Deloitte.

Deloitte GPS
Zero Trust Practice

August 2022

MAKING AN IMPACT THAT MATTERS since 1845

Level Set on Zero Trust Definition

Zero Trust is based on the premise of least privilege access.

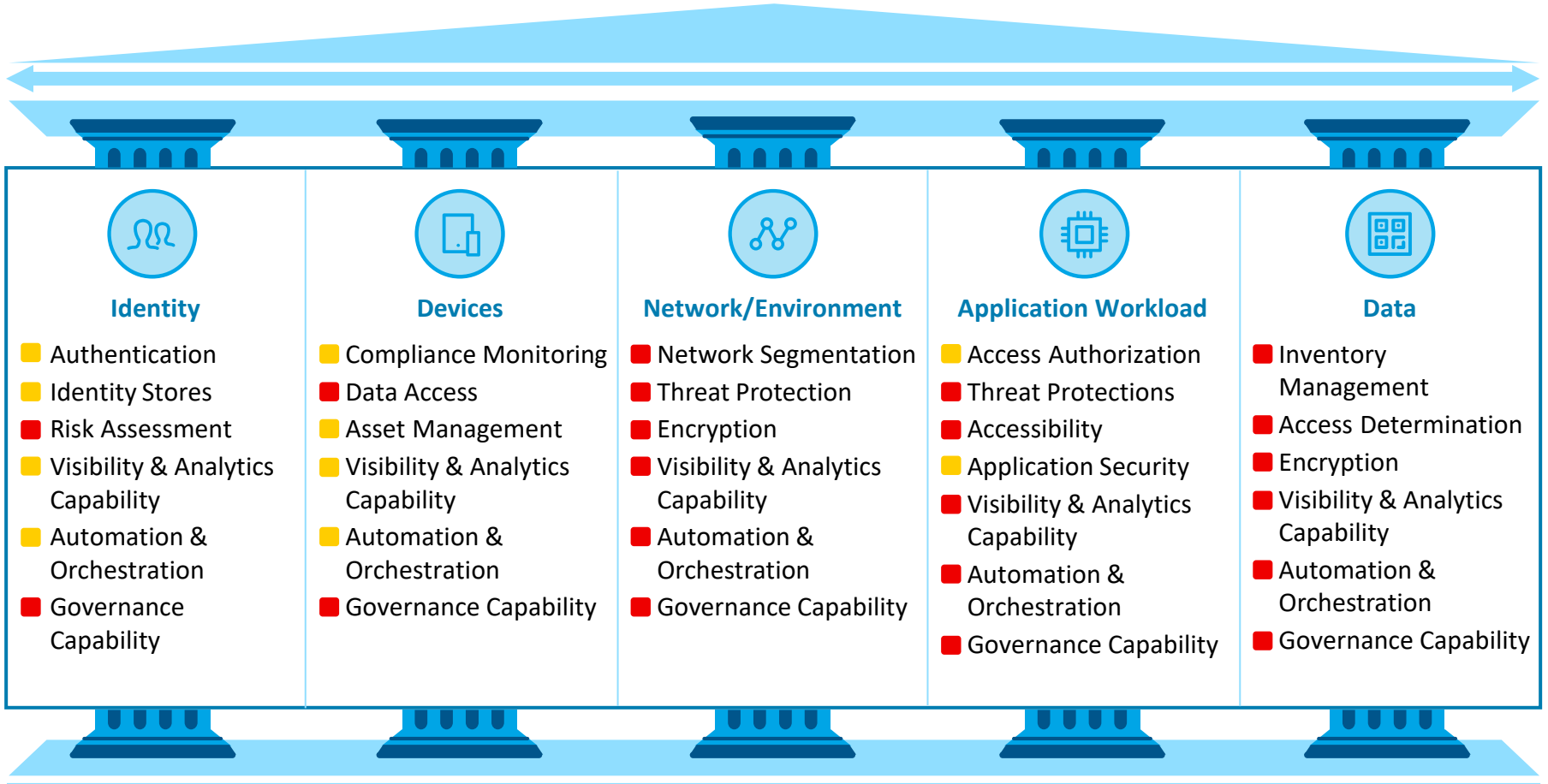
Never Trust, Always Verify.

