SINTESI DELLA SOLUZIONE

Accesso remoto sicuro per la forza lavoro degli enti pubblici su vasta scala

Sintesi preliminare

Gli enti pubblici devono affrontare una serie di potenziali situazioni di emergenza, come malattie, inondazioni, uragani e blackout. Gli enti pubblici devono fungere da punto di gestione e di coordinamento di fronte alle avversità, comunicando con i cittadini in modo chiaro e trasparente. L'attuazione di un piano di Business Continuity è essenziale per garantire che gli enti pubblici siano in grado di garantire le operazioni di fronte alle avversità e di prepararsi a potenziali calamità. Siamo entrati in una nuova era in cui ai lavoratori degli enti pubblici può essere richiesto di lavorare a distanza.

Una considerazione importante nello sviluppo di un piano di Business Continuity è che potrebbe non essere possibile sostenere le normali attività in sede. La capacità di supportare i dipendenti che lavorano a distanza è essenziale per garantire sia la Business Continuity che la sicurezza. Le soluzioni Fortinet offrono uno strumento integrato per supportare il telelavoro su larga scala. I firewall NGFW FortiGate integrano il supporto di SSL e VPN IPsec, consentendo ai telelavoratori di connettersi in modo sicuro alla rete dell'ente pubblico senza ulteriori licenze. Con la protezione degli endpoint fornita da FortiClient e l'autenticazione a più fattori (MFA) garantita da FortiAuthenticator, gli enti pubblici possono supportare il telelavoro e garantire la Business Continuity in tutta sicurezza.

La capacità di supportare in modo sicuro i telelavoratori è una componente essenziale del piano di Business Continuity e disaster recovery di qualsiasi ente pubblico. A causa di un blackout o un evento analogo, come anche di una malattia o un'alluvione che può rendere insicura la presenza dei dipendenti, un ente pubblico potrebbe non riuscire a sostenere le normali attività in sede.

In tali situazioni, un ente pubblico deve essere in grado di supportare una connettività remota sicura alla rete. Per oltre 400.000 clienti di Fortinet, la distribuzione della tecnologia esistente prevede già questa funzionalità. I firewall NGFW FortiGate integrano il supporto di SSL e VPN IPsec, consentendo una connettività sicura per i dipendenti che lavorano da postazioni di lavoro alternative.

Garantire la sicurezza dei telelavoratori degli enti pubblici con i firewall NGFW FortiGate

Le soluzioni Fortinet sono progettate appositamente per garantire facilità di utilizzo e manutenzione. I firewall NGFW FortiGate includono funzionalità di distribuzione zero-touch per garantire la Business Continuity e il supporto per il telelavoro. In questo modo, è possibile distribuire rapidamente le appliance in sedi distaccate con una preconfigurazione minima, nonché recuperare automaticamente le impostazioni di configurazione su connessioni sicure e completare la configurazione una volta che sono collegati in sede.

La VPN integrata in ogni firewall NGFW FortiGate offre un modello di distribuzione estremamente flessibile. I telelavoratori possono trarre vantaggio da un'esperienza senza client o accedere a funzionalità aggiuntive attraverso un thick client integrato nella soluzione di sicurezza degli endpoint FortiClient. I power user e i super user degli enti pubblici possono trarre vantaggio dalla distribuzione di un FortiAP o un firewall NGFW FortiGate per ulteriori funzionalità.

Il Fortinet Security Fabric sfrutta un sistema operativo Fortinet comune e un ambiente API (Application Programming Interface) aperto per creare un'architettura di sicurezza ampia, integrata e automatizzata. Grazie al Fortinet Security Fabric, tutti i dispositivi di un'organizzazione, compresi quelli distribuiti in remoto per supportare il telelavoro, possono essere monitorati e gestiti da un'unica interfaccia. Da un firewall NGFW FortiGate o una piattaforma di gestione centralizzata FortiManager distribuita nell'ambiente della sede centrale, il team di sicurezza può ottenere la piena visibilità di tutti i dispositivi e gli utenti collegati, indipendentemente dalla loro situazione di distribuzione.

Nel caso in cui calamità naturali o altri eventi dovessero interrompere le normali attività aziendali, un'organizzazione deve essere in grado di passare rapidamente a una forza lavoro completamente remota. Nella tabella 1 viene mostrato il numero di utenti VPN simultanei che ogni modello di firewall NGFW FortiGate può supportare.

