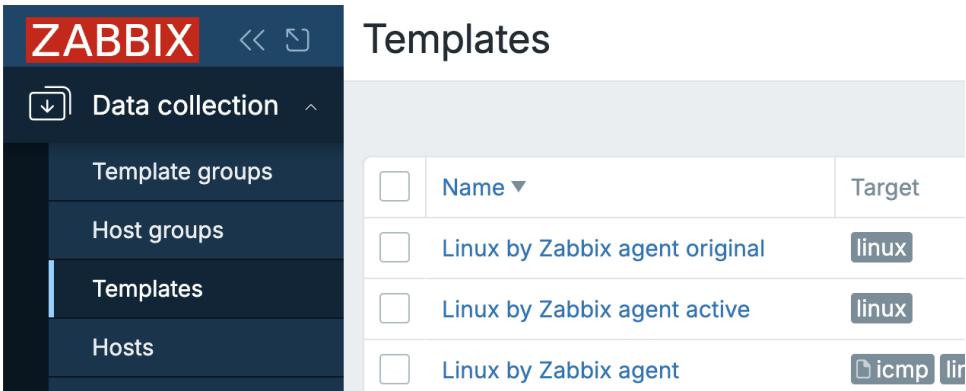
Integrators

User role

Admin based

Access in Zabbix

- Manage templates
- Created dev hosts
- Limited set of host/template groups



Zabbix administrators

User group

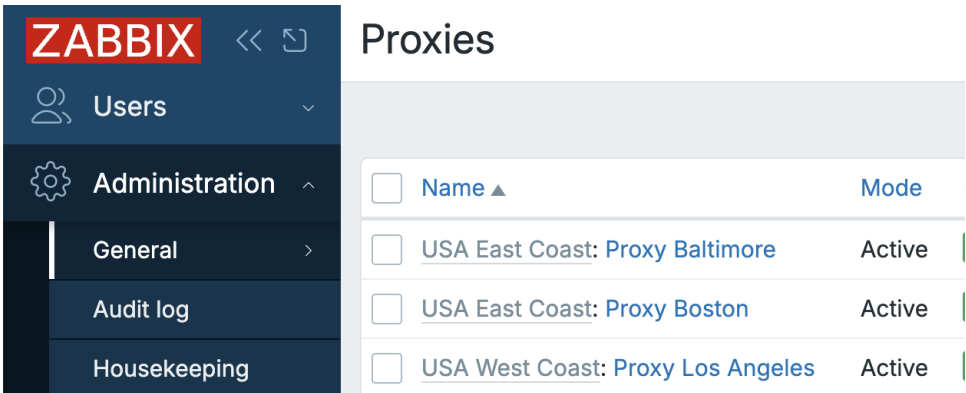
Zabbix Admins

User role

Super admin based

Access in Zabbix

- Full configuration access
- Managing other user's permissions
- Controlling infra-administration