Only allow access to a specific service for a controlled time to a user with valid credentials originating from a compliant device. (Continuous verification across all resources)

Copyright © 2022 Deloitte Development LLC. All rights reserved.

Federal Zero Trust Strategy Maturity Model

Example assessment leveraging the CISA Zero Trust Maturity Model to identify current state maturity levels for the five pillars are depicted below:



MATURITY LEVELS KEY

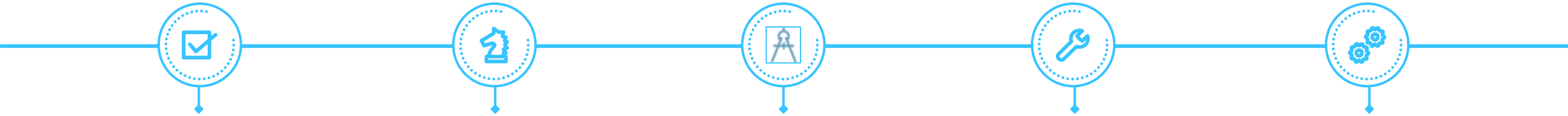
The below listed maturity level definitions are sourced from the CISA Zero Trust Maturity Model:

- **Traditional** - Manual configurations and pillar-level solutions dependent on external systems for response and mitigation deployment.
- **Advanced** - Some cross-pillar coordination, centralized visibility and identity control, and increased detail in dependencies with external systems that offer some least privilege changes.
- **Optimal** - Fully automated assignments of attributes to assets and resources, and dynamic policies based on automated/observed triggers for dynamic least privilege assets in alignment with cross-pillar interoperability.

Copyright © 2022 Deloitte Development LLC. All rights reserved.

Deloitte's Zero Trust Approach

Deloitte can provide cyber services to assist clients seeking to adopt a Zero Trust security approach through Assessing, Strategizing, Architecting, Implementing, and in select cases, Managing, next-generation security capabilities.



ASSESS

Assist clients in assessing existing capabilities / readiness for adoption:

- Asset inventory mgmt.
- Device management processes / procedures
- User / group directory management
- Network architecture, segmentation, and connectivity readiness
- Application readiness for MFA and/or third-party proxy integration
- Third-party vendor technology integration readiness
- Data discovery and criticality review

STRATEGIZE

Develop strategic roadmaps / actionable recommendations:

- Create user identity journeys to map processes and technology integrations
- Prioritize "context aware access" based on business transformation drivers
- Define roadmap for network segmentation across Cloud / on-prem
- Define data protection / privacy models, policies, and procedures aligned to laws and regulations

ARCHITECT

Develop technical architectures for on-prem and hybrid-Cloud models:

- Design approach for automating roll-out of ZT capabilities (e.g., agents and extensions to end user devices)
- Engineer app architectures for legacy / future apps to integrate with ZT target state
- Map access control rules between users, groups, and resources
- Define high-level and low-level designs in order to achieve desired target state (e.g., network segmentation approach to meet requirements)

IMPLEMENT

Assist with implementation of security controls across on-prem and Cloud:

- Perform verification / testing of apps integrating with security vendor ZT products
- Provide security PMO function to assist with migration / onboarding of ZT capabilities and tooling
- Deploy third-party vendor ZT products to end user devices
- Facilitate change management and required enhancements to operational and end user processes

MANAGE

Manage and operate select ZT capabilities across the framework:

- Determine onboarding plan and timeline
- Define service requirements, use cases, and operating model
- Provision Deloitte access into client environment and onboard to client's security tools / technologies
- Perform run-state operations (e.g., administrate ZT-centric third-party vendor security tools for client)
- Provide service reports (e.g., SLAs, KPIs, and KRIs)