Oltre a garantire la crittografia dei dati in transito tramite VPN, le soluzioni Fortinet offrono una serie di altre funzionalità che possono aiutare un'organizzazione a proteggere la propria forza lavoro remota. Tra queste, si annoverano:

- **Autenticazione a più fattori (MFA).** FortiToken e FortiAuthenticator consentono l'autenticazione a due fattori dei dipendenti remoti.
- **Data Loss Prevention (DLP).** FortiGate e FortiWiFi forniscono la funzionalità DLP per i telelavoratori, che è essenziale per i dirigenti che, in modalità di telelavoro, accedono frequentemente a dati aziendali sensibili.
- **Sicurezza degli endpoint.** FortiEDR fornisce una Advanced Threat Protection per i computer dei telelavoratori, compresa la risoluzione automatica.
- **Advanced Threat Protection.** FortiSandbox analizza il malware e altri contenuti sospetti all'interno di un ambiente sandbox prima che raggiungano la loro destinazione.

- **Connettività wireless.** Gli access point FortiAP garantiscono un accesso wireless sicuro alle postazioni di lavoro remote con gestione completa dell'integrazione e della configurazione da un'unica interfaccia.
- **Gestione degli accessi ai dispositivi.** FortiNAC è in grado di applicare i le policy BYOD (Bring Your Own Device) anche su connessioni VPN remote, consentendo all'organizzazione di controllare quali tipi di dispositivi possono connettersi e quali accessi ricevono.
- **Telefonia.** FortiFone è una soluzione di telefonia VoIP (Voice over IP) sicura, il cui traffico è protetto, gestito e monitorato da un firewall NGFW FortiGate. Disponibile come soft client e in varie versioni hardware.

Modello	Utenti VPN SSL simultanei	Utenti VPN IPsec simultanei	FortiAP gestiti (modalità tunneling)
100E	500	10.000	32
100F	500	16.000	64
300E	5.000	50.000	256
500E	10.000	50.000	256
600E	10.000	50.000	512
1100E	10.000	100.000	2.048
2000E	30.000	100.000	2.048
Tutti i modelli più grandi*	30.000	100.000	2.048
*3300E supporta 1.024 access point in modalità tunneling			

Tabella 1: Numero di connessioni VPN simultanee supportate da vari modelli di firewall NGFW FortiGate.

Casi d'uso dei prodotti Fortinet che supportano il telelavoro per gli enti pubblici

Non tutti i dipendenti di un ente pubblico richiedono lo stesso livello di accesso alle risorse quando sono in modalità di telelavoro. Fortinet fornisce soluzioni di telelavoro su misura per ogni dipendente remoto:

1. **Lavoratore di un ente pubblico standard.** La maggior parte di questi lavoratori richiede l'accesso alla posta elettronica, a Internet, alle teleconferenze, alla condivisione di file limitata e alle funzionalità specifiche in base al ruolo ricoperto (risorse umane ecc.) dalla postazione di telelavoro. È compreso l'accesso ai servizi Software-as-a-Service (SaaS) nel cloud, come Microsoft Office 365, nonché una connessione sicura alla rete dell'ente pubblico.

   Si connettono utilizzando il software client VPN integrato in FortiClient e verificano la propria identità con FortiToken per l'autenticazione a più fattori.