Least privileges principle using Zabbix

Use all the extra features

Zabbix allows to enforce even stricter security using

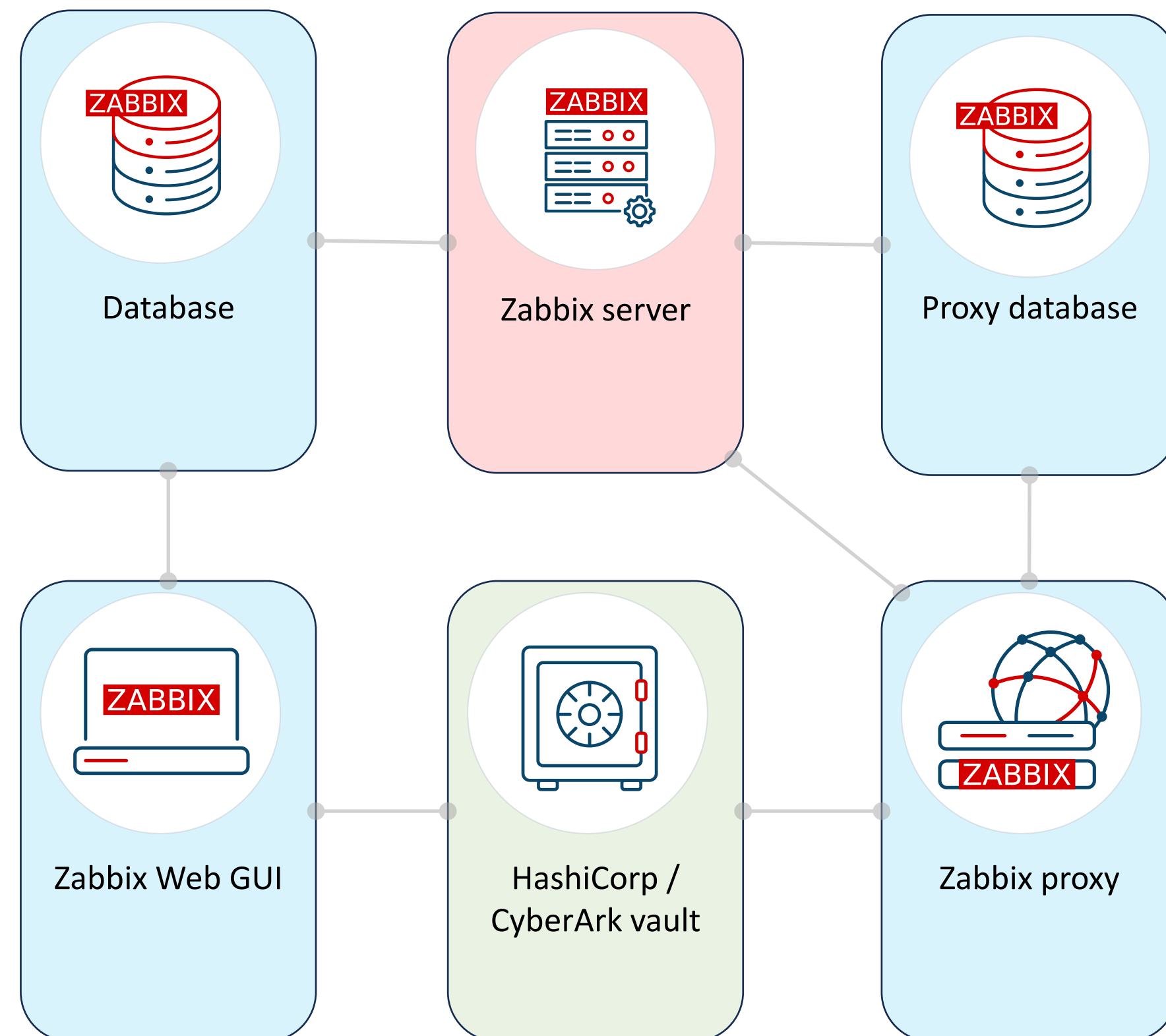
API Token only access

Allow/Deny specific checks

Secret macros

Vault storage

HashiCorp/CyberArk – extra level on secret access verification in a segmented storage