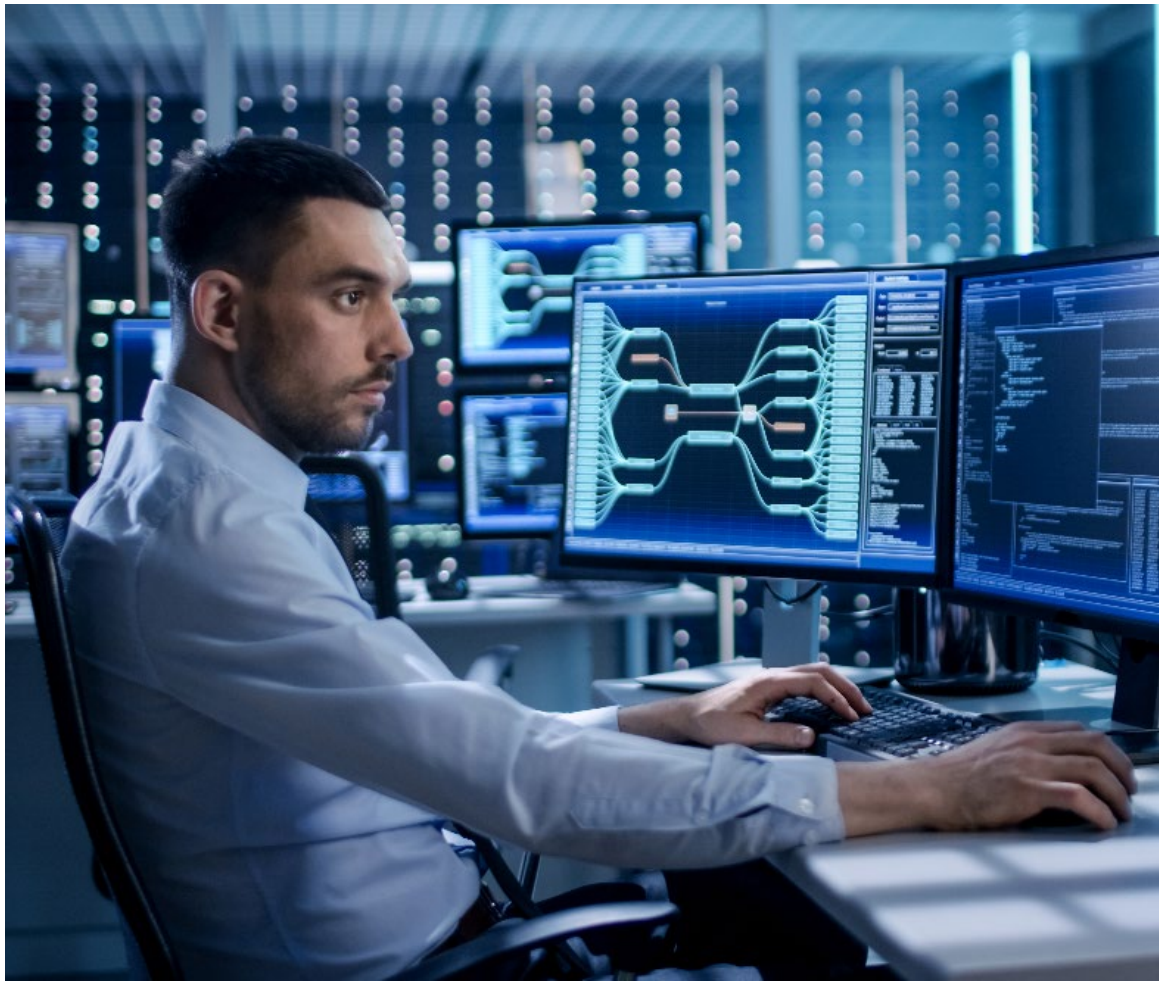
Copyright © 2022 Deloitte Development LLC. All rights reserved.

