SINTESI DEL: CISA - ZERO TRUST MATURITY MODEL

ZT MATURITY MODEL

DATA CREAZIONE: 8 Giugno 2023

PREMESSA

L'argomento trattato in questa mia sintesi, tratta da "CISA - ZTMM - ZERO TRUST MATURITY MODEL", *è estremamente importante sia per la progettazione di nuove architetture informatiche sia per l'aggiornamento di quelle esistenti.*

Quindi, lo studio di questo PARADIGMA *è sicuramente molto utile per i progettisti di architetture informatiche, per chi si occupa di sicurezza informatica e per chi è coinvolto nella gestione di tutte le implicazioni afferenti agli aspetti tecnico-legislativi del trattamento dei dati.*

Allo scopo di ottenere un'adeguata difesa informatica contro le continue minacce, le organizzazioni devono adottare gli approcci delineati in questa guida perché tali minacce richiedono maggiore velocità e agilità per superarle, inducendo sostanzialmente l'aumento dei costi che i malintenzionati devono affrontare e migliorando la resilienza necessaria al ripristino rapido della piena capacità operativa.

A riguardo, CISA (*) *ha realizzato la guida* ZTMM *per comprendere, gestire e ridurre il rischio di sicurezza informatica. Questa guida, di fatto, fornisce un approccio per ottenere continui adeguamenti alle innovazioni relative allo* ZT *in continua evoluzione ed è complementare al* NIST SP 800-207.

CISA *afferma che* ZTMM *è uno dei tanti percorsi che un'organizzazione può intraprendere nella progettazione e nell'implementazione del proprio piano di transizione verso architetture* ZT (ZTA).

(*) CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY - https://www.cisa.gov

INDICE DEGLI ARGOMENTI

Titolo_____ Pag.

CHE COSA È ZERO TRUST (ZT) 3

ZT MATURITY MODEL 4

Guiding Criteria to Identify Maturity Model 6

Pilastro 1: Identity 10

Pilastro 2: Devices 12

Pilastro 3: Networks 15

Pilastro 4: Applications and Workloads 18

Pilastro 5: Data 21

Cross-Cutting Capabilities 24

CHE COSA È ZERO TRUST (ZT)

La pubblicazione speciale (SP) 800-207 del NIST fornisce la seguente definizione.

ZT fornisce una raccolta di concetti e idee progettati per ridurre al minimo l'incertezza nell'applicazione di decisioni di accesso accurate e con privilegi minimi per richiesta in sistemi e servizi informativi di fronte a una rete considerata compromessa.

ZTA è un piano di sicurezza informatica aziendale che utilizza concetti ZT e comprende relazioni tra componenti, pianificazione del flusso di lavoro e policy di accesso.

Pertanto, un'impresa ZT è l'infrastruttura di rete (fisica e virtuale) e le politiche operative in atto come prodotto di un piano ZTA.

SP 800-207 *sottolinea che l'obiettivo di* ZT *è quello di:*

"Impedire l'accesso non autorizzato a dati e servizi e a rendere l'applicazione del controllo degli accessi il più granulare possibile".

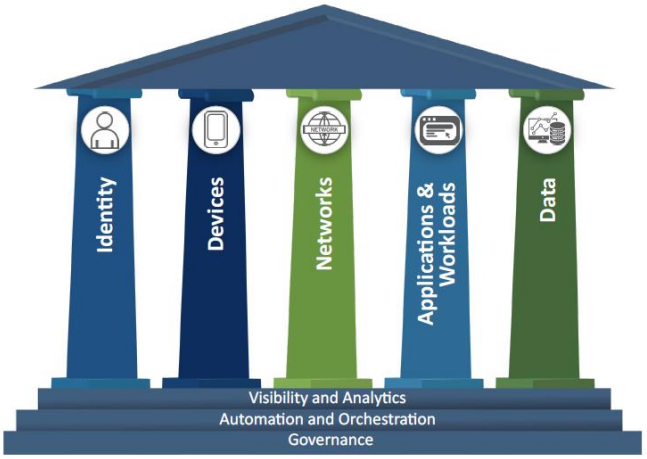
ZT *presenta un passaggio da un* **modello incentrato sulla posizione a un approccio incentrato sull'identità, sul contesto e sui dati con controlli di sicurezza granulari** *tra utenti, sistemi, applicazioni, dati e risorse che cambiano nel tempo.*

Fondamentalmente, ZT *può richiedere un cambiamento nella filosofia e nella cultura della sicurezza informatica di un'organizzazione.*

ZT MATURITY MODEL

ZTMM *rappresenta un gradiente di implementazione attraverso 5 pilastri distinti, in cui è possibile apportare piccoli progressi nel tempo verso l'ottimizzazione.*

FIGURA 1: ZT MATURITY MODEL PILLARS



I 5 pilastri, illustrati nella Figura 1, sono:

1) IDENTITY,
2) DEVICES,
3) NETWORKS,
4) APPLICATIONS & WORKLOADS,
5) DATA.

Ogni pilastro include dettagli generali relativi alle seguenti FUNZIONALITÀ TRASVERSALI*:*

1) VISIBILITY E ANALITICS,
2) AUTOMATION & ORCHESTRATION,
3) GOVERNANCE.

Diverse pubblicazioni ZTA *hanno informato lo sviluppo di questo modello di maturità (cfr. sezione 6 per ulteriori dettagli).*

Questo modello riflette i 7 principi di ZT *delineati nel* NIST SP 800-207*:*

1. *Tutte le origini dati e i servizi di elaborazione sono considerati risorse.*
2. *Tutte le comunicazioni sono protette indipendentemente dal percorso di rete.*
3. *L'accesso alle singole risorse aziendali viene concesso in base alla sessione.*
4. *L'accesso alle risorse è determinato da criteri dinamici.*
5. *L'azienda monitora e misura l'integrità e la sicurezza di tutte le risorse possedute e associate.*
6. *Tutte le autorizzazioni e autenticazione delle risorse sono dinamiche e rigorosamente applicate prima che l'accesso sia consentito.*
7. *L'azienda raccoglie quante più informazioni possibili sullo stato corrente delle risorse, dell'infrastruttura di rete e delle comunicazioni e le utilizza per migliorare il proprio livello di sicurezza.*

In linea con i passaggi del NIST *per la transizione verso il modello* ZT*, valutare: sistemi, risorse, infrastrutture, personale e processi aziendali.*