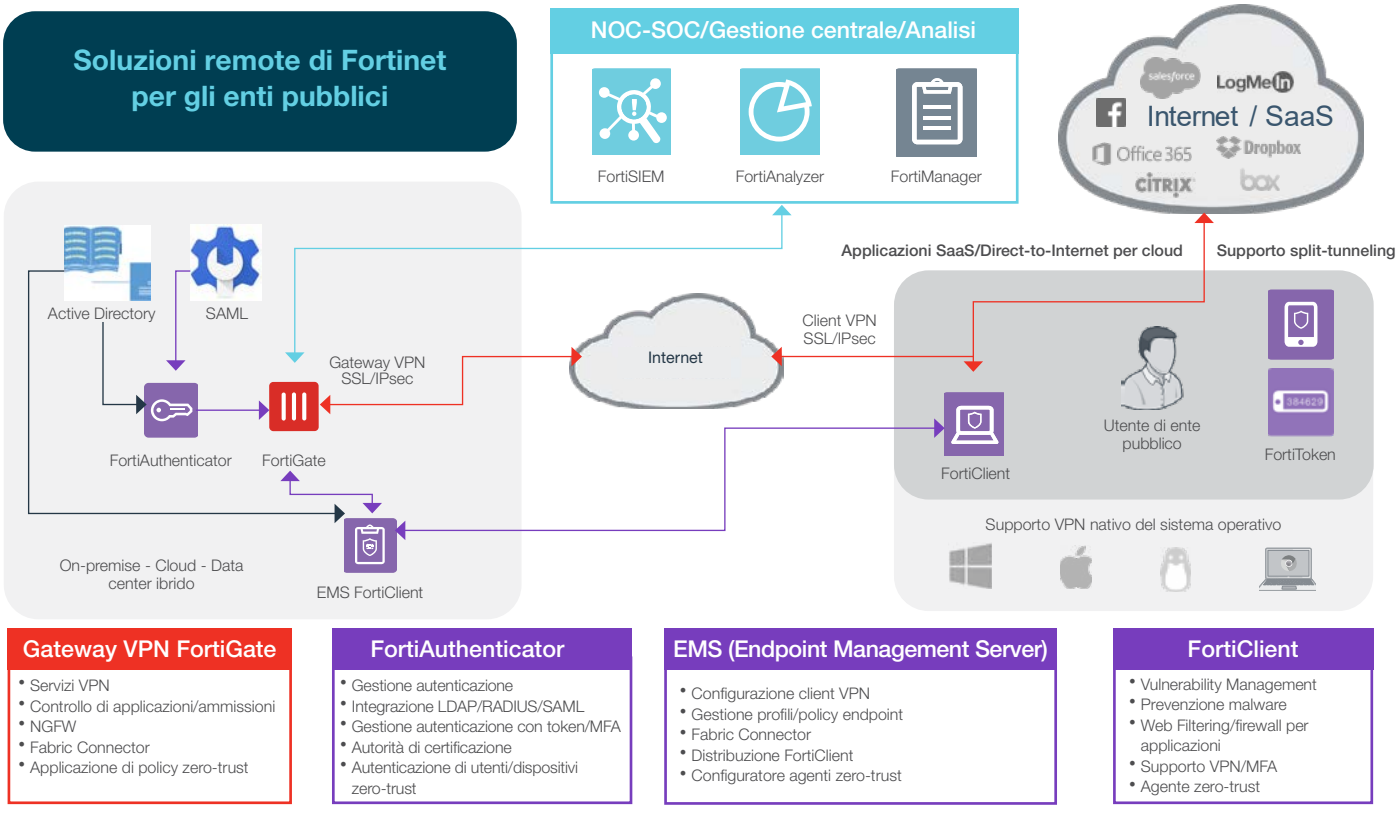

Figura 1: distribuzione della soluzione Fortinet per i lavoratori degli enti pubblici standard.

2. **Power user di enti pubblici.** I power user sono dipendenti di enti pubblici che richiedono un livello più elevato di accesso alle risorse dell'ente pubblico quando lavorano da una postazione remota. In ciò può rientrare la capacità di operare in più ambienti IT paralleli, ad esempio amministratori di sistema, tecnici di supporto IT e personale di emergenza. Ai power user, la distribuzione di un access point FortiAP presso la loro postazione di lavoro alternativa garantisce il livello di accesso e sicurezza di cui hanno bisogno, garantendo una connettività wireless sicura con tunneling sicuro e persistente verso la rete dell'ente pubblico. Gli access point FortiAP possono essere distribuiti con provisioning zero-touch (ZTP, Zero-Touch Provisioning) e saranno gestiti dai firewall NGFW FortiGate in ufficio. Se dovesse essere necessario distribuire un telefono dell'ente pubblico, può semplicemente collegarsi all'access point FortiAP per la connettività con l'ufficio dell'ente.