Significant Challenges

There are significant risks to implementation of Zero Trust in any enterprise

Cohesion across the entire IT organization requires a programmatic approach to move to Zero Trust

General resistance to change and retooling, Zero Trust forces modernization of mindsets as well as technology



Copyright © 2022 Deloitte Development LLC. All rights reserved.

Federal Government Agency – Zero Trust Assessment and Roadmap

Overview

The client engaged Deloitte to rapidly assess their current security posture and produce a Zero Trust Road Map with detailed recommendations

Client challenges included:

- Time sensitive reporting requirement
- Misconceptions on zero trust security
- No current assessment of security posture nor zero trust readiness
- Missing cohesive security plan

Deloitte provided zero trust security education, architecture, and leadership throughout the course of the engagement in order to assist the client in achieving its target state.

What We Did

- **Designed** cross agency zero trust program that emphasized zero trust adoption and depicted client's current and future state
- **Utilized** Deloitte, NIST, and CISA ZTA maturity models and publications for reference
- **Assessed** key Zero Trust pillars for readiness current state
- **Identified** security controls that presented opportunities for improvement
- **Aligned** with multiple groups to collect required information
- **Prioritized** identity, device, and workload protection initiatives across application platforms
- **Developed** a starting road map that included targets for the next 3 years

Outcomes

Delivered current and future state definitions and associated timeline

Created report content for agency compliance with the Executive Order

Defined zero trust program and detailed goals for entire agency

Socialized zero trust program concept and key future projects to reach target state

Copyright © 2022 Deloitte Development LLC. All rights reserved.

Federal Government Agency – Zero Trust Program and Pilot

Overview

The client engaged Deloitte to assess their current security posture and produce a Zero Trust reference design for a pilot application

Client challenges included:

- Multi-department cohesion
- Extreme number of technology solutions in place
- No current assessment of security posture nor zero trust readiness

Deloitte provided zero trust program management, design and architecture guidance, and cyber security leadership throughout the course of the engagement in order to assist the client in achieving its target state.

What We Did

- **Created** cross agency zero trust program that emphasized zero trust adoption and depicted client's current and future state
- **Utilized** CISA and DoD ZTA maturity models and publications for reference
- **Assessed** key Zero Trust pillars for readiness current state
- **Pinpointed** security controls that required improvement
- **Guided** multiple groups to collect information and execute sub projects
- **Prioritized** identity, device, and workload protection modernization across applications
- **Developed** a reference Zero Trust design for pilot program, and reference architecture for all other ZT implementations

Outcomes

Delivered current state assessment, gap analysis, and reference designs

Created report content for agency compliance with the Executive Order and associated memos

Defined zero trust program and detailed goals for entire agency

Socialized zero trust program to entire IT organization and leadership

Copyright © 2022 Deloitte Development LLC. All rights reserved.

Challenges

People

- Change from static security to context-based configurations.
- Trust in roles and identity attributes to determine permissions and access rights.
- Cannot be effective without strong and centralized identity and access management, implemented across all applications and data locations.
- Adoption often requires a cultural shift, including change management and training.

Process

- Monitoring and compensating for gaps during the transition to Zero Trust.
- Continuous monitoring, configuration, and maintenance.
- Zero-disruption to operations.
- Long-term commitment by leadership.
- Adapting current identity and access management procedures.
- Foundational cyber hygiene is crucial to realizing the benefits of the Zero Trust model.

Technology

- Fragmented Zero Trust technologies with no single vendor offering the full range of tools (e.g., cloud integration of apps, single sign-on, multi-factor authentication).
- Extensibility with existing invested technologies.
- Extended leave-related compliance posture.
- Maturity in automation and orchestration tools.

Zero Trust Problem Sets

REMOTE WORKFORCE & MODERNIZATION

Sudden shift to remote work overburdens legacy systems and IT and security capabilities.

REGULATORY COMPLIANCE

Managing compliance with NIST, FedRAMP, FIPS, DFARS-CUI, and other policies and regulations.