Le 3 fasi del percorso ZTM *sono:*

1^ fase: da TRADITIONAL *a* INITIAL

2^ fase: da INITIAL *a* ADVANCED

3^ fase: da ADVANCED *a* OPTIMAL

FIGURA 2: ZT MATURITY JOURNEY

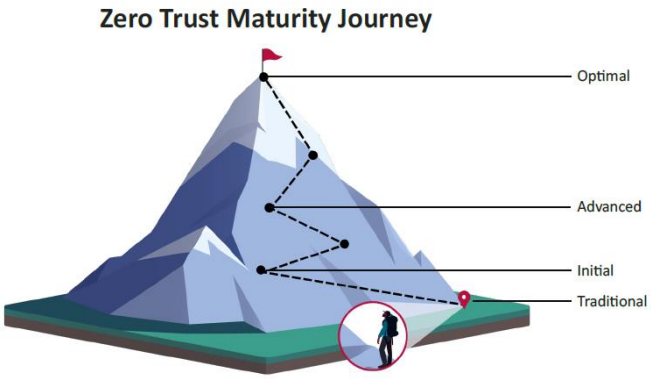
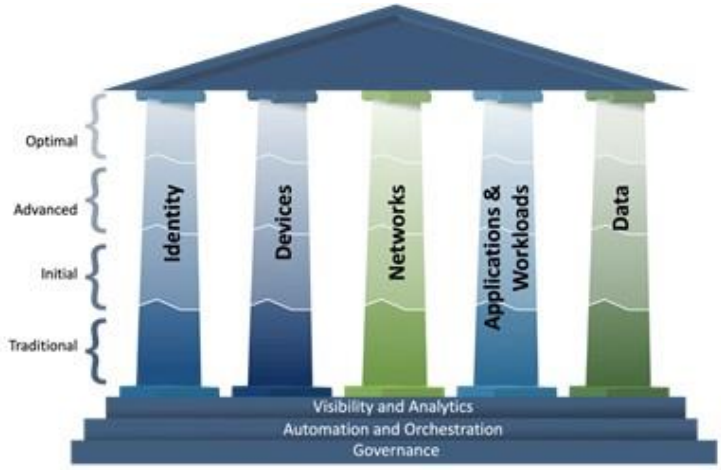


Figure 2: Zero Trust Maturity Journey

Come illustrato nella Figura 2, le agenzie dovrebbero aspettarsi che i livelli di impegno richiesti e i benefici realizzati aumentino significativamente man mano che la maturità ZT progredisce attraverso e all'interno dei pilastri.

FIGURA 3: ZT MATURITY EVOLUTION



La Figura 3 evidenzia l'evoluzione prevista nel tempo da uno stato tradizionale a uno stato futuro che presenta aggiornamenti più dinamici, processi automatizzati, funzionalità integrate e altre caratteristiche delle fasi ottimali (come descritto nel modello di maturità).

GUIDING CRITERIA TO IDENTIFY MATURITY MODEL

Utilizzare i seguenti criteri guida di ciascuno dei 4 stati al fine di identificare la maturità per ciascun pilastro tecnologico ZT e fornire coerenza in tutto il MATURITY MODEL.

1) TRADITIONAL

a. *cicli di vita tradizionali configurati manualmente (ad esempio, dalla creazione alla disattivazione) e assegnazioni di attributi (sicurezza e registrazione);*
b. *policy e soluzioni di sicurezza statiche che affrontano un pilastro alla volta con dipendenze discrete da sistemi esterni;*
c. *privilegi minimi stabiliti solo al provisioning;*
d. *pilastri isolati di applicazione delle policy;*
e. *distribuzione manuale di risposta e mitigazione;*
f. *correlazione limitata di dipendenze, registri e telemetria.*

2) INITIAL

a. *avvio dell'automazione dell'assegnazione degli attributi e della configurazione dei cicli di vita,*
b. *decisioni e applicazione delle policy e soluzioni iniziali tra pilastri con integrazione di sistemi esterni;*
c. *modifiche reattive al privilegio minimo dopo il provisioning;*
d. *visibilità aggregata per i sistemi interni.*

3) ADVANCED

a. *controlli avanzati: ove applicabile, automatizzati per il ciclo di vita e l'assegnazione di configurazioni e policy con coordinamento tra pilastri;*
b. *visibilità centralizzata e controllo dell'identità;*
c. *applicazione delle policy integrata tra pilastri;*
d. *risposta a mitigazioni predefinite;*
e. *modifiche al privilegio minimo in base alle valutazioni del rischio e della postura;*
f. *sviluppo verso la consapevolezza a livello aziendale (comprese le risorse ospitate esternamente).*

4) OPTIMAL

a. *cicli di vita just-in-time completamente automatizzati e assegnazioni di attributi ad asset e risorse che si auto-segnalano con policy dinamiche basate su trigger automatizzati/osservati;*

b. *accesso dinamico con privilegi minimi (appena sufficiente ed entro soglie) per le risorse e le rispettive dipendenze a livello aziendale;*

c. *interoperabilità* cross-pillar *con monitoraggio continuo;*

d. *visibilità centralizzata con consapevolezza situazionale completa.*

La figura 4 fornisce una panoramica generale dello ZTMM, *compresi gli aspetti chiave delle funzioni specifiche per ciascun pilastro e in ogni stato di maturità.*

FIGURA 4: HIGH-LEVEL ZT MATURITY MODEL OVERVIEW

	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

Transizione verso il principio ZT attraverso i 5 diversi pilastri:

1) IDENTITY,
2) DEVICES,
3) NETWORKS,
4) APPLICATIONS & WORKLOADS,
5) DATA.

Per supportare l'integrazione con il pilastro e in tutto il modello, ogni pilastro include anche dettagli generali relativi alle funzionalità di:

1) VISIBILITY E ANALITICS,
2) AUTOMATION E ORCHESTRATION
3) GOVERNANCE

Le suddette 3 funzionalità trasversali evidenziano le attività a sostegno dell'interoperabilità delle funzioni tra i pilastri sulla base delle seguenti descrizioni:

1) VISIBILITY *e* ANALITICS

   La Visibilità si riferisce agli artefatti osservabili che derivano dalle caratteristiche e dagli eventi all'interno degli ambienti aziendali.

   L'Analisi dei dati relativi al cyber può aiutare a prendere decisioni politiche informate, facilitare le attività di risposta e costruire un profilo di rischio per sviluppare misure di sicurezza proattive prima che si verifichi un incidente.

2) AUTOMATION *e* ORCHESTRATION

   ZT *fa pieno uso di strumenti e flussi di lavoro automatizzati che supportano le funzioni di risposta alla sicurezza tra prodotti e servizi, mantenendo al contempo supervisione, sicurezza e interazione del processo di sviluppo per tali funzioni, prodotti e servizi.*

3) GOVERNANCE

   Si riferisce alla definizione e all'applicazione associata di politiche, procedure e processi di sicurezza informatica dell'agenzia, all'interno e tra i pilastri, per gestire l'impresa di un'agenzia e mitigare i rischi per la sicurezza a sostegno dei principi ZT e dell'adempimento dei requisiti federali.

ZTMM *copre molti aspetti della sicurezza informatica critici per le imprese federali, ma non affronta altri aspetti della sicurezza informatica come le attività relative alla risposta agli incidenti, le specifiche per la registrazione, il monitoraggio, l'allarme, l'analisi forense, l'accettazione del rischio, il recupero.*

Il modello di maturità non dovrebbe essere visto come un insieme rigoroso di requisiti, ma come una guida generale per aiutare ad implementare con successo la loro ZTA *e adottare una posizione di sicurezza informatica complessivamente migliorata.*

PILASTRO 1: IDENTITY

Un'identità si riferisce a un attributo o a un insieme di attributi che descrive in modo univoco un utente o un'entità, incluse le entità non personali.