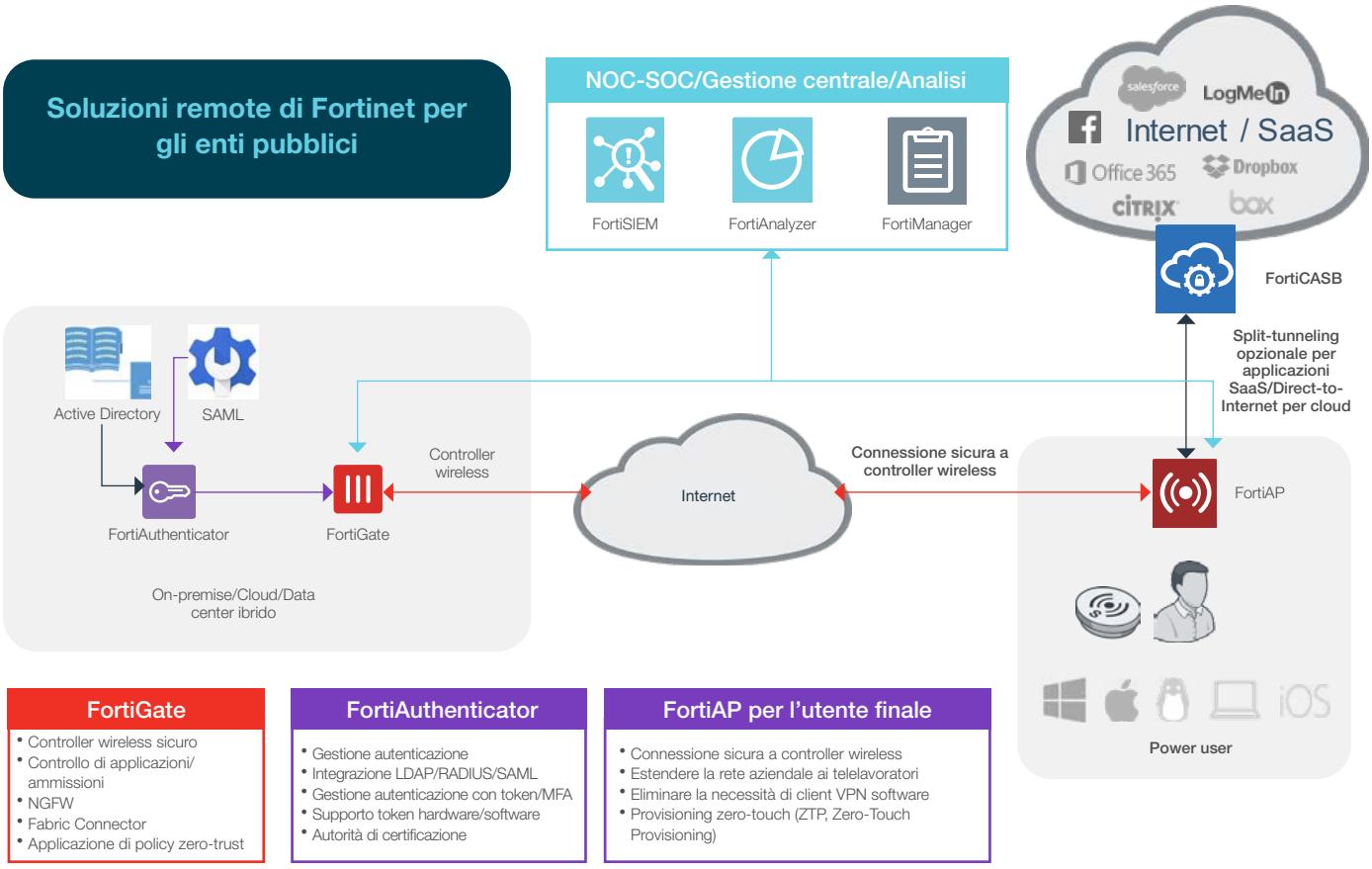

Figura 2: distribuzione di una soluzione Fortinet per il power user dell'ente pubblico.

3. **Super user di enti pubblici.** Un super user è un dipendente che richiede un accesso avanzato alle risorse riservate dell'ente pubblico, anche quando lavora da un ufficio alternativo. Spesso tratta informazioni estremamente sensibili e riservate. Questo profilo di dipendente include amministratori con accesso privilegiato al sistema, tecnici di supporto, partner di rilievo dell'ente pubblico e organizzazioni allineate al piano di continuità, personale di emergenza, dirigenti pubblici, ad esempio responsabili, presidenti, sindaci e il loro personale.

   Per i super user, la sede di lavoro alternativa deve essere configurata come un ufficio alternativo. Se da un lato richiede le stesse soluzioni dei lavoratori degli enti pubblici standard e dei power user, dall'altro richiede anche funzionalità aggiuntive. FortiAP può essere integrato con un'appliance NGFW FortiGate o FortiWiFi per una connettività wireless sicura con DLP integrato. FortiFone fornisce versioni soft client o hardware di telefonia tramite VoIP gestite e protette mediante firewall NGFW FortiGate in sede o una piattaforma di gestione centralizzata FortiManager distribuita presso la sede dell'ufficio.

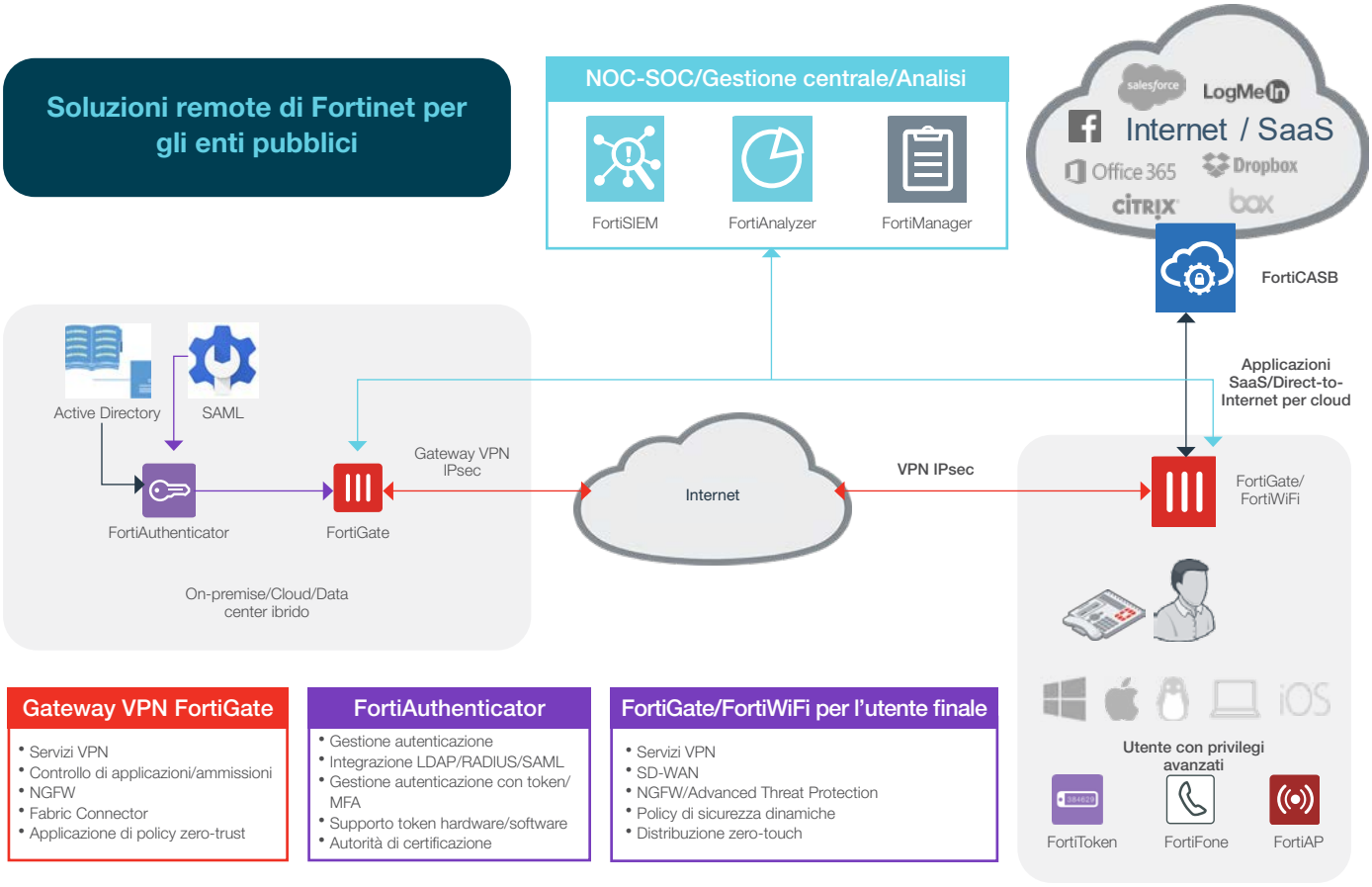

Figura 3: distribuzione di una soluzione Fortinet per il super user dell'ente pubblico.

Ottenere la piena integrazione della sicurezza con le soluzioni Fortinet

Il Fortinet Security Fabric consente una perfetta integrazione della forza lavoro remota di un ente pubblico. Tutte le soluzioni Fortinet sono collegate tramite il Fortinet Security Fabric, che garantisce visibilità, configurazione e monitoraggio tramite un'unica interfaccia. Una serie di Fabric Connector, un ambiente API aperto, il supporto della community DevOps e un ampio ecosistema Security Fabric esteso garantiscono l'integrazione con oltre 250 soluzioni di terzi.