SOFTWARE DEFINED APPROACH IN EVOLVING PERIMETERS

As the perimeter continues to dissolve, attack surfaces widen. Traditional models must evolve to identify and protect all data, devices, applications, and systems.

DIGITALIZATION AND THE MOVE TO THE CLOUD

Use of emerging technologies like Cloud drive better engagement with stakeholders but increases the surface area for potential vulnerabilities.

Copyright © 2022 Deloitte Development LLC. All rights reserved.

GPS Zero Trust

General Use Cases

Copyright © 2022 Deloitte Development LLC. All rights reserved.

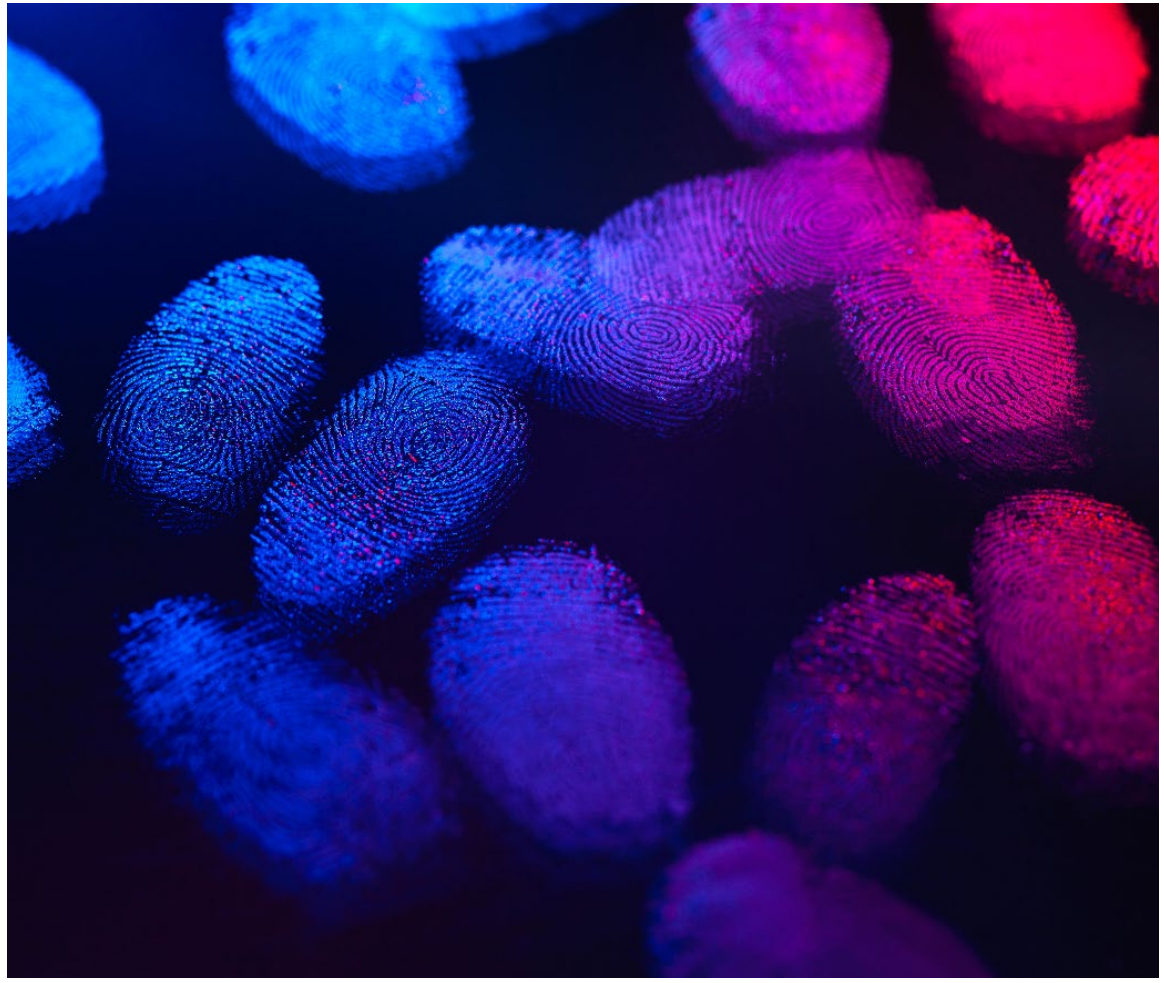
Use Case 1 – Highly Secure Remote Application Access / Digital Worker Access

REQUIREMENT

Enterprise users require a highly secure method to access applications controlled and not controlled by the organization.