OBIETTIVI

- *Garantire e imporre l'accesso degli utenti e delle entità alle risorse giuste al momento giusto per lo scopo giusto senza concedere un accesso eccessivo.*

- *Integrare soluzioni di gestione delle identità, delle credenziali e degli accessi, ove possibile, in tutta l'azienda per applicare l'autenticazione avanzata, concedere autorizzazioni personalizzate basate sul contesto e valutare il rischio di identità per gli utenti e le entità dell'agenzia.*

Nella tabella 2 sono elencate le FUNZIONI DI IDENTITÀ *relative al principio* ZT *e le considerazioni per la visibilità e l'analisi, l'automazione e l'orchestrazione e la governance nel contesto dell'identità.*

TABLE 2: IDENTITY PILLAR

FUNCTION	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
AUTENTICAZIONE	*L'agenzia autentica l'identità utilizzando password o autenticazione a più fattori (MFA) con accesso statico per l'identità dell'entità.*	*L'agenzia autentica l'identità utilizzando MFA, che può includere password come un fattore e richiede la convalida di più attributi di entità (ad esempio, impostazioni locali o attività).*	*L'agenzia inizia a autenticare tutte le identità utilizzando MFA e attributi resistenti al phishing, inclusa l'implementazione iniziale di password meno MFA tramite FIDO2 o PIV.*	*L'agenzia convalida continuamente l'identità con MFA resistente al phishing, non solo quando l'accesso viene inizialmente concesso.*
ARCHIVI DI IDENTITÀ	*L'agenzia utilizza solo archivi di identità locali autogestiti (ovvero pianificati, distribuiti e gestiti dall'agenzia).*	*L'agenzia ha una combinazione di archivi di identità autogestiti e archivi di identità ospitati (ad esempio, cloud o altra agenzia) con un'integrazione minima tra gli archivi (ad esempio, Single Signon).*	*Agency inizia a consolidare e integrare in modo sicuro alcuni archivi di identità autogestiti e ospitati.*	*L'agenzia integra in modo sicuro i propri archivi di identità in tutti i partner e gli ambienti, a seconda dei casi.*
VALUTAZIONI DEL RISCHIO	*L'agenzia effettua determinazioni limitate per il rischio di identità (cioè la probabilità che un'identità sia compromessa).*	*L'agenzia determina il rischio di identità utilizzando metodi manuali e regole statiche per supportare la visibilità.*	*L'agenzia determina il rischio di identità con alcune analisi automatizzate e regole dinamiche per informare le decisioni di accesso e le attività di risposta.*	*L'agenzia determina il rischio di identità in tempo reale sulla base di analisi continue e regole dinamiche per fornire una protezione continua.*
GESTIONE DEGLI ACCESSI (NOVITÀ FUNZIONE)	*L'Agenzia autorizza l'accesso permanente con revisione periodica sia per gli account privilegiati che per quelli non privilegiati.*	*L'Agenzia autorizza l'accesso, anche per le richieste di accesso privilegiato, che scade con la revisione automatica.*	*L'Agenzia autorizza l'accesso basato sulle esigenze e sulla sessione, anche per le richieste di accesso privilegiato, che è adattato alle azioni e alle risorse.*	*L'agenzia utilizza l'automazione per autorizzare l'accesso just-in-time e just-enough su misura per le singole azioni e le esigenze delle singole risorse.*
CAPACITÀ DI VISIBILITÀ E ANALISI	*Agency raccoglie i registri delle attività degli utenti e delle entità, in particolare per le credenziali privilegiate, ed esegue alcune analisi manuali di routine.*	*Agency raccoglie i registri delle attività degli utenti e delle entità ed esegue analisi manuali di routine e alcune analisi automatizzate, con una correlazione limitata tra i tipi di registro.*	*L'agenzia esegue analisi automatizzate su alcuni tipi di log delle attività di utenti ed entità e aumenta la raccolta per colmare le lacune nella visibilità.*	*L'agenzia mantiene una visibilità completa e la consapevolezza situazionale in tutta l'azienda eseguendo analisi automatizzate sui tipi di log delle attività degli utenti, inclusa l'analisi basata sul comportamento.*
CAPACITÀ DI AUTOMAZIONE E ORCHESTRAZIONE	*L'agenzia orchestra manualmente (onboard, offboard e disabilita) le identità autogestite (utenti ed entità), con poca integrazione, ed esegue revisioni regolari.*	*L'agenzia orchestra manualmente le identità privilegiate ed esterne e automatizza l'orchestrazione degli utenti non privilegiati e delle entità autogestite.*	*Agency orchestra manualmente le identità degli utenti privilegiati e automatizza l'orchestrazione di tutte le identità con l'integrazione in tutti gli ambienti.*	*L'agenzia automatizza Orchestrazione di tutte le identità con integrazione completa in tutti gli ambienti in base a comportamenti, registrazioni ed esigenze di distribuzione.*
CAPACITÀ DI GOVERNANCE	*L'agenzia implementa politiche di identità (autenticazione, credenziali, accesso, ciclo di vita, ecc.) con applicazione tramite meccanismi tecnici statici e revisione manuale.*	*L'agenzia definisce e inizia a implementare criteri di identità per l'applicazione a livello aziendale con automazione minima e aggiornamenti manuali.*	*L'agenzia implementa criteri di identità per l'applicazione a livello aziendale con l'automazione e aggiorna periodicamente le politiche.*	*Agency implementa e automatizza completamente le policy di identità a livello aziendale per tutti gli utenti e le entità su tutti i sistemi con applicazione continua e aggiornamenti dinamici.*

PILASTRO 2: DEVICES

Un dispositivo si riferisce a qualsiasi risorsa (inclusi hardware, software, firmware e così via) in grado di connettersi a una rete, inclusi server, computer desktop e portatili, stampanti, telefoni cellulari, dispositivi IoT, apparecchiature di rete e altro ancora.

I dispositivi possono essere di proprietà o BYOD (BRING-YOUR-OWN-DEVICE) *di dipendenti, partner o visitatori.*

OBIETTIVI

- *Proteggere tutti i dispositivi,*
- *Gestire i rischi dei dispositivi autorizzati che non sono controllati dall'agenzia e*
- *Impedire ai dispositivi non autorizzati di accedere alle risorse.*

La gestione dei dispositivi include il mantenimento di un inventario dinamico di tutte le risorse, inclusi hardware, software, firmware, ecc., insieme alle loro configurazioni e vulnerabilità associate man mano che diventano note.

Molti dispositivi presentano sfide ZTA *specifiche e devono essere valutati caso per caso come parte di un processo basato sul rischio. Ad esempio, le apparecchiature di rete, le stampanti e altri possono offrire opzioni limitate per l'autenticazione, la visibilità e la sicurezza.*

La gestione delle risorse informatiche locali comporta la documentazione e la gestione delle risorse fisiche (dispositivi).

