SECURE WORKSTATION

Cos'è

Il servizio gestito per proteggere la vostra rete e i vostri sistemi informativi (client e server) da accessi non autorizzati.
Il servizio Secure Workstation, grazie a un sapiente mix tra strumenti e professionalità dei nostri specialisti, garantisce il blocco proattivo di attacchi e minacce provenienti da internet, agevola il costante aggiornamento delle policy di sicurezza e aiuta a prevenire i comportamenti "a rischio" degli utilizzatori.
Funzionalità di sicurezza avanzate come *stateful inspection*, *web filtering*, *advanced threat control* e *sand box analyzer* sono state racchiuse in un unico servizio, versatile ed efficace, in grado di garantire una protezione completa alle reti aziendali di ogni dimensione.

Caratteristiche del servizio e funzionalità supportate

- Assesment iniziale del sistema informativo del cliente e produzione di un report di remediation.
- Check preventivo e applicazione delle remediation suggerite
  - Upgrade/eliminazione di sistemi operativi fuori supporto (es. Windows 7)
  - Upgrade di sistemi operativi non aggiornati
  - Upgrade di programmi o utility non più supportati o non aggiornati
  - Correzione di configurazioni o policy di Windows.
- Protezione in tempo reale delle singole postazioni, monitorandone costantemente nuove eventuali problematiche:
  - Protezione completa per Windows, macOS, iOS e Android
  - Tecnologie innovative per proteggere dagli attacchi zero-day
  - Protezione da ransomware multi-livello per mantenere i file al sicuro
  - Possibilità di utilizzare una VPN sicura per una completa privacy online[1]
  - Servizio Antimalware
  - Advanced Threat control
  - Anti-exploit avanzato
  - Impatto minimo sulle prestazioni del sistema
  - Protezione base e avanzata della rete, grazie al software di firewalling, collegato direttamente al cloud di BitDefender per applicare in automatico nuove policy di sicurezza atte a proteggere i sistemi da nuove minacce
  - Protezione mail avanzata multilivello, completamente trasparente rispetto ai client di posta.
  - Controllo dei contenuti e dei dispositivi
  - Mitigazione dei comportamenti "a rischio" da parte degli utenti
  - Mitigazione delle vulnerabilità
  - Gestione dei dispositivi a rischio
  - Correzione delle configurazioni errate
  - Sandbox Analyzer, un ambiente confinato in cloud che permette di effettuare controlli su file dubbi prima di aprirli in locale.
- Gestione dei dispositivi mobili[2]. La soluzione **Secure Workstation** aiuta i nostri clienti a gestire l'esplosione del mercato dei dispositivi mobili, espandendo la sicurezza con un ricco portafoglio di servizi gestiti. Potete chiamarla "mobilità in sicurezza!!
- Navigazione protetta. Aiutare i dipendenti a rimanere produttivi, grazie a regole di navigazione web basate sul buon senso e appositamente studiate per gli ambienti

[1] Servizio opzionale
[2] Il sistema di gestione degli endpoint mobili è fornito con piattaforma distinta e opzionale di bitdefender

professionali impedendo di visitare accidentalmente siti che inviano malware, proteggendoli dal phishing, dai proxy, da spyware, adware, botnet ecc., aiuta a proteggere il business dalle responsabilità penali e ridurre il rischio di violazioni della sicurezza

- Monitoraggio proattivo: consente di essere sempre un passo avanti rispetto ai problemi di disponibilità, prestazioni ed esperienza degli utenti. Il monitoraggio automatizzato, efficiente e affidabile, rappresenta l'unico modo per ottenere informazioni critiche sui sistemi e fornire servizi gestiti economici e di valore.
- Gestione supervisionata da una console remota da parte degli specialisti SecureNet: aiuta l'IT del cliente a focalizzare le risorse aziendali sull'espansione del business, anziché sulle attività di routine:
    - Monitoraggio in tempo reale
    - Accesso remoto agli endpoint, dietro autorizzazione dell'utilizzatore o del responsabile IT del Cliente
    - Policy enforcing (es. per gli aggiornamenti di sistema operativo)
    - Riavvio della macchina
    - Avvio di scansioni mirate
    - Isolamento dalla rete di un end point a rischio fino alla neutralizzazione della minaccia.
- Possibilità di gestire ruoli distinti in modo da definire al meglio i limiti operativi tra il responsabile IT del cliente e gli specialisti SecureNet (amministratori, auditor, utenti…)
- Possibilità di creare pacchetti di installazione personalizzati per il cliente e per tipologia di utente (lavoratori in sede, in remoto, macchine server…)
- Gestione aggiornamenti. Ogni settimana vengono annunciate nuove vulnerabilità informatiche, mentre centinaia di applicazioni diverse sono in esecuzione: un servizio professionale supportato da uno strumento efficace per la gestione patch è quindi fondamentale per mantenere l'efficienza e la sicurezza dei sistemi.
- Possibilità di gestire endpoint distribuiti sul territorio e connessi ad internet. Nel momento in cui un endpoint vada offline, rimane protetto con l'ultimo aggiornamento di definizioni antivirus scaricato, per riallinearsi non appena online con una scansione completa e approfondita.
- Tracciabilità asset e inventario. La gestione e la tracciabilità automatiche dei componenti hardware e software riducono i tempi di inventario e permettono una gestione corretta degli asset.
- Reportistica completa sugli eventi e interventi. Grazie a potenti strumenti di reportistica è possibile individuare i trend nelle prestazioni del sistema evidenziandone la necessità di intervento:
    - Endpoint gestiti
    - Endpoint attivi
    - Minacce gestite
    - Minacce Top five
    - Ranking di sicurezza del sistema informativo
    - Stato degli incidenti di sicurezza
    - Azioni di risanamento
    - Comportamenti a rischio da parte degli utenti
    - Vulnerabilità
    - Dispositivi a rischio
    - Configurazioni errate
- Help desk di primo e secondo livello. Il servizio SecureNet di assistenza clienti aumenta allo stesso tempo la produttività e ottimizza le procedure di supporto, in modo che il cliente possa concentrarsi sul proprio business, non sul sistema informativo.
    - Interventi su base chiamata: lun-ven 9-18.
    - Interventi proattivi in tempo reale in base alla segnalazione del sistema di monitoraggio.