Continuous Verification Through Monitoring



Using to enforce Zero trust

Expected state

Investigate what is the expected state of behaviour of the monitored entity

Actual state

Use items to monitor the current real-time state of the entities

Compare

Triggers with items will constantly compare the state of the environment

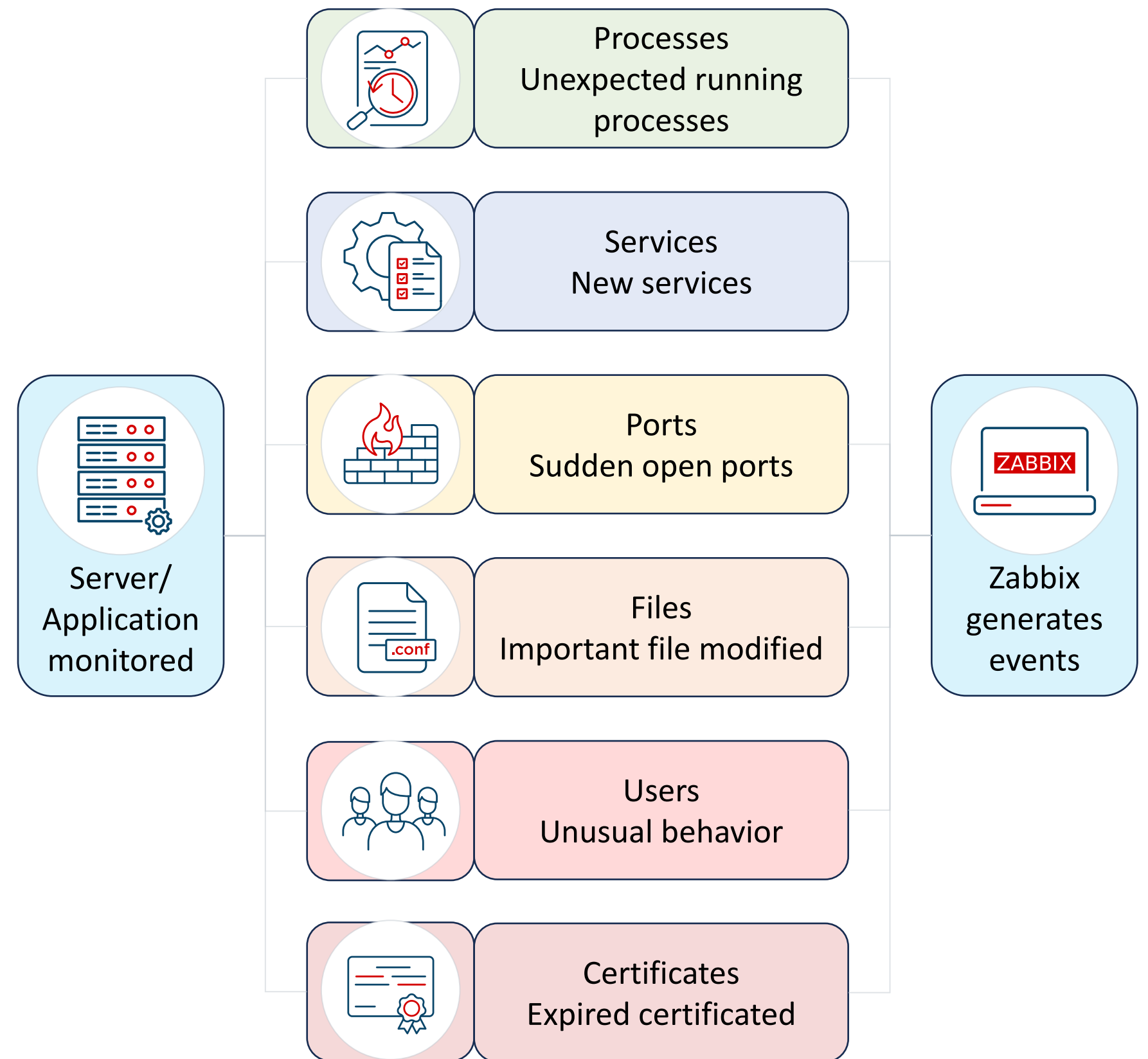
Deviation

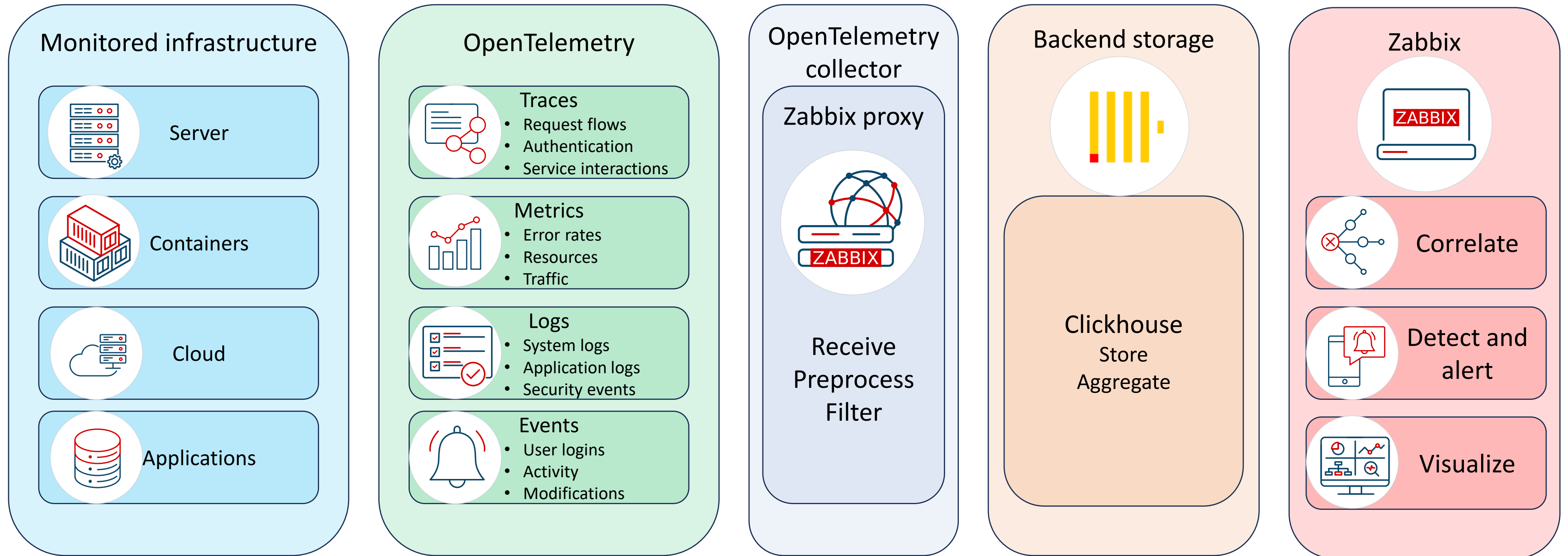
As soon as there is a deviation from expected behaviour be alerted and investigate