Questo approccio è fondamentale quando gli enti pubblici stanno approntando un piano di Business Continuity poiché potrebbero essere costretti a passare a una forza lavoro completamente remota con poco o nessun preavviso. La visibilità e la gestione da un'unica interfaccia dell'architettura di sicurezza di assicura che il supporto del telelavoro non metta a rischio la sicurezza informatica.

Le seguenti soluzioni fanno parte del Fortinet Security Fabric e supportano un telelavoro sicuro:

- **FortiClient.** FortiClient rafforza la sicurezza degli endpoint grazie all'integrazione di visibilità, controllo e difesa proattiva, consentendo alle organizzazioni di individuare, monitorare e valutare i rischi degli endpoint in tempo reale.
- **FortiGate (BYOL, PAYG).** I firewall NGFW FortiGate utilizzano processori di sicurezza informatica appositamente realizzati per garantire la massima protezione, la visibilità end-to-end e il controllo centralizzato, oltre all'ispezione a elevate prestazioni del traffico in chiaro e crittografato.
- **FortiWiFi.** I gateway wireless FortiWiFi abbinano i vantaggi di sicurezza dei firewall NGFW FortiGate a un access point wireless, fornendo una soluzione di rete e sicurezza integrata per i telelavoratori.
- **FortiFone.** FortiFone garantisce comunicazioni vocali unificate con connettività VoIP protetta e gestita tramite firewall NGFW FortiGate. L'interfaccia del soft client FortiFone consente agli utenti di effettuare o ricevere chiamate, accedere alla segreteria telefonica, controllare la cronologia delle chiamate ed eseguire ricerche nella directory dell'organizzazione direttamente da un dispositivo mobile. Sono disponibili diverse opzioni hardware.
- **FortiToken.** FortiToken conferma l'identità degli utenti aggiungendo un secondo fattore al processo di autenticazione grazie a token basati su dispositivi fisici o applicazioni per dispositivi mobili.

- **FortiAuthenticator.** FortiAuthenticator fornisce servizi di autenticazione centralizzata, compresi servizi SSO, gestione dei certificati e gestione degli ospiti.
- **FortiAP.** FortiAP garantisce un accesso sicuro e wireless alle imprese distribuite e ai telelavoratori e può essere facilmente gestito da un firewall NGFW FortiGate o tramite cloud.
- **FortiWeb Cloud (BYOL, PAYG).** I WAF Fortinet proteggono le applicazioni web ospitate sia da vulnerabilità note che da minacce zero-day utilizzando metodi di rilevamento multilivello e correlati.
- **FortiManager (BYOL).** FortiManager fornisce un'unica interfaccia di gestione e controllo delle policy in tutta la Extended Enterprise per analizzare le minacce basate sul traffico a livello di rete. Include anche funzionalità per contenere gli attacchi avanzati e la scalabilità per gestire fino a 10.000 dispositivi Fortinet.
- **FortiAnalyzer (BYOL).** FortiAnalyzer garantisce la sicurezza informatica e la gestione dei registri sulla base dell'analisi per consentire un migliore rilevamento delle minacce e una maggiore prevenzione delle violazioni.
- **FortiSandbox (BYOL, PAYG).** Le soluzioni sandbox Fortinet offrono una potente combinazione di rilevamento avanzato, attenuazione automatizzata, informazioni dettagliate fruibili e distribuzione flessibile per bloccare gli attacchi mirati e la conseguente perdita di dati.

Una base sicura a garanzia della Business Continuity

Approntare un piano di Business Continuity e disaster recovery è di vitale importanza per qualsiasi organizzazione. Una sua componente importante è la capacità di supportare una forza lavoro in gran parte o completamente remota con poco o nessun preavviso.

Quando si sviluppano piani di Business Continuity, è fondamentale assicurarsi che l'organizzazione disponga delle risorse necessarie per proteggere la forza lavoro remota. Le soluzioni Fortinet, facilmente distribuibili e configurabili, consentono all'organizzazione di garantire pienamente sicurezza, visibilità e controllo, indipendentemente dall'ambiente di distribuzione.

FORTINET®

www.fortinet.com

giugno30,20209:41AM
C:\Users\rafal.kotkowski\Downloads\Fortinet\P-358235\09_wf\Work\A-358235-1090227_FortinetIT\sb-FA-secure-remote-access-for-your-government-workforce-482020-a4_IT\sb-FA-secure-remote-access-for-your-government-workforce-482020-a4_IT