Nella tabella 3 sono elencate le funzioni per i dispositivi che rientrano in ZT, *nonché considerazioni su* VISIBILITY *e* ANALYTICS, AUTOMATION *e* ORCHESTRATION *e* GOVERNANCE *nel contesto dei dispositivi.*

TABLE 3: DEVICES PILLAR

FUNCTION	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
APPLICAZIONE DELLE POLITICHE & MONITORAGGIO DELLA CONFORMITÀ (NUOVA FUNZIONE)	*L'agenzia ha limitato, se del caso, visibilità (cioè capacità di ispezionare il comportamento del dispositivo) nella conformità del dispositivo con pochi metodi di applicazione dei criteri o di gestione di software, configurazioni o vulnerabilità.*	*L'agenzia riceve l'auto-segnalazione Caratteristiche del dispositivo (ad esempio, chiavi, token, utenti, ecc., sul dispositivo) ma ha meccanismi di applicazione limitati. L'agenzia dispone di un processo preliminare di base per approvare l'uso del software e inviare aggiornamenti e modifiche alla configurazione dei dispositivi.*	*L'agenzia ha verificato approfondimenti (cioè, un amministratore può ispezionare e verificare i dati sul dispositivo) all'accesso iniziale al dispositivo e applica la conformità per la maggior parte dei dispositivi e delle risorse virtuali. L'agenzia utilizza metodi automatizzati per gestire dispositivi e risorse virtuali, approvare software, identificare vulnerabilità e installare patch.*	*L'Agenzia verifica continuamente Approfondimenti e applicazione conformità per tutta la durata di vita dei dispositivi e delle risorse virtuali. Agency integra la gestione di dispositivi, software, configurazione e vulnerabilità in tutti gli ambienti dell'agenzia, comprese le risorse virtuali.*
GESTIONE DEL RISCHIO DELL'ASSET & SUPPLY CHAIN (NOVITÀ FUNZIONE)	*L'agenzia non tiene traccia delle risorse fisiche o virtuali in modo aziendale o crossvendor e gestisce la propria acquisizione di dispositivi e servizi nella supply chain in modo ad hoc con una visione limitata dei rischi aziendali.*	*L'agenzia tiene traccia di tutte le risorse fisiche e di alcune risorse virtuali e gestisce i rischi della catena di approvvigionamento stabilendo politiche e linee di base di controllo in base alle raccomandazioni federali utilizzando un solido quadro (ad esempio, NIST SCRM.)*	*L'agenzia inizia a sviluppare una visione aziendale completa delle risorse fisiche e virtuali tramite processi automatizzati che possono funzionare su più fornitori per verificare le acquisizioni, tenere traccia dei cicli di sviluppo e fornire valutazioni di terze parti.*	*L'agenzia ha una visione completa, in tempo reale o quasi, di tutte le risorse tra fornitori e fornitori di servizi, automatizza la gestione del rischio della supply chain a seconda dei casi, crea operazioni che tollerano i guasti della supply chain e incorpora le migliori pratiche.*
ACCESSO ALLE RISORSE (PRECEDENTEMENTE ACCESSO AI DATI)	*L'agenzia non richiede visibilità dei dispositivi o delle risorse virtuali utilizzati per accedere alle risorse.*	*L'agenzia richiede alcuni dispositivi o risorse virtuali per segnalare le caratteristiche, quindi utilizzare queste informazioni per approvare l'accesso alle risorse.*	*La risorsa iniziale dell'Agenzia Access prende in considerazione informazioni dettagliate verificate sul dispositivo o sulle risorse virtuali.*	*Accesso alle risorse dell'Agenzia Considera l'analisi dei rischi in tempo reale all'interno di dispositivi e risorse virtuali.*
PROTEZIONE DALLE MINACCE DEL DISPOSITIVO (NUOVA FUNZIONE)	*L'agenzia distribuisce manualmente le funzionalità di protezione dalle minacce su alcuni dispositivi.*	*L'agenzia dispone di alcuni processi automatizzati per la distribuzione e l'aggiornamento delle funzionalità di protezione dalle minacce ai dispositivi e alle risorse virtuali con un'applicazione limitata delle policy e l'integrazione del monitoraggio della conformità.*	*L'agenzia inizia a consolidare le funzionalità di protezione dalle minacce in soluzioni centralizzate per dispositivi e risorse virtuali e integra la maggior parte di queste funzionalità con l'applicazione delle policy e il monitoraggio della conformità.*	*L'agenzia dispone di una o più soluzioni centralizzate per la protezione dalle minacce implementate con funzionalità avanzate per tutti i dispositivi e le risorse virtuali e un approccio unificato per la protezione dalle minacce dei dispositivi, l'applicazione delle policy e il monitoraggio della conformità.*
CAPACITÀ DI VISIBILITÀ E ANALISI	*L'agenzia utilizza un inventario fisicamente etichettato e un monitoraggio software limitato per rivedere*	*L'agenzia utilizza identificatori digitali (ad esempio, indirizzi di interfaccia, tag digitali) insieme a un inventario manuale e al monitoraggio degli*	*Agency automatizza sia la raccolta dell'inventario (incluso il monitoraggio degli endpoint su tutti i dispositivi utente standard, ad esempio*	*Agency automatizza la raccolta dello stato di tutti i dispositivi connessi alla rete e delle risorse virtuali, correlando al contempo le identità,*

FUNCTION	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
	regolarmente i dispositivi con alcune analisi manuali.	*endpoint dei dispositivi, quando disponibili.* *Alcuni dispositivi dell'agenzia e risorse virtuali sono sottoposti ad analisi automatizzata (ad esempio, scansione basata su software) per il rilevamento delle anomalie in base al rischio.*	*desktop e laptop, telefoni cellulari, tablet e le loro risorse virtuali) sia il rilevamento delle anomalie per rilevare i dispositivi non autorizzati.*	*conducendo il monitoraggio degli endpoint ed eseguendo il rilevamento delle anomalie per informare l'accesso alle risorse.* *L'agenzia tiene traccia dei modelli di provisioning e/o deprovisioning delle risorse virtuali per rilevare anomalie.*
CAPACITÀ DI AUTOMAZIONE E ORCHESTRAZIONE	*L'agenzia effettua manualmente il provisioning, configura e/o registra i dispositivi all'interno dell'azienda.*	*L'agenzia inizia a utilizzare strumenti e script per automatizzare il processo di provisioning, configurazione, registrazione e/o deprovisioning per dispositivi e risorse virtuali.*	*L'agenzia ha implementato meccanismi di monitoraggio e applicazione per identificare e disconnettere manualmente o isolare dispositivi e risorse virtuali non conformi (certificato vulnerabile e non verificato, indirizzo* mac *non registrato).*	*L'agenzia dispone di processi completamente automatizzati per il provisioning, la registrazione, il monitoraggio, l'isolamento, la correzione e il deprovisioning di dispositivi e risorse virtuali.*
CAPACITÀ DI GOVERNANCE	*L'agenzia stabilisce alcune politiche per il ciclo di vita dei propri dispositivi informatici tradizionali e periferici e si affida a processi manuali per mantenere (ad esempio, aggiornare, patchare, disinfettare) questi dispositivi.*	*L'agenzia stabilisce e applica politiche per l'approvvigionamento di nuovi dispositivi, il ciclo di vita di dispositivi informatici non tradizionali e risorse virtuali e per condurre regolarmente il monitoraggio e la scansione dei dispositivi.*	*L'agenzia stabilisce criteri a livello aziendale per il ciclo di vita dei dispositivi e delle risorse virtuali, inclusa la loro enumerazione e responsabilità, con alcuni meccanismi di applicazione automatizzati.*	*Agency automatizza le policy per il ciclo di vita di tutti i dispositivi connessi alla rete e delle risorse virtuali in tutta l'azienda.*

PILASTRO 3: NETWORKS

Una rete si riferisce a un mezzo di comunicazione aperto che include canali tipici come le reti interne delle agenzie, le reti wireless e Internet, nonché altri canali potenziali come i canali cellulari e a livello di applicazione utilizzati per trasportare i messaggi.

ZTA CONSENTE DI:

1. *Allontanarsi dai tradizionali approcci alla sicurezza incentrati sul perimetro e consentono di gestire i flussi di traffico interni ed esterni, isolare gli host, applicare la crittografia, segmentare l'attività e migliorare la visibilità della rete a livello aziendale.*

2. *Implementare controlli di sicurezza più vicino alle applicazioni, ai dati e ad altre risorse e aumentano le protezioni tradizionali basate sulla rete e migliorano la profondità della difesa.*

Ogni applicazione può essere trattata in modo univoco dalla rete per le sue esigenze di accesso, priorità, raggiungibilità, connessioni ai servizi di dipendenza e percorsi di connessione.

Queste richieste di applicazioni di rete possono essere acquisite come profilo dell'applicazione e i profili ripetuti possono quindi essere trattati come una classe di traffico.

Nella tabella 4 sono elencate le funzioni di rete relative al modello ZT e le considerazioni relative a VISIBILITY *e* ANALYTICS, AUTOMATION *e* ORCHESTRATION *e* GOVERNANCE *nel contesto delle reti.*

TABLE 4: NETWORKS PILLAR

FUNCTION	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
SEGMENTAZIONE DELLA RETE	*L'agenzia definisce la propria architettura di rete utilizzando un ampio perimetro/macro-segmentazione con restrizioni minime sulla raggiungibilità all'interno dei segmenti di rete. L'agenzia può anche fare affidamento su interconnessioni multiservizio (ad esempio, tunnel VPN per il traffico di massa).*	*L'agenzia inizia a implementare l'architettura di rete con l'isolamento dei carichi di lavoro critici, limitazione della connettività ai principi di funzione minima e transizione verso interconnessioni specifiche del servizio.*	*L'agenzia espande l'implementazione dei meccanismi di isolamento dei profili degli endpoint e delle applicazioni a una maggiore architettura di rete con microperimetri in ingresso/uscita e interconnessioni specifiche per il servizio.*	*L'architettura di rete dell'agenzia è costituita da microperimetri in ingresso/uscita completamente distribuiti e da un'ampia microsegmentazione basata su profili applicativi con connettività dinamica just-in-time e just-enough per interconnessioni specifiche del servizio.*
GESTIONE DEL TRAFFICO DI RETE (NUOVA FUNZIONE)	*L'agenzia implementa manualmente regole e configurazioni di rete statiche per gestire il traffico durante il provisioning dei servizi, con capacità di monitoraggio limitate (ad esempio, monitoraggio delle prestazioni delle applicazioni o rilevamento delle anomalie) e audit manuali e revisioni delle modifiche del profilo per applicazioni mission-critical.*	*L'agenzia stabilisce profili di applicazione con caratteristiche di gestione del traffico distinte e inizia a mappare tutte le applicazioni a questi profili. L'agenzia si espande applicazione di regole statiche a tutte le applicazioni ed esegue audit manuali periodici delle valutazioni del profilo applicativo.*	*L'Agenzia implementa regole e configurazioni di rete dinamiche per l'ottimizzazione delle risorse che vengono periodicamente adattate in base alla consapevolezza automatizzata del rischio e valutazioni e monitoraggio del profilo applicativo sensibile al rischio.*	*L'agenzia implementa dinamiche Regole e configurazioni di rete che si evolvono continuamente per soddisfare le esigenze del profilo delle applicazioni e ridefinire le priorità delle applicazioni in base alla criticità della missione, al rischio, ecc.*
CRITTOGRAFIA DEL TRAFFICO (PRECEDENTEMENTE CRITTOGRAFIA)	*Agency crittografa il traffico minimo e si affida a processi manuali o ad hoc per gestire e proteggere le chiavi di crittografia.*	*L'agenzia inizia a crittografare tutto traffico verso applicazioni interne, per preferire la crittografia per il traffico verso applicazioni esterne, per formalizzare i criteri di gestione delle chiavi e per proteggere le chiavi di crittografia server/servizio.*	*L'agenzia garantisce la crittografia per tutti gli interni e protocolli di traffico esterno, gestisce l'emissione e la rotazione di chiavi e certificati e inizia a incorporare le migliori pratiche per l'agilità crittografica.*	*L'agenzia continua a crittografare Traffico come appropriato, applica i principi dei privilegi minimi per la gestione sicura delle chiavi in tutta l'azienda e incorpora le best practice per l'agilità crittografica il più ampiamente possibile.*
RESILIENZA DELLA RETE (NUOVA FUNZIONE)	*L'agenzia configura le funzionalità di rete caso per caso per soddisfare solo le richieste di disponibilità delle singole applicazioni con meccanismi di resilienza limitati per carichi di*	*L'agenzia inizia a configurare le funzionalità di rete per gestire le richieste di disponibilità per applicazioni aggiuntive ed espandere i meccanismi di resilienza per i*	*Agency ha configurato le funzionalità di rete per gestire dinamicamente le richieste di disponibilità e i meccanismi di resilienza per la*	*L'agenzia integra la consegna olistica e la consapevolezza nell'adattarsi ai cambiamenti nelle richieste di disponibilità per tutti i carichi di lavoro e fornisce resilienza proporzionata.*

FUNCTION	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
	lavoro non considerati mission-critical.	*carichi di lavoro non considerati mission-critical.*	*maggior parte delle loro applicazioni.*	
CAPACITÀ DI VISIBILITÀ E ANALISI	*L'agenzia incorpora limitate capacità di monitoraggio della rete incentrate sui confini con Analisi minima per iniziare a sviluppare la consapevolezza situazionale centralizzata.*	*L'Agenzia impiega capacità di monitoraggio della rete basate su indicatori noti di compromissione (inclusa l'enumerazione della rete) per sviluppare la consapevolezza situazionale in ogni ambiente e inizia a correlare la telemetria tra tipi di traffico e ambienti per l'analisi e le attività di ricerca delle minacce.*	*L'Agenzia implementa funzionalità di rilevamento della rete basate sulle anomalie per sviluppare la consapevolezza situazionale in tutti gli ambienti inizia a correlare la telemetria da più fonti per l'analisi e incorpora processi automatizzati per solide attività di ricerca delle minacce.*	*L'agenzia mantiene la visibilità sulla comunicazione attraverso tutte le reti dell'agenzia e ambienti abilitando al contempo la consapevolezza situazionale a livello aziendale e funzionalità di monitoraggio avanzate che Automatizza la correlazione dei dati di telemetria in tutte le origini di rilevamento.*
CAPACITÀ DI AUTOMAZIONE E ORCHESTRAZIONE	*L'agenzia utilizza processi manuali per gestire la configurazione e il ciclo di vita delle risorse per le reti e gli ambienti dell'agenzia con integrazione periodica dei requisiti delle policy e della consapevolezza situazionale.*	*L'agenzia inizia a utilizzare metodi automatizzati per gestire la configurazione e il ciclo di vita delle risorse per alcune reti o ambienti dell'agenzia e garantisce che tutte le risorse abbiano una durata definita in base a criteri e telemetria.*	*L'agenzia utilizza metodi automatizzati di gestione delle modifiche (ad esempio, CI/CD) per gestire la configurazione e il ciclo di vita delle risorse per tutte le reti e gli ambienti dell'agenzia, rispondendo e applicando politiche e protezioni contro i rischi percepiti.*	*Le reti e gli ambienti delle agenzie sono definiti utilizzando l'infrastruttura come codice gestita da metodi automatizzati di gestione delle modifiche, tra cui l'avvio e la scadenza automatizzati per allinearsi alle mutevoli esigenze.*
CAPACITÀ DI GOVERNANCE	*L'agenzia implementa politiche di rete statiche (accesso, protocolli, segmentazione, avvisi e bonifica) con un approccio incentrato sulle protezioni perimetrali.*	*L'agenzia definisce e inizia ad attuare le politiche su misura per i singoli segmenti e risorse di rete, ereditando al contempo le regole a livello aziendale, se del caso.*	*L'Agenzia incorpora l'automazione nell'attuazione di politiche su misura e facilita la transizione da Protezioni focalizzate sul perimetro.*	*L'Agenzia implementa politiche di rete a livello aziendale che consentono controlli locali su misura; aggiornamenti dinamici; e connessioni esterne sicure in base ai flussi di lavoro delle applicazioni e degli utenti.*

PILASTRO 4: APPLICATIONS AND WORKLOADS

Le applicazioni e i carichi di lavoro includono sistemi, programmi per computer e servizi eseguiti in locale, su dispositivi mobili e in ambienti cloud.

OBIETTIVI

- *Gestire e proteggere le loro applicazioni distribuite,*
- *Garantire la distribuzione sicura delle applicazioni.*

I controlli granulari degli accessi e le protezioni integrate dalle minacce possono offrire una maggiore consapevolezza della situazione e mitigare le minacce specifiche dell'applicazione.

Nella tabella 5 sono elencate le funzioni del carico di lavoro delle applicazioni relative al modello ZT, *nonché le considerazioni relative a visibilità e analisi, automazione e orchestrazione e governance nel contesto delle applicazioni e dei carichi di lavoro.*

TABLE 5: APPLICATIONS AND WORKLOADS

FUNCTION	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
ACCESSO ALLE APPLICAZIONI (PRECEDENTEMENTE AUTORIZZAZIONE ACCESSO)	*L'agenzia autorizza l'accesso alle applicazioni principalmente in base all'autorizzazione locale e agli attributi statici.*	*L'agenzia inizia a implementare funzionalità di autorizzazione dell'accesso alle applicazioni che incorporano informazioni contestuali (ad esempio, identità, conformità del dispositivo e/o altri attributi) per richiesta con scadenza.*	*Agency automatizza le decisioni di accesso alle applicazioni con informazioni contestuali estese e condizioni di scadenza applicate che aderiscono ai principi dei privilegi minimi.*	*L'agenzia autorizza continuamente l'accesso alle applicazioni, incorporando analisi dei rischi in tempo reale e fattori come il comportamento o i modelli di utilizzo.*
PROTEZIONI DALLE MINACCE ALLE APPLICAZIONI (PRECEDENTEMENTE THREAT PROTECTION)	*Le protezioni dalle minacce delle agenzie hanno un'integrazione minima con i flussi di lavoro delle applicazioni, applicando l'uso generico Protezioni per minacce note.*	*L'agenzia integra le protezioni dalle minacce nei flussi di lavoro delle applicazioni mission-critical, applicando Protezioni contro le minacce note e alcune minacce specifiche dell'applicazione.*	*Agency integra le protezioni dalle minacce in tutti i flussi di lavoro delle applicazioni, proteggendo da alcuni Minacce mirate e specifiche dell'applicazione.*	*Agency integra protezioni avanzate dalle minacce in tutti i flussi di lavoro delle applicazioni, offrendo visibilità in tempo reale e protezioni content-aware contro attacchi sofisticati su misura per le applicazioni.*
APPLICAZIONI ACCESSIBILI (PRECEDENTEMENTE ACCESSIBILITY)	*Agency rende disponibili alcune applicazioni mission-critical solo su reti private e connessioni di rete pubbliche protette (ad esempio, VPN) con monitoraggio.*	*Agency rende disponibili alcune delle sue applicazioni mission-critical applicabili su reti pubbliche aperte agli utenti autorizzati che necessitano tramite connessioni intermediate.*	*L'agenzia rende disponibile la maggior parte delle applicazioni mission-critical applicabili tramite connessioni di rete pubbliche aperte agli utenti autorizzati, se necessario.*	*L'Agenzia rende disponibili tutte le applicazioni applicabili su reti pubbliche aperte agli utenti e ai dispositivi autorizzati, se del caso, se necessario.*
SVILUPPO SICURO DELLE APPLICAZIONE E FLUSSO DI LAVORO DELLA DISTRIBUZIONE (NUOVA FUNZIONE)	*Agency dispone di ambienti di sviluppo, test e produzione ad hoc con meccanismi di distribuzione del codice non affidabili.*	*L'agenzia fornisce l'infrastruttura per gli ambienti di sviluppo, test e produzione (compresa l'automazione) con meccanismi formali di distribuzione del codice attraverso pipeline CI/CD e controlli di accesso necessari a supporto dei principi dei privilegi minimi.*	*L'agenzia utilizza team distinti e coordinati per lo sviluppo, la sicurezza e le operazioni, rimuovendo al contempo l'accesso degli sviluppatori all'ambiente di produzione per la distribuzione del codice.*	*Agency sfrutta carichi di lavoro immutabili ove possibile, consentendo solo l'effetto delle modifiche tramite la ridistribuzione e rimuove l'accesso dell'amministratore agli ambienti di distribuzione a favore di processi automatizzati per la distribuzione del codice.*
TEST SICUREZZA DELLE APPLICAZIONI (PRECEDENTEMEN	*L'agenzia esegue test di sicurezza delle applicazioni prima della distribuzione,*	*L'agenzia inizia a utilizzare metodi di test statici e dinamici (ovvero l'applicazione è in*	*L'Agenzia integra i test di sicurezza delle applicazioni nel processo di sviluppo*	*Agency integra i test di sicurezza delle applicazioni durante tutto il*