SOLUTION

Creating secure access from anywhere on any network if a user has valid credentials and is coming from a secure system. This high level of access security can be created via a combination of device endpoint security solutions, identity and privilege access management, and micro segmentation to organization controlled workloads. Access to SaaS solutions on the Internet will utilize the device and identity solutions that are part of the ZT architecture, with the inclusion of cloud based web proxy, CASB, and browser isolation solutions to ensure a defense in depth approach.



Copyright © 2022 Deloitte Development LLC. All rights reserved.

Use Case 2 – Workload and Container Hardening

REQUIREMENT

Data breaches in multi-tier applications and lateral movement of attacks inside data centers and cloud instances continue to be a high risk. A solution is needed to mitigate or remove this risk across all modern workloads in an organization.

SOLUTION

The proper implementation of a best of breed workload protection solution can automatically baseline application workflows and create policy to that will result in a hardened workload environment. Best of breed workload protection also monitors for CVE compliance with automated isolation when a system falls out of compliance, and includes process behavior anomaly detection that even stops side channel and management channel attacks. These newer tools help to remove human errors, negligence, and supply chain risks on workloads.

Copyright © 2022 Deloitte Development LLC. All rights reserved.

Use Case 3 – Higher Security on Legacy Applications and Systems

REQUIREMENT

Legacy applications and systems are unable to properly integrate with the direction modern security tools. A solution must support legacy applications and systems that are unable to natively integrate

SOLUTION

The proper solution in this case is application modernization; however, there are zero trust designs that can stretch modern solutions into legacy multi-tier applications. Each case is very specific to each environment and no one solution fits every situation. With a combination of proxy, next generation firewalls, and next generation telemetry the security posture of legacy applications can be increased to a much higher standard. Some older methods to achieve zero trust can be implemented and newer solutions can front end legacy applications to get much closer to a zero trust posture on legacy systems.

Copyright © 2022 Deloitte Development LLC. All rights reserved.

Use Case 4 - Secure Operational Technology and Internet of Things Devices

REQUIREMENT

OT and IoT systems are traditionally behind on security updates, there is a need to create highly visible and controlled OT/IoT ecosystem in an organization.

SOLUTION

Zero trust architecture requires devices to be validated to be secure. OT/IoT devices traditionally fall out of compliance with patching, thus should not be implicitly trusted. It is highly unlikely that OT/IoT will meet the strict requirements of a zero trust architecture, but just like legacy applications specific older zero trust methods and tools can be utilized to create a much higher security posture for an OT/IoT solution in an organization. While OT/IoT devices can be vulnerable to attack, the workload / server involved in an OT/IoT system may be modern and support newer security tools.

Copyright © 2022 Deloitte Development LLC. All rights reserved.

Use Case 5 – Application/Code Hardening

REQUIREMENT

Insider threats and credential theft are a considerable risk to large organizations. Applications need to be secured from internal threats.

SOLUTION

While the concept of zero trust security will not stop insider threat or the combination of credential theft and control of a trusted host. Other aspects of a comprehensive zero trust approach can mitigate these vectors. Regular application penetration testing and secure application development practices address some of the risks of insider threat. Custom visibility and control code imbedded in libraries or code can be utilized to ramp up the detection of malicious behavior. Web application firewalls and workload behavior anomaly detection can provide another layer of depth to the overall security of an application.

Copyright © 2022 Deloitte Development LLC. All rights reserved.

Deloitte.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Copyright © 2022 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited