Forcepoint

Sintesi della soluzione

Le soluzioni di Forcepoint per soddisfare gli standard NIST 2.0

SFIDA

- **Rischi e normative in evoluzione:** le organizzazioni lottano per gestire l'aumento dei rischi informatici e i cambiamenti dei requisiti normativi.
- **Politiche di sicurezza incoerenti:** i controlli di sicurezza frammentati nei canali di accesso creano mancanze di conformità.
- **Visibilità e controllo limitati:** la mancanza di gestione centralizzata e di avvisi rende difficile il rilevamento dei rischi per la sicurezza e delle violazioni delle politiche.

Soluzione

- **Sicurezza Zero Trust:** monitoraggio continuo che protegge i dati attraverso endpoint, rete, cloud, web ed e-mail.
- **Classificazione basata sull'IA:** il motore di data classification dell'apprendimento continuo intelligente migliora la precisione per un'efficace applicazione delle politiche.
- **Distribuzione flessibile:** opzioni su cloud, on-prem e ibride per allinearsi alle esigenze aziendali.

Risultato

- **Conformità semplificata:** la protezione centralizzata e adattiva riduce i rischi di perdita di dati prima che si verifichino violazioni della conformità.
- **Carico operativo ridotto:** la gestione unificata e l'applicazione automatizzata riducono al minimo lo sforzo manuale.
- **Consente la crescita del business:** proteggere la collaborazione per supportare l'innovazione aziendale.

Il framework di sicurezza informatica del National Institute of Standards and Technology (NIST) è una pietra miliare per molte organizzazioni che mirano a rafforzare la loro sicurezza in molti domini diversi nella salvaguardia di risorse e dati critici, migliorando al contempo la gestione e la risposta a rischi e minacce.

Con la passata introduzione del NIST 2.0 CSF (Cybersecurity Framework) nel febbraio 2024, la nuova linea guida aiuta le organizzazioni a migliorare la loro posizione di sicurezza informatica con un approccio più semplificato.

Forcepoint riconosce il ruolo significativo che il NIST svolge nel guidare le organizzazioni verso pratiche di sicurezza migliori. Ci impegniamo a sostenere questi sforzi fornendo soluzioni che aiutano a identificare, classificare e proteggere i dati sensibili, abilitando al contempo il rilevamento e la risposta a potenziali incidenti di fuoriuscite. Allineandosi ai principi del NIST, Forcepoint consente alle organizzazioni di soddisfare gli standard di conformità, migliorare la protezione dei dati e difendersi dai rischi nel panorama sempre più digitale di oggi.

Cos'è il NIST?

Il National Institute of Standards and Technology è un'agenzia del Dipartimento del Commercio degli Stati Uniti che fornisce guida su conformità, privacy e sicurezza. Nel regno della sicurezza informatica, il NIST Cybersecurity Framework (NIST CSF) offre informazioni sulle funzioni chiave per consentire alle organizzazioni di attivarsi e realizzare un programma di sicurezza informatica di successo. Il framework delinea le funzioni di Identificare, Proteggere, Rilevare, Rispondere e Recuperare con la funzione generale, Governare, che consente all'azienda di determinare quali decisioni si adattano meglio alla sua strategia. Essendo un framework volontario, NIST CSF è progettato per offrire una guida di alto livello mentre altri standard come NIST SP 800-53, 800-221, 800-171 e altri forniscono linee guida specifiche.

Proteggere i dati dalle minacce emergenti

Il framework della sicurezza informatica di NIST consente alle organizzazioni di essere flessibili nella loro postura di sicurezza informatica. CSF descrive i risultati desiderati dei diversi controlli di sicurezza ad alto livello, fornendo al contempo gli strumenti e le risorse per una descrizione più granulare di processi, persone e tecnologia.

Con l'adozione sempre crescente di nuove tecnologie come l'IA generativa, molte organizzazioni affrontano la sfida di proteggere i loro dati sensibili mentre utilizzano questi strumenti. L'abuso di questi strumenti, intenzionale o meno, può portare a gravi conseguenze per le organizzazioni. Informazioni riservate o sensibili possono essere trapelate su questi strumenti, oppure l'addestramento di un modello di IA può essere avvelenato a causa di contenuti dannosi. Forcepoint si dedica ad aiutare le organizzazioni a ottenere visibilità sui loro dati, proteggerli e prevenirne l'uso improprio.

Il CSF continua a fornire guida e migliori pratiche per le organizzazioni nella realizzazione, implementazione e mantenimento dei propri programmi di sicurezza informatica. Grazie alla nuova tecnologia, le organizzazioni dovranno pensare a come utilizzare questi strumenti in modo da poter comunicare, misurare e monitorare i rischi.

La protezione con Zero Trust

Incorporare Zero Trust rappresenta la pratica e la comprensione che ogni richiesta può rappresentare una potenziale minaccia. Applicazioni, sistemi e persone non sono attendibili a meno che non possano essere autenticati, all'interno o all'esterno della rete.

Il framework NIST 2.0 ha abbracciato i principi dell'architettura Zero Trust, in cui le funzioni chiave si concentrano sulla Gestione delle identità e degli accessi e sulla Gestione degli accessi privilegiati. Queste linee guida e l'architettura aiutano le organizzazioni a mitigare il rischio proteggendo al contempo i dati.

Forcepoint offre soluzioni di sicurezza incentrate sui dati con Zero Trust in mente. Ciò consente alle organizzazioni di mitigare il rischio prevenendo le fuoriuscite di dati sensibili per consentire loro di rimanere allineati alla conformità, indipendentemente da dove si trovino i loro dipendenti o i loro dati.

Navigare tra i rischi per la sicurezza e i requisiti di conformità in evoluzione

Il NIST Cybersecurity Framework (CSF) 2.0 fornisce alle organizzazioni un approccio flessibile e di alto livello per gestire i rischi di sicurezza informatica. Tuttavia, l'implemento efficace delle sue funzioni principali e la priorità ai controlli restano una sfida. Le organizzazioni devono determinare quali misure di sicurezza si allineano meglio alle loro esigenze aziendali, garantendo al contempo l'adattabilità a lungo termine.

Poiché NIST CSF è una linea guida volontaria, alcune organizzazioni rischiano di adottare un approccio "check-the-box", concentrandosi solo sulla conformità piuttosto che costruire una strategia di sicurezza dinamica e resiliente. Per massimizzare l'efficacia, le aziende devono valutare continuamente i rischi, affinare le politiche di sicurezza e allineare le risorse per stare al passo con le minacce in evoluzione.

Principali sfide di conformità che le organizzazioni devono affrontare:

- → **Giocare d'anticipo sulle minacce e sui regolamenti in evoluzione:** le aziende lottano per stare al passo con i rischi informatici sempre più sofisticati e i cambiamenti dei requisiti normativi.
- → **Applicazione incoerente delle politiche:** molte organizzazioni mancano di una strategia di sicurezza unificata tra endpoint, app SaaS, traffico web ed e-mail, portando a lacune nella sicurezza e rischi di conformità.
- → **Lacune nella visibilità e nel controllo:** senza la gestione centralizzata della protezione dei dati e l'applicazione in tempo reale, l'identificazione delle lacune della sicurezza, delle violazioni delle politiche e delle minacce interne diventa significativamente più difficile.

Per aderire con successo al NIST 2.0 e rafforzare la resilienza della sicurezza, le organizzazioni hanno bisogno di un approccio proattivo e basato sul rischio che garantisca l'applicazione delle politiche unificata, l'individuazione della minaccia in tempo reale e il monitoraggio continuo in tutti gli ambienti digitali.

Un approccio unificato e adattivo alla protezione dei dati

Le organizzazioni che adottano NIST CSF 2.0 hanno bisogno di un approccio strutturato alla gestione del rischio, all'applicazione delle politiche e alla protezione dei dati che si allinei con le funzioni principali del framework. Forcepoint fornisce soluzioni progettate per aiutare le organizzazioni a soddisfare questi requisiti migliorando le operazioni di sicurezza, riducendo la complessità della conformità e affrontando i rischi per la sicurezza prima che diventino violazioni della conformità.

Framework Zero Trust Security

L'architettura di protezione dei dati di Forcepoint si basa sui principi Zero Trust, garantendo che l'utilizzo dei dati sia monitorato e verificato continuamente, che vengano applicate le politiche del privilegio minimo e i potenziali rischi, sia esterni che interni, vengano mitigati in tempo reale. Questo approccio si allinea alle raccomandazioni del NIST per la gestione proattiva del rischio e il controllo degli accessi.

Gestione unificata delle politiche e della conformità

- → **Politiche di sicurezza unificate:** un unico framework di politiche applica controlli di sicurezza uniformi su endpoint, app SaaS, web ed e-mail, affrontando l'esigenza del NIST per la gestione integrata della sicurezza.
- → **Controlli di conformità automatizzati:** politiche pre-costruite e personalizzabili per la protezione dei dati, il controllo degli accessi e la risposta agli incidenti in linea con le raccomandazioni del NIST CSF 2.0.
- → **Classificazione dei dati basata sull'IA:** identifica e categorizza con precisione i dati sensibili a riposo, in movimento e in uso, riducendo i punti ciechi della conformità.

Rilevamento e applicazione basati sul comportamento

- → **Risk-Adaptive Protection:** utilizza l'analisi comportamentale per regolare automaticamente l'applicazione delle politiche in base ai livelli di rischio in tempo reale.
- → **Analisi forense e indagini sugli incidenti:** fornisce registrazione e analisi dettagliate degli eventi di sicurezza e delle violazioni delle politiche, aiutando le organizzazioni a rafforzare i loro processi di risposta agli incidenti.

Flessibilità e scalabilità della distribuzione

- → **Opzioni cloud, on-prem e ibride:** le organizzazioni possono distribuire le soluzioni di Forcepoint in base alle loro esigenze della infrastruttura di sicurezza, mantenendo la coerenza delle politiche.
- → **Gestione della sicurezza scalabile:** man mano che le esigenze di sicurezza e conformità si evolvono, Forcepoint consente alle organizzazioni di espandere la loro protezione senza interruzioni operative.

Le soluzioni di Forcepoint sono progettate per aiutare le organizzazioni a rendere operazionali le linee guida NIST 2.0, applicare le politiche di sicurezza su scala e rafforzare la loro postura generale di sicurezza informatica.

Semplificare la conformità per abilitare l'innovazione e la crescita

L'allineamento al NIST CSF 2.0 offre un approccio strutturato e basato sul rischio alla sicurezza informatica, aiutando le organizzazioni a rafforzare la protezione dei dati semplificando al contempo la conformità. Il monitoraggio continuo e i controlli adattivi riducono il rischio di perdita di dati e di violazioni identificando proattivamente le vulnerabilità prima che diventino violazioni dei regolamenti.

Integrando la moderna protezione dei dati con le operazioni aziendali, le organizzazioni possono abilitare la collaborazione sicura, supportare la trasformazione digitale e guidare l'innovazione senza compromettere la conformità. Un approccio strutturato e basato sul rischio rafforza la sicurezza, ottimizza le operazioni e consente alle aziende di concentrarsi sulla crescita.

Protezione dei dati

L'approccio alla protezione dei dati ovunque di Forcepoint protegge le informazioni sensibili su tutti i canali di accesso chiave, unificando l'applicazione della sicurezza e semplificando la gestione.

SOLUZIONI FORCEPOINT PER LA SICUREZZA DEI DATI
Forcepoint Data Loss Prevention (on-premise / Ibrido / Cloud) - Endpoint, Rete, Discovery, E-mail, app SaaS, Web
Forcepoint DSPM (Data Security Posture Management, On-Premises / Cloud)
Forcepoint Risk-Adaptive Protection (on-premise / cloud)

Protezione della rete

Le soluzioni di sicurezza di Forcepoint offrono una protezione completa su reti, applicazioni cloud, e-mail e web per prevenire la perdita di dati, controllare l'accesso e garantire la conformità.

SOLUZIONI DI FORCEPOINT NETWORK
Forcepoint (CASB e ZTNA)
Forcepoint Web Security (on-premise / ibrido / cloud)
Forcepoint Email Security (on-premise / cloud)
Forcepoint NGFW e Secure SD-WAN
Forcepoint RBI (Remote Browser Isolation) con CDR (Content Disarm and Reconstruction)

Le soluzioni di Forcepoint mappate al NIST CSF 2.0

FUNZIONE E SOTTO-CATEGORIA	DESCRIZIONE	PRODOTTI FORCEPOINT	VALORE
IDENTIFICAZIONE			
ID.AM-02	Vengono mantenuti gli inventari di software, servizi e sistemi gestiti dall'organizzazione	Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint possono fornire log e report che possono aiutare le organizzazioni a comprendere il traffico web, le applicazioni cloud e l'utilizzo dei dati. I controlli delle politiche consentono inoltre alle organizzazioni di determinare quali siti web e applicazioni cloud sono appropriati per l'uso, identificando o bloccando le categorie e le applicazioni cloud inappropriate o non sicure.
ID.AM-03	Vengono mantenute le rappresentazioni della comunicazione di rete autorizzata dell'organizzazione e dei flussi di dati di rete interni ed esterni	Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint possono monitorare l'utilizzo della rete, del web, del cloud e delle applicazioni private per reti/dispositivi gestiti e non gestiti. Con i controlli delle politiche, le soluzioni di Forcepoint possono identificare o bloccare l'accesso a queste destinazioni in base al rischio, alla conformità o persino alla perdita di produttività.
ID.AM-04	Vengono mantenuti gli inventari dei servizi forniti dai fornitori	Soluzioni di rete di Forcepoint	Forcepoint CASB, Web Security e NGFW possono anche rilevare, gestire e bloccare il traffico, nonché l'accesso, a siti esterni e applicazioni SaaS gestite e non gestite. Inoltre, Forcepoint NGFW può monitorare lo stato dei servizi.
ID.AM-05	Le risorse hanno la priorità in base alla classificazione, alla criticità, alle risorse e all'impatto sulla missione	Soluzioni Forcepoint per la sicurezza dei dati	Forcepoint aiuta a classificare, identificare e dare la priorità ai dati per la protezione attraverso Forcepoint DSPM, Forcepoint Classification, Data Detection and Response (DDR), Enterprise DLP e Risk-Adaptive Protection (RAP). Le soluzioni di rete di Forcepoint possono anche applicare le regole QoS e il monitoraggio dello stato di salute.
ID.AM-07	Vengono mantenuti gli inventari di dati e i metadati corrispondenti per i tipi di dati designati	Soluzioni Forcepoint per la sicurezza dei dati	Forcepoint consente alle organizzazioni di scoprire, inventariare e taggare i dati all'interno dell'ambiente, inclusa la capacità di mantenere il registro dei dati e delle parti responsabili.
ID.AM-08	Sistemi, hardware, software, servizi e dati sono gestiti durante tutto il loro ciclo di vita	Forcepoint Data Security	Forcepoint DSPM + DDR monitora continuamente i dati durante tutto il loro ciclo di vita per classificare e riclassificare i dati man mano che cambiano, tracciando il lignaggio e persino segnalando i dati ROT alla fine del ciclo di vita.

Le soluzioni di Forcepoint mappate al NIST CSF 2.0

FUNZIONE E SOTTO-CATEGORIA	DESCRIZIONE	PRODOTTI FORCEPOINT	VALORE
IDENTIFICAZIONE			
ID.RA-01	Le vulnerabilità delle risorse vengono identificate, convalidate e registrate	Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint possono identificare i rischi con i siti Web in tempo reale e affrontare i punteggi di rischio con le applicazioni cloud. Forcepoint offre approfondimenti sul motivo per cui tali risorse cloud sono rischiose, con prompt sullo schermo o messaggistica nella console. Inoltre, le funzionalità di Forcepoint NGFW IPS/Inspection valutano le vulnerabilità al di fuori dei canali web standard.
ID.RA-02	L'intelligence delle minacce informatiche viene ricevuta da forum e fonti di condivisione delle informazioni	Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint attingono ai feed delle minacce da varie fonti e ai nostri team dedicati che ricercano e analizzano le minacce informatiche. Queste informazioni vengono alimentate nel nostro ACE (Advanced Classification Engine) e congiuntamente alla nostra rete di ThreatSeeker Intelligence, che viene utilizzata per aiutare a identificare e bloccare le minacce informatiche con le nostre soluzioni. Con queste informazioni, le organizzazioni possono anche creare categorie personalizzate per le soluzioni di Forcepoint Web Security.
ID.RA-03	Vengono identificate e registrate le minacce interne ed esterne all'organizzazione	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Qualsiasi minaccia rilevata o bloccata dalle soluzioni di Forcepoint viene loggata e registrata. Le organizzazioni possono utilizzare queste informazioni per identificare la fonte, la destinazione e altri dettagli associati all'evento.
ID.RA-04	Vengono identificati e registrati i potenziali impatti e le probabilità di minacce che sfruttano le vulnerabilità	Soluzioni di rete di Forcepoint	Qualsiasi minaccia informatica che Forcepoint identifica e blocca viene loggata e registrata. Inoltre, Forcepoint aggiorna quotidianamente i propri motori di individuazione della minaccia. Altre soluzioni di Forcepoint come Remote Browser Isolation, Content Disarm and Reconstruction e Advanced Malware Detection sono progettate per identificare e bloccare le minacce zero-day.
ID.RA-05	Minacce, vulnerabilità, probabilità e impatti vengono utilizzati per comprendere il rischio inerente e informare sulla priorità della risposta al rischio	Soluzioni di rete di Forcepoint	Per qualsiasi minaccia informatica rilevata/bloccata da Forcepoint, i log sono disponibili per le organizzazioni per comprendere la fonte e il tipo di minaccia. Inoltre, le minacce sono classificate per livello di gravità a seconda del tipo di minaccia.
ID.RA-06	Le risposte al rischio vengono scelte, prioritizzate, pianificate, monitorate e comunicate	Soluzioni di rete di Forcepoint	Forcepoint assiste in questo obiettivo fornendo informazioni e monitoraggio in base alla minaccia rilevata o bloccata, fornendo informazioni come fonte, destinazione, tipo di minaccia, ecc.
ID.RA-07	Le modifiche e le eccezioni sono gestite, valutate per l'impatto sul rischio, registrate e tracciate		Qualsiasi modifica alla configurazione all'interno delle soluzioni di Forcepoint viene registrata in modo che le organizzazioni possano rivedere e implementare nuovamente le politiche in base alla loro valutazione. Inoltre, Forcepoint supporta un framework del flusso di lavoro e un'API bidirezionale per l'integrazione con le soluzioni di gestione dei ticket di terze parti.
ID.RA-09	L'autenticità e l'integrità di hardware e software vengono valutate prima dell'acquisizione e dell'utilizzo		I fornitori critici vengono valutati prima di essere acquisiti
ID.RA-10	Forcepoint fornisce hash per tutti i file scaricabili del software rilasciati.	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Forcepoint può condividere qualsiasi informazione relativa ai prodotti che offriamo, come amministrarli e qualsiasi dettaglio relativo al contratto.

Le soluzioni di Forcepoint mappate al NIST CSF 2.0

FUNZIONE E SOTTO-CATEGORIA	DESCRIZIONE	PRODOTTI FORCEPOINT	VALORE
IDENTIFICAZIONE			
ID.IM-02	I miglioramenti vengono identificati da test ed esercitazioni di sicurezza, inclusi quelli effettuati in coordinamento con i fornitori e le terze parti rilevanti		Le soluzioni di Forcepoint forniscono dettagli relativi alle minacce informatiche o agli eventi di protezione dei dati. I report generati da queste informazioni possono aiutare le organizzazioni a determinare quali aree necessitano di miglioramento.
ID.IM-03	I miglioramenti vengono identificati dall'esecuzione di procedure, attività e processi operativi		Le soluzioni di Forcepoint forniscono dettagli relativi alle minacce informatiche o agli eventi di protezione dei dati. I report generati da queste informazioni possono aiutare le organizzazioni a determinare quali aree necessitano di miglioramento.

FUNZIONE E SOTTO-CATEGORIA	DESCRIZIONE	PRODOTTI FORCEPOINT	VALORE
PROTEGGI			
PR.AA-01	Identità e credenziali sono gestite per dispositivi e utenti autorizzati	Soluzioni Forcepoint per la sicurezza dei dati	Indirettamente coinvolto, Forcepoint aiuta a limitare le interazioni con i dati sensibili che lasciano l'ambiente con Enterprise DLP e DLP per e-mail. Inoltre, Forcepoint CASB può offrire accesso condizionale per le app SaaS basate sull'autenticazione SAML SSO.
PR.AA-02	Le identità sono provate e legate alle credenziali in base al contesto delle interazioni	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint forniscono registri dettagliati delle attività che possono aiutare le organizzazioni a identificare utenti o sistemi che eseguono azioni. Con Risk-Adaptive Protection, le credenziali sono legate al contesto degli utenti, dei sistemi e delle azioni dei dati locali.
PR.AA-03	Utenti, servizi e hardware vengono autenticati	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint implementano i metodi Zero Trust per autenticare gli utenti. Inoltre, vengono utilizzate connessioni ad Active Directory, Single Sign-On e servizi di autenticazione multi-factor.
PR.AA-04	Le affermazioni di identità sono protette, trasmesse e verificate	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint che utilizzano qualsiasi SAML 2.0 SSO o l'autenticazione tramite sistemi federati seguono gli standard del settore.
PR.AA-05	Le autorizzazioni, i diritti e le autorizzazioni di accesso sono definiti in una politica, gestiti, applicati e rivisti e incorporano i principi del privilegio minimo e della separazione dei doveri	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le organizzazioni possono utilizzare Forcepoint per limitare l'accesso alle risorse web, alle applicazioni private, ai dati e alle reti. Inoltre, le soluzioni di Forcepoint offrono controlli degli accessi basati sul ruolo che possono vietare l'accesso alle aree all'interno delle soluzioni. In base al ruolo, gli utenti possono avere accesso per creare/modificare i controlli delle politiche, eseguire report e gestire la configurazione dell'infrastruttura o della piattaforma.

Le soluzioni di Forcepoint mappate al NIST CSF 2.0

FUNZIONE E SOTTO-CATEGORIA	DESCRIZIONE	PRODOTTI FORCEPOINT	VALORE
PROTEGGI			
PR.AT-01	Al personale viene fornita consapevolezza e formazione in modo che possieda le conoscenze e le competenze per svolgere compiti generali tenendo presente i rischi per la sicurezza informatica	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint possono fornire messaggistica personalizzata per la formazione. Questa forma di coaching degli utenti può consentire alle organizzazioni di essere più consapevoli delle potenziali minacce alla sicurezza informatica.
PR.AT-02	Agli individui in ruoli specializzati viene fornita consapevolezza e formazione in modo che possiedano le conoscenze e le competenze per svolgere compiti rilevanti tenendo presente i rischi per la sicurezza informatica	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Forcepoint richiede ai nostri partner e incoraggia gli utenti delle nostre soluzioni a sottoporsi alla nostra formazione sui prodotti. Forcepoint fornisce anche molti articoli di conoscenza, video pratici e documentazione per fornire competenze e conoscenze agli utenti delle nostre soluzioni.
PR.DS-01	La riservatezza, l'integrità e la disponibilità dei dati a riposo sono protette	Soluzioni Forcepoint per la sicurezza dei dati	Forcepoint può scoprire e classificare i dati-a-riposo con Forcepoint DSPM. Le soluzioni sono in grado di fornire questa funzionalità su tutte le risorse on-prem e cloud pur essendo una soluzione distribuita in modalità ibrida.
PR.DS-02	La riservatezza, l'integrità e la disponibilità dei dati in transito sono protette	Soluzioni Forcepoint per la sicurezza dei dati	Forcepoint DLP può proteggere i dati sensibili in transito su risorse Web come siti Web, applicazioni cloud e personalizzate, e-mail e canali degli endpoint. Le soluzioni sono in grado di fornire questa funzionalità su tutte le risorse on-prem e cloud pur essendo una soluzione distribuita in modalità ibrida.
PR.DS-10	La riservatezza, l'integrità e la disponibilità dei dati in uso sono protette	Soluzioni Forcepoint per la sicurezza dei dati	Forcepoint DLP protegge i dati sensibili prevenendo le fuoriuscite non autorizzate dei dati che vengono tagliati/copiati/incollati, le applicazioni che accedono ai file, la stampa, i supporti rimovibili e le e-mail. I controlli di applicazione della DLP sono attivi indipendentemente da dove si trovi la macchina dell'utente. I controlli sono attivi in loco e da remoto. Le soluzioni sono in grado di fornire questa funzionalità su tutte le risorse on-prem e cloud pur essendo una soluzione distribuita in modalità ibrida.
PR.PS-01	Vengono stabilite e applicate le pratiche di gestione della configurazione	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint hanno controlli predefiniti che possono consentire alle organizzazioni di applicare le migliori pratiche per quanto riguarda i controlli di rete e le esigenze di protezione dei dati. Queste politiche predefinite consentono alle organizzazioni di distribuire rapidamente i controlli di sicurezza per l'ambiente.
PR.PS-04	Le voci di registro vengono generate e rese disponibili per il monitoraggio continuo	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le organizzazioni possono utilizzare le soluzioni di Forcepoint per monitorare l'attività degli utenti su diversi canali per assicurarsi che siano conformi alla politica aziendale. Ciò include sia i canali di rete che i canali per le fuoriuscite di dati. Forcepoint DLP conserva i record di dati forensi per gli audit futuri.
PR.PS-05	Vengono prevenute l'installazione e l'esecuzione di software non autorizzato	Soluzioni di rete di Forcepoint	Forcepoint può prevenire il download di payload potenzialmente dannosi prevenendo in modo proattivo l'esecuzione sulla macchina dell'utente.

Le soluzioni di Forcepoint mappate al NIST CSF 2.0

FUNZIONE E SOTTO-CATEGORIA	DESCRIZIONE	PRODOTTI FORCEPOINT	VALORE
PROTEGGI			
PR.IR-01	Reti e ambienti sono protetti dall'accesso e dall'uso logico non autorizzato	Soluzioni di rete di Forcepoint	Le soluzioni di rete di Forcepoint possono prevenire agli utenti di accedere a categorie specifiche delle applicazioni Web e cloud e possono rilevare e prevenire il traffico in ingresso/in uscita alle reti oltre al traffico est-ovest tramite SD-WAN/NGFW.
PR.IR-02	Le risorse tecnologiche dell'organizzazione sono protette dalle minacce ambientali	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint possono essere distribuite in configurazioni ad alta disponibilità per conformarsi ai piani di recupero d'emergenza.
PR.IR-03	Vengono implementati i meccanismi per raggiungere i requisiti di resilienza in situazioni normali e avverse	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le soluzioni cloud di Forcepoint dispongono di meccanismi per mantenere l'uptime. Per qualsiasi distribuzione on-premise, Forcepoint consiglia distribuzioni ibride e ad alta disponibilità.

FUNZIONE E SOTTO-CATEGORIA	DESCRIZIONE	PRODOTTI FORCEPOINT	VALORE
RILEVA			
DE.CM-01	Le reti e i servizi di rete vengono monitorati per trovare eventi potenzialmente avversi	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Forcepoint monitora il traffico Web e di rete per la potenziale perdita di dati, il traffico di rete generale e dannoso e il monitoraggio delle minacce interne tramite Risk-Adaptive Protection e Forcepoint Insider Threat.
DE.CM-03	Le attività del personale e l'uso della tecnologia vengono monitorati per trovare eventi potenzialmente avversi	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint possono monitorare l'attività degli utenti con calcolo del rischio in tempo reale per monitorare gli eventi di rete e dei dati. Inoltre, Forcepoint Risk-Adaptive Protection può monitorare l'attività degli utenti con calcoli del rischio in tempo reale su oltre 130 indicatori di comportamento.
DE.CM-06	Le attività e i servizi dei fornitori di servizi esterni vengono monitorati per trovare eventi potenzialmente avversi	Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint possono monitorare l'attività degli utenti e le applicazioni della soluzione con calcolo del rischio in tempo reale per monitorare gli eventi di rete e di dati. Inoltre, i controlli di Forcepoint come ZTNA possono aiutare a monitorare le connessioni esterne alle applicazioni interne per identificare e bloccare eventi potenzialmente avversi.
DE.CM-09	Hardware e software di calcolo, ambienti di esecuzione e i loro dati vengono monitorati per trovare eventi potenzialmente avversi	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint possono monitorare l'attività degli utenti e le applicazioni della soluzione con calcolo del rischio in tempo reale per monitorare gli eventi di rete e di dati. Le soluzioni di Forcepoint monitorano/bloccano le fuoriuscite di dati e il traffico di rete per determinare se gli eventi sono avversi in base ai controlli delle politiche stabiliti.

Le soluzioni di Forcepoint mappate al NIST CSF 2.0

FUNZIONE E SOTTO-CATEGORIA	DESCRIZIONE	PRODOTTI FORCEPOINT	VALORE
RILEVA			
DE.AE-02	Gli eventi potenzialmente avversi vengono analizzati per comprendere meglio le attività associate	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Forcepoint può fornire dettagli degli incidenti che possono aiutare a determinare se un evento è avverso o meno, abilitando i team SOC con dettagli di log e analisi forensi approfonditi.
DE.AE-03	Le informazioni sono correlate da più fonti	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint possono fornire reportistica centralizzata per aiutare a consolidare gli incidenti e aiutare le organizzazioni a rispondere in modo appropriato. Inoltre, la rete ThreatSeeker correla da tutte le distribuzioni di Forcepoint per aiutare a identificare le minacce.
DE.AE-04	Sono compresi l'impatto stimato e la portata degli eventi avversi	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint possono fornire ricchi dettagli degli incidenti insieme a classificazioni di gravità e rischio per aiutare le organizzazioni a comprendere l'impatto.
DE.AE-06	Le informazioni sugli eventi avversi vengono fornite al personale e agli strumenti autorizzati	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint forniscono informazioni dettagliate sugli eventi che possono essere controllati per la visualizzazione da RBAC. Quando Forcepoint rileva un incidente, è possibile generare avvisi da inviare ai team appropriati tramite avvisi della dashboard, e-mail e integrazione con strumenti di terze parti (ad es. SIEM, sistemi di ticket)
DE.AE-07	L'intelligence delle minacce informatiche e altre informazioni contestuali sono integrate nell'analisi	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le politiche di Forcepoint utilizzano l'analisi contestuale e le integrazioni con altri feed (ad es. SIEM, feed di intelligence di terze parti) per identificare gli eventi di rischio e/o identificare e bloccare le azioni di fuoriuscite dei dati.
DE.AE-08	Gli incidenti vengono dichiarati quando gli eventi avversi soddisfano i criteri definiti per gli incidenti	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Forcepoint fornisce dettagli degli incidenti in base ai controlli delle politiche stabiliti violati per assistere le organizzazioni nel processo di dichiarazione.

Le soluzioni di Forcepoint mappate al NIST CSF 2.0

FUNZIONE E SOTTO-CATEGORIA	DESCRIZIONE	PRODOTTI FORCEPOINT	VALORE
RISPONDI			
RS.MA-01	Il piano di risposta agli incidenti viene eseguito in coordinamento con le terze parti rilevanti una volta dichiarato un incidente	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le politiche di Forcepoint offrono azioni proattive e reattive che si allineano ai piani di risposta agli incidenti dell'organizzazione. L'API bidirezionale aiuta anche nei flussi di lavoro di risposta agli incidenti con soluzioni di terze parti.
RS.MA-02	I report degli incidenti vengono smistati e convalidati	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint forniscono gestione centralizzata e reportistica per aiutare a smistare e indagare sulle minacce.
RS.MA-03	Gli incidenti vengono classificati e assegnati la priorità	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Gli incidenti di Forcepoint possono essere ordinati in base alla fonte, alla gravità, alla politica, ecc. La priorità può essere basata sulla gravità più recente, più alta, il punteggio di classificazione del rischio più elevato, ecc.
RS.MA-04	Gli incidenti vengono intensificati o elevati in base alle necessità	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Forcepoint fornisce informazioni dettagliate sugli incidenti con livelli di gravità/punteggi di rischio che possono aiutare a dare la priorità agli incidenti/casi per l'escalation.
RS.MA-05	Vengono applicati i criteri per avviare il recupero degli incidenti	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Forcepoint può fornire informazioni dettagliate su un incidente che possono contribuire ai processi di recupero degli incidenti.
RS.AN-03	Viene eseguita l'analisi per stabilire cosa è avvenuto durante un incidente e la causa principale dell'incidente	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Forcepoint può fornire informazioni dettagliate su un incidente per includere sorgente, destinazione, canale e regole violate insieme a informazioni forensi per gli eventi di protezione dei dati rilevati.
RS.AN-06	Le azioni eseguite durante un'indagine vengono registrate e l'integrità e la provenienza dei record vengono preservate	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Forcepoint mantiene un audit trail delle attività di amministrazione insieme ai dettagli degli incidenti forensi, che possono essere preservati all'interno di una posizione crittografata.

Le soluzioni di Forcepoint mappate al NIST CSF 2.0

FUNZIONE E SOTTO-CATEGORIA	DESCRIZIONE	PRODOTTI FORCEPOINT	VALORE
RISPONDI			
RS.AN-07	Vengono raccolti i dati e i metadati degli incidenti e vengono preservate la loro integrità e provenienza	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le soluzioni di Forcepoint raccolgono e archiviano le informazioni sugli incidenti forensi che vengono archiviate in un repository crittografato.
RS.AN-08	La grandezza di un incidente viene stimata e convalidata	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Forcepoint fornisce informazioni dettagliate sugli incidenti con livelli di gravità/punteggi di rischio che possono aiutare a dare la priorità agli incidenti/casi per l'escalation.
RS.CO-02	Gli stakeholder interni ed esterni vengono notificati degli incidenti	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Forcepoint può fornire informazioni sugli incidenti e inviare avvisi alle parti designate. Con Forcepoint DSPM, il registro degli asset può notificare ai vari proprietari dei dati di rilevamenti e modifiche alla classificazione o al rischio dei dati di loro responsabilità.
RS.CO-03	Le informazioni vengono condivise con gli stakeholder interni ed esterni designati	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le politiche di Forcepoint utilizzano l'analisi contestuale e le integrazioni con altri feed (ad es. SIEM, feed di intelligence di terze parti) per identificare gli eventi di rischio e/o identificare e bloccare le azioni di fuoriuscite dei dati.
RS.MI-01	Gli incidenti sono contenuti Forcepoint	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le politiche di Forcepoint offrono azioni proattive e reattive che si allineano ai piani di risposta agli incidenti dell'organizzazione. Forcepoint DLP può bloccare/mettere in quarantena automaticamente i dati per prevenire le fuoriuscite.
RS.MI-02	Gli incidenti vengono sradicati Forcepoint	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Le politiche di Forcepoint offrono azioni proattive e reattive che si allineano ai piani di risposta agli incidenti dell'organizzazione.

Le soluzioni di Forcepoint mappate al NIST CSF 2.0

FUNZIONE E SOTTO-CATEGORIA	DESCRIZIONE	PRODOTTI FORCEPOINT	VALORE
RISTABILIRE			
RC.RP-01	La parte di recupero del piano di risposta agli incidenti viene eseguita una volta avviata dal processo di risposta agli incidenti	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	La revisione degli incidenti e delle risposte di Forcepoint DLP può essere integrata nei piani di recupero e miglioramento dell'organizzazione.
RC.RP-06	La fine del recupero degli incidenti viene dichiarata in base ai criteri e viene completata la documentazione relativa all'incidente	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Forcepoint può aiutare le organizzazioni nel processo fornendo dettagli sugli incidenti.
RC.CO-04	Gli aggiornamenti pubblici sul recupero degli incidenti vengono condivisi utilizzando metodi e messaggistica approvati	Soluzioni Forcepoint per la sicurezza dei dati Soluzioni di rete di Forcepoint	Forcepoint può aiutare le organizzazioni fornendo dettagli degli incidenti su una violazione rilevata dalle soluzioni di Forcepoint, in modo da poter effettuare un aggiornamento e un messaggio.

forcepoint.com/contact