FUNCTION	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
TE APPLICATION SECURITY)	*principalmente tramite metodi di test manuali.*	*esecuzione) per eseguire test di sicurezza, inclusa l'analisi manuale degli esperti, prima della distribuzione dell'applicazione.*	*e distribuzione delle applicazioni, compreso l'uso di metodi di test dinamici periodici.*	*ciclo di vita dello sviluppo software in tutta l'azienda con test automatizzati di routine delle applicazioni distribuite.*
CAPACITÀ *di* VISIBILITÀ E ANALISI	*L'agenzia esegue alcuni monitoraggi delle prestazioni e della sicurezza delle applicazioni mission-critical con aggregazione e analisi limitate.*	*L'agenzia inizia ad automatizzare il profilo dell'applicazione (ad esempio, stato, integrità e prestazioni) e il monitoraggio della sicurezza per migliorare la raccolta, l'aggregazione e l'analisi dei log.*	*Agency automatizza il monitoraggio dei profili e della sicurezza per la maggior parte delle applicazioni con euristica per identificare le tendenze specifiche dell'applicazione e a livello aziendale e perfeziona i processi nel tempo per colmare le lacune nella visibilità.*	*Agency esegue un monitoraggio continuo e dinamico su tutte le applicazioni per mantenere una visibilità completa a livello aziendale.*
CAPACITÀ DI AUTOMAZIONE E ORCHESTRAZIONE	*L'agenzia stabilisce manualmente la posizione di hosting delle applicazioni statiche e l'accesso al provisioning con manutenzione e revisione limitate.*	*L'Agenzia modifica periodicamente le configurazioni delle applicazioni (inclusi posizione e accesso) per soddisfare gli obiettivi di sicurezza e prestazioni pertinenti.*	*Agency automatizza le configurazioni delle applicazioni per rispondere ai cambiamenti operativi e ambientali.*	*Agency automatizza le configurazioni delle applicazioni per ottimizzare continuamente la sicurezza e le prestazioni.*
CAPACITÀ DI GOVERNANCE	*L'agenzia si basa principalmente su politiche di applicazione manuale per l'accesso alle applicazioni, lo sviluppo, la distribuzione, la gestione delle risorse software, test e valutazione della sicurezza (ST&E) per l'inserimento di tecnologie, l'applicazione di patch e il monitoraggio delle dipendenze del software.*	*L'agenzia inizia ad automatizzare l'applicazione delle policy per lo sviluppo delle applicazioni (incluso l'accesso all'infrastruttura di sviluppo), la distribuzione, la gestione delle risorse software, la ST&E all'inserimento tecnologico, l'applicazione di patch e il monitoraggio delle dipendenze software in base alle esigenze della missione (ad esempio, con la distinta base software).*	*L'agenzia implementa policy su più livelli e personalizzate a livello aziendale per le applicazioni e tutti gli aspetti dello sviluppo delle applicazioni e dei cicli di vita di distribuzione e sfrutta l'automazione, dove possibile, per sostenere l'applicazione.*	*Agency automatizza completamente le policy che regolano lo sviluppo e la distribuzione delle applicazioni, inclusa l'incorporazione di aggiornamenti dinamici per le applicazioni tramite la pipeline CI/CD.*

PILASTRO 5: DATA

I dati includono tutti i file e i frammenti strutturati e non strutturati che risiedono o hanno risieduto in sistemi, dispositivi, reti, applicazioni, database, infrastrutture e backup federali (inclusi ambienti locali e virtuali), nonché i metadati associati.

OBIETTIVI

- *Proteggere i dati nei dispositivi, nelle applicazioni e sulle reti in conformità con i requisiti federali.*
- *Inventariare, categorizzare ed etichettare i dati; proteggere i dati inattivi e in transito; e implementare meccanismi per rilevare e fermare l'esfiltrazione dei dati.*
- *Elaborare e rivedere attentamente le politiche di governance dei dati per garantire che tutti gli aspetti della sicurezza del ciclo di vita dei dati siano applicati in modo appropriato in tutta l'azienda.*

Nella tabella 6 sono elencate le funzioni dati relative al principio ZT*, nonché le considerazioni relative a* VISIBILITY *e* ANALYTICS*,* AUTOMATION *e* ORCHESTRATION *e* GOVERNANCE *nel contesto dei dati.*

TABLE 6: DATA

FUNCTION	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
GESTIONE INVENTARIO DEI DATI	*L'agenzia identifica e inventaria manualmente alcuni dati dell'agenzia (ad esempio, dati mission-critical).*	*L'agenzia inizia ad automatizzare i processi di inventario dei dati sia per ambienti locali che cloud, coprendo la maggior parte dei dati dell'agenzia e inizia a incorporare protezioni contro la perdita di dati.*	*Agency automatizza l'inventario e il monitoraggio dei dati a livello aziendale, coprendo tutti i dati dell'agenzia applicabile, con strategie di prevenzione della perdita di dati basate su attributi statici e/o etichette.*	*L'agenzia inventaria continuamente tutti i dati dell'agenzia applicabile e impiega solide strategie di prevenzione della perdita di dati che bloccano dinamicamente la sospetta esfiltrazione dei dati.*
CATEGORIZZAZIONE DEI DATI (NUOVA FUNZIONE)	*L'agenzia impiega capacità di categorizzazione dei dati limitate e ad hoc.*	*L'agenzia inizia a implementare una strategia di categorizzazione dei dati con etichette definite e meccanismi di applicazione manuale.*	*Agency automatizza alcuni processi di categorizzazione ed etichettatura dei dati in modo coerente, a più livelli e mirato con formati semplici e strutturati e revisioni periodiche.*	*Agency automatizza la categorizzazione e l'etichettatura dei dati a livello aziendale con tecniche robuste; formati granulari e strutturati; e meccanismi per indirizzare tutti i tipi di dati.*
DISPONIBILITÀ DEI DATI (NUOVA FUNZIONE)	*Agency rende disponibili principalmente i dati dagli archivi dati locali con alcuni backup off-site.*	*Agency rende disponibili alcuni dati da archivi dati ridondanti e ad alta disponibilità (ad esempio, cloud) e gestisce backup off-site per i dati locali.*	*L'agenzia rende disponibili principalmente i dati provenienti da archivi di dati ridondanti e ad alta disponibilità e garantisce l'accesso ai dati storici.*	*L'agenzia utilizza metodi dinamici per ottimizzare la disponibilità dei dati, compresi i dati storici, in base alle esigenze dell'utente e dell'entità.*
ACCESSO AI DATI	*L'agenzia regola l'accesso di utenti ed entità (ad esempio, autorizzazioni per leggere, scrivere, copiare, concedere ad altri l'accesso, ecc.) ai dati attraverso controlli di accesso statici.*	*L'agenzia inizia a implementare controlli di accesso ai dati automatizzati che incorporano elementi di privilegio minimo in tutta l'azienda.*	*L'agenzia automatizza i controlli di accesso ai dati che considerano vari attributi come identità, rischio del dispositivo, applicazione, categoria di dati, ecc. E sono limitati nel tempo ove applicabile.*	*Agency automatizza i controlli dinamici di accesso ai dati just-in-time e just-enough in tutta l'azienda con la revisione continua delle autorizzazioni.*
CRITTOGRAFIA DEI DATI	*Agency crittografa i dati minimi dell'agenzia a riposo e in transito e si affida a processi manuali o ad hoc per gestire e proteggere le chiavi di crittografia.*	*L'Agenzia crittografa tutti i dati in transito e, ove possibile, i dati inattivi (ad esempio, dati mission-critical e dati archiviati in ambienti esterni) e inizia a formalizzare le politiche di gestione delle chiavi e le chiavi di crittografia sicure.*	*Agency crittografa tutti i dati inattivi e in transito all'interno dell'azienda nella massima misura possibile, inizia a incorporare l'agilità crittografica e protegge le chiavi di crittografia (ad esempio, i segreti non sono codificati e vengono ruotati regolarmente).*	*L'Agenzia crittografa i dati in uso ove appropriato, applica i principi dei privilegi minimi per la gestione sicura delle chiavi in tutta l'azienda e applica la crittografia utilizzando standard e crittografia aggiornati agilità nella misura del possibile.*

FUNCTION	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
CAPACITÀ DI VISIBILITÀ E ANALISI	*L'agenzia ha una visibilità limitata sui dati, tra cui posizione, accesso e utilizzo, con analisi che consistono principalmente in processi manuali.*	*L'agenzia ottiene visibilità in base alla gestione dell'inventario dei dati, alla categorizzazione, alla crittografia e ai tentativi di accesso, con alcuni Analisi e correlazione automatizzate.*	*L'agenzia mantiene la visibilità dei dati in modo più completo a livello aziendale con analisi e correlazioni automatizzate e inizia a utilizzare l'analisi predittiva.*	*L'agenzia ha visibilità sull'intero ciclo di vita dei dati con analisi solide, comprese le analisi predittive, che supportano viste complete dei dati dell'agenzia e valutazione continua della postura di sicurezza.*
CAPACITÀ DI AUTOMAZIONE E ORCHESTRAZIONE	*L'agenzia implementa il ciclo di vita dei dati e le politiche di sicurezza (ad esempio, accesso, utilizzo, archiviazione, crittografia, configurazioni, protezioni, backup, categorizzazione, sanificazione) attraverso processi manuali e potenzialmente ad hoc.*	*L'agenzia utilizza alcuni processi automatizzati per implementare il ciclo di vita dei dati e le politiche di sicurezza.*	*L'agenzia implementa il ciclo di vita dei dati e le policy di sicurezza principalmente attraverso metodi automatizzati per la maggior parte dei dati dell'agenzia in modo coerente, a più livelli e mirato in tutta l'azienda.*	*L'agenzia automatizza, nella massima misura possibile, i cicli di vita dei dati e le policy di sicurezza per tutti i dati dell'agenzia in tutta l'azienda.*
CAPACITÀ DI GOVERNANCE	*L'agenzia si basa su politiche di governance dei dati ad hoc (ad esempio, per la protezione, la categorizzazione, l'accesso, l'inventario, l'archiviazione, il ripristino, la rimozione, ecc.) con implementazione manuale.*	*L'agenzia definisce politiche di governance dei dati di alto livello e si basa principalmente sull'implementazione manuale e segmentata.*	*L'Agenzia inizia l'integrazione di Applicazione delle policy del ciclo di vita dei dati in tutta l'azienda, consentendo definizioni più unificate per le policy di governance dei dati.*	*Le policy del ciclo di vita dei dati dell'agenzia sono unificate nella massima misura possibile e applicate dinamicamente in tutta l'azienda.*

CROSS-CUTTING CAPABILITIES

Le funzionalità trasversali di VISIBILITY *e* ANALYTICS, AUTOMATION *e* ORCHESTRATION *e* GOVERNANCE *offrono l'opportunità di integrare i progressi in ciascuno dei 5 pilastri.*

- VISIBILITY *e* ANALYTICS: *supportano una visibilità completa che informa le decisioni sulle policy e facilita le attività di risposta.*
- AUTOMATION *e* ORCHESTRATION: *sfruttano queste informazioni per supportare operazioni solide e semplificate per gestire gli incidenti di sicurezza e rispondere agli eventi non appena si presentano.*
- GOVERNANCE: *consente alle agenzie di gestire e monitorare i propri requisiti normativi, legali, ambientali, federali e operativi a supporto del processo decisionale basato sul rischio; inoltre, garantiscono che siano disponibili le persone, i processi e la tecnologia adeguati a supportare gli obiettivi di missione, rischio e conformità.*

La tabella 7 fornisce un'evoluzione della maturità di alto livello per ciascuna di queste capacità trasversali.

TABLE 7: CROSS-CUTTING CAPABILITIES

FUNCTION	TRADITIONAL	INITIAL	ADVANCED	OPTIMAL
VISIBILITÀ E ANALISI	*L'agenzia raccoglie manualmente registri limitati in tutta l'azienda con bassa fedeltà e analisi minime.*	*L'agenzia inizia ad automatizzare la raccolta e l'analisi di registri ed eventi per le funzioni mission-critical e valuta regolarmente i processi per le lacune nella visibilità.*	*Agency espande la raccolta automatizzata di log ed eventi a livello aziendale (inclusi gli ambienti virtuali) per un'analisi centralizzata correlata tra più fonti.*	*L'agenzia mantiene una visibilità completa a livello aziendale tramite il monitoraggio dinamico centralizzato e l'analisi avanzata di registri ed eventi.*
AUTOMAZIONE E ORCHESTRAZIONE	*L'agenzia si affida a processi statici e manuali per orchestrare le operazioni e le attività di risposta con un'automazione limitata.*	*L'agenzia inizia ad automatizzare le attività di orchestrazione e risposta a supporto delle funzioni critiche della missione.*	*Agency automatizza le attività di orchestrazione e risposta a livello aziendale, sfruttando le informazioni contestuali provenienti da più fonti per prendere decisioni informate.*	*Le attività di orchestrazione e risposta delle agenzie rispondono dinamicamente alle mutevoli esigenze e ai cambiamenti ambientali a livello aziendale.*
GOVERNANCE	*L'agenzia implementa le politiche in modo ad hoc in tutta l'azienda, con politiche applicate tramite processi manuali o meccanismi tecnici statici.*	*L'agenzia definisce e inizia a implementare criteri per l'applicazione a livello aziendale con automazione minima e aggiornamenti manuali.*	*L'agenzia implementa policy su misura a più livelli in tutta l'azienda e sfrutta l'automazione ove possibile per supportare l'applicazione. Le decisioni relative ai criteri di accesso incorporano Informazioni contestuali provenienti da più fonti.*	*L'agenzia implementa e automatizza completamente le policy a livello aziendale che consentono controlli locali personalizzati con applicazione continua e aggiornamenti dinamici.*