Observability layer

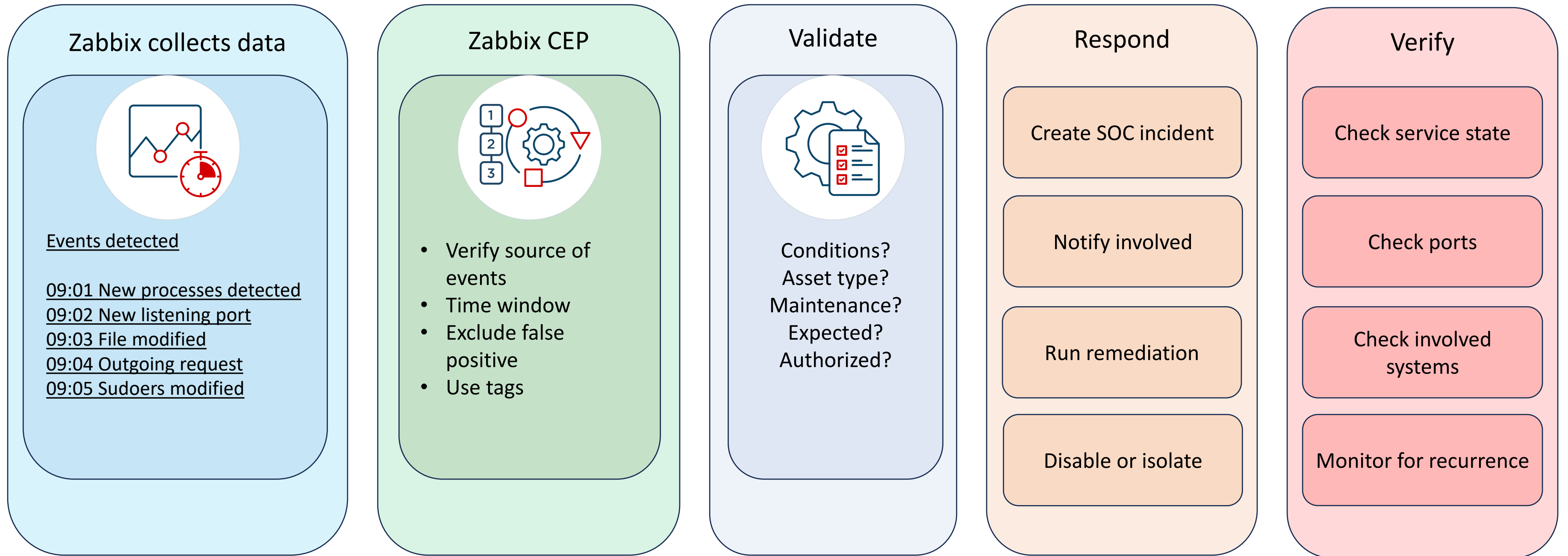
Zabbix

- Metrics
- Availability information
- Logs
- Events
- Configuration monitoring
- Application monitoring
- Network monitoring
- API-based data collection
- OTEL
- Automated actions





Extend even further with OTEL



Combine Zabbix monitoring with pro-active approach

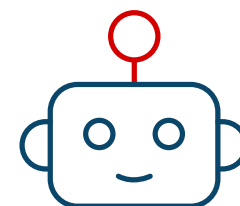
AI changes the security landscape



AI can be both

Attacker

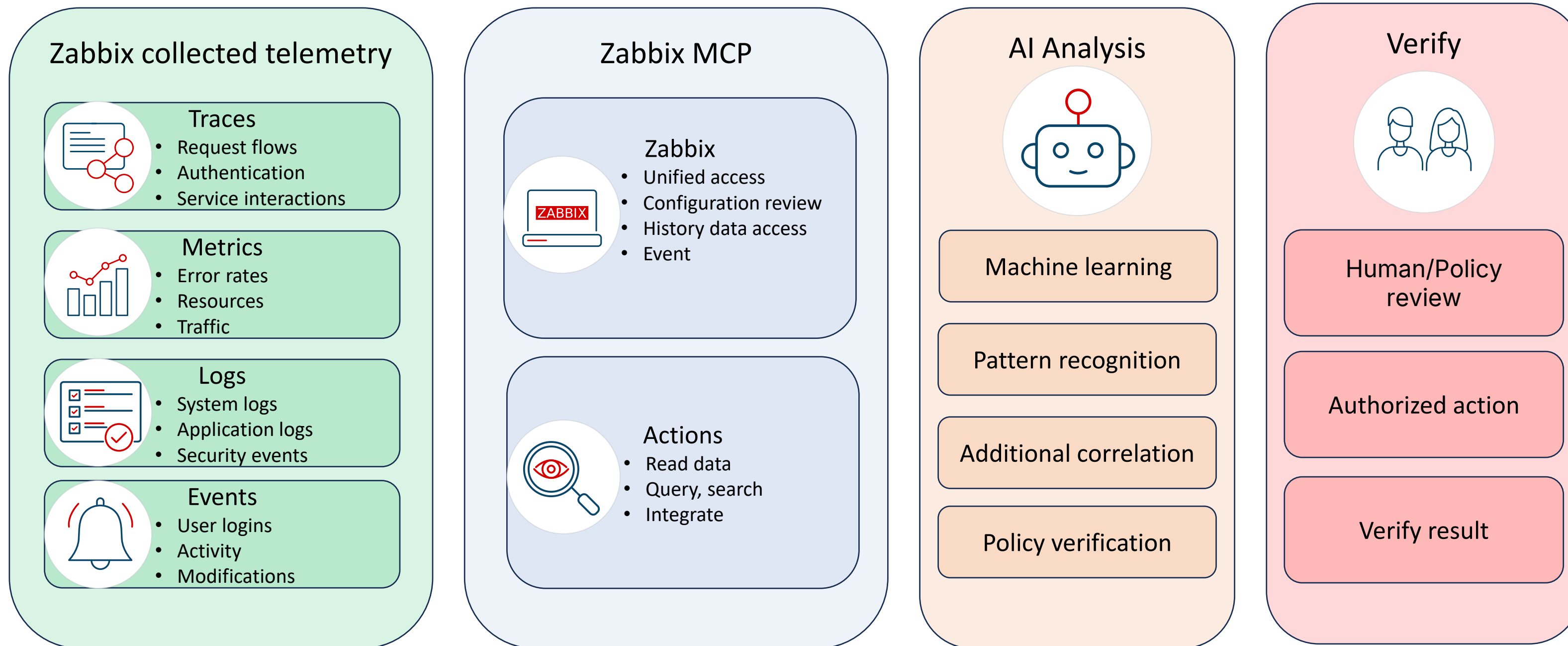
- faster reconnaissance
- automated attack attempts
 - credential attacks
- rapidly generated malicious activity
 - adaptive behavior



Defender

- analyze large volumes of telemetry
 - identify unusual behavior
 - correlate events
 - assist investigation
 - recommend actions





Use Zabbix MCP to improve security even further
AI assists the decision process, but does not perform automated actions

Extending to Mobile

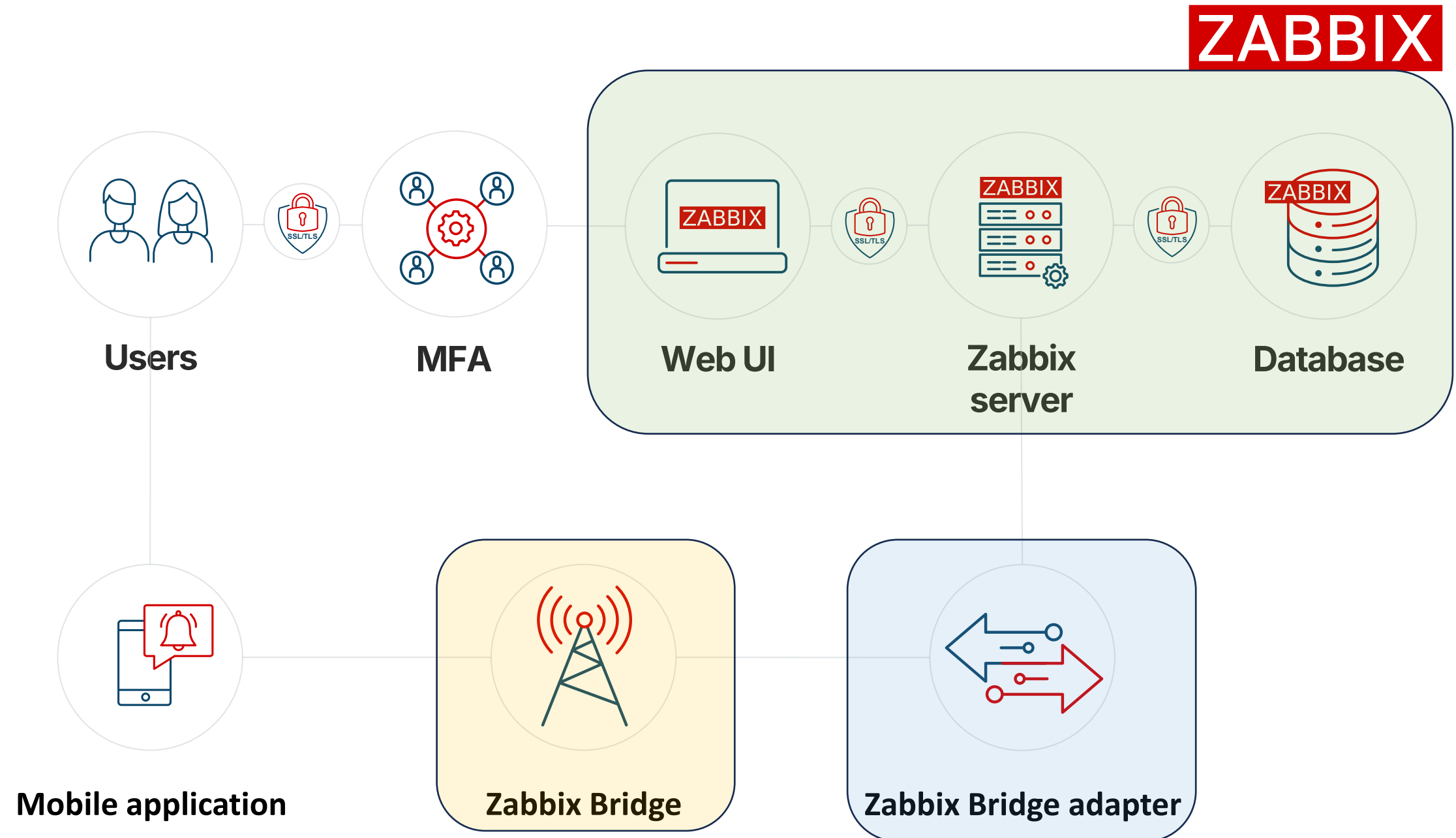


Bridge security

Make sure the bridge is segmented by the network

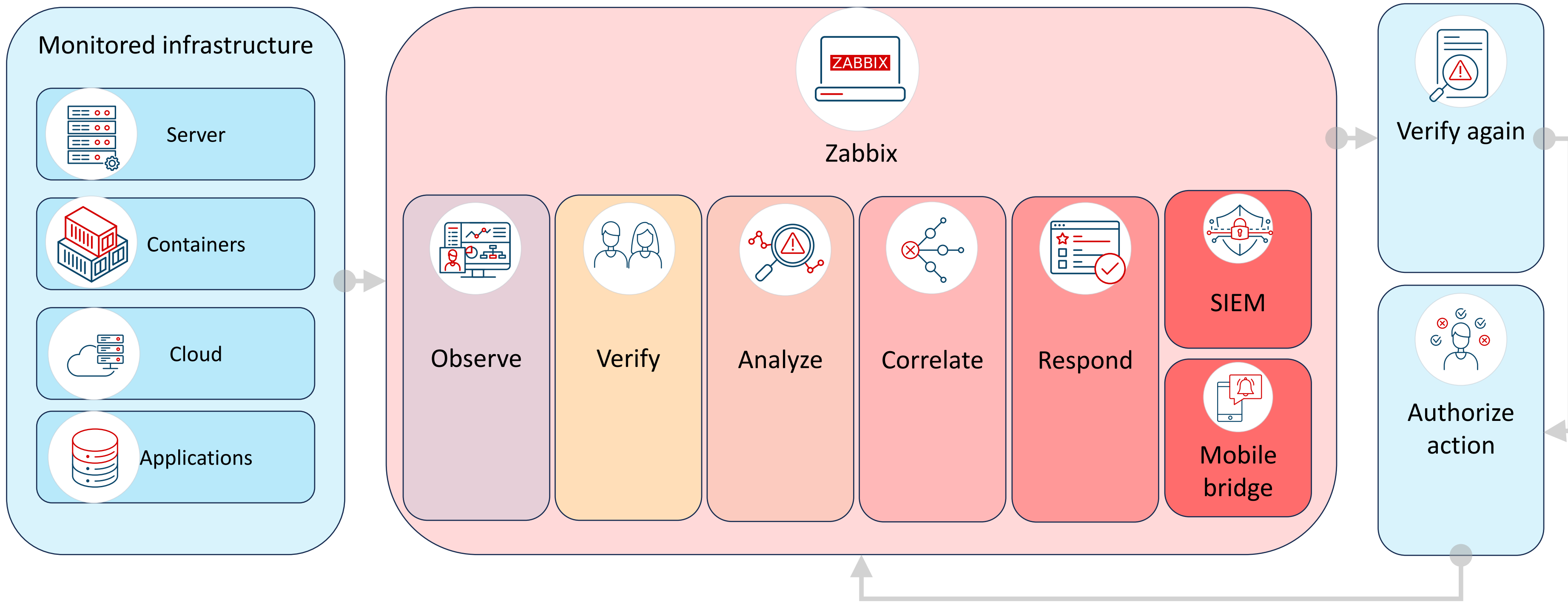
Encrypted protocols are in use

Multiple authentication methods already implemented from Zabbix side



The Complete Secure Observability Workflow





Thank you!