

PROUDLY POWERED BY
ENTERPRISE SRL

MIRIUM

BUSINESS LOG

AI POWERED

VERSIONE CLOUD





B U S I N E S S L O G S E R V E R

DEFINIZIONI GENERALI.

Di seguito vengono riportati i concetti principali di contesto per comprendere al meglio Business LOG, la Suite di Log Management leader di mercato in Italia da oltre 10 anni.

CHI È L'AMMINISTRATORE DI SISTEMA PER IL LEGISLATORE ITALIANO?

Il provvedimento vigente definisce l'Amministratore di Sistema come "una figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali sistemi ERP (Enterprise Resource Planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali."

COSA IMPONE IL PROVVEDIMENTO N.300 DEL 24.12.2008?



Il provvedimento definisce la figura dell'Amministratore di Sistema e prevede l'**obbligo di registrazione degli accessi logici** (access log) degli stessi Amministratori di Sistema (sia server che client).

Le registrazioni devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste, devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

COSA È UNA SUITE DI LOG MANAGEMENT?

Business LOG è una Suite di Log Management. Una Suite di Log Management è la soluzione perfetta per essere compliance al provvedimento n. 300/2008 del Garante per la Privacy, in quanto serve proprio a registrare gli Access Log degli Amministratori di Sistema secondo le specifiche direttive del provvedimento (inalterabilità, completezza, possibilità di verifica e tempistiche di conservazione). Le aziende non in regola potranno essere sanzionate dal Garante (anche in ragione del Piano Sanzionatorio previsto dal GDPR).



BUSINESS LOG SERVER

MERCATO E TARGET DELLA SOLUZIONE.

Di seguito vengono elencati i principali settori interessati all'implementazione della Suite di Log Management.

MERCATO E TARGET DELLA SOLUZIONE.

Settore Sanitario.

Ambulatori, ospedali, aziende farmaceutiche, laboratori, ecc.



Settore Bancario.

Banche, cooperative di credito, enti di gestione del risparmio, ecc.



Pubbliche Amministrazioni.

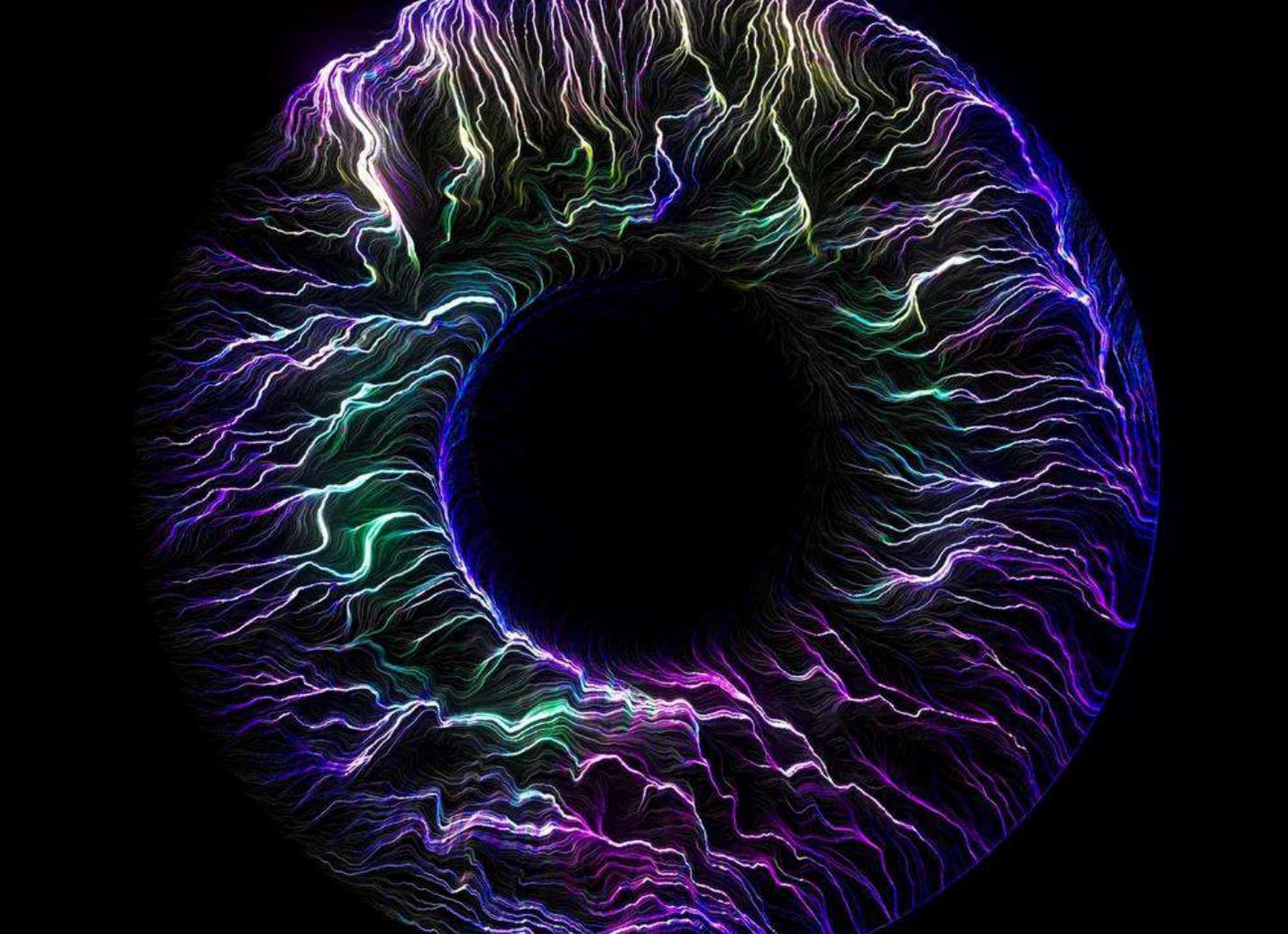
Tutte le Pubbliche Amministrazioni con sistemi informatici che trattano dati informatici.



Tutte le aziende con ADS.

Oltre ai settori riportati, sono interessate tutte le aziende con un Amministratore di Sistema.





BUSINESS LOG SERVER

CARATTERISTICHE DELLA SOLUZIONE.

Definizione della soluzione, come funziona e quali sono le principali funzioni disponibili.

BUSINESS LOG SERVER

COS'È BUSINESS LOG SERVER?

Business LOG Server è una Suite di Log Management per la compliance al provvedimento n.300 del 24.12.2008, alle disposizioni in materia di Privacy Europea (GDPR 2016/679) ed alla ISO 27001.

Business LOG Server permette l'acquisizione a livello server senza l'utilizzo di agent o servizi esterni su tutte le macchine presenti nella struttura aziendale in dominio.

I nodi configurabili nel sistema non richiedono l'installazione di nessun agent, facilitando la configurazione e la gestione di infrastrutture di qualsiasi dimensione, dalle più piccole fino ad architetture di livello enterprise.

La raccolta dei Log è centralizzata all'interno di una macchina adibita a Log Box (la macchina scelta può essere sia fisica che virtuale).



**Business LOG Server
Edition installato**

Time	Source	Message
2014-01-01 10:00:00	192.168.1.1	Microsoft Windows [Version 6.0.6002.18005] Copyright (c) 2009 Microsoft Corporation. All rights reserved.
2014-01-01 10:00:01	192.168.1.1	C:\Windows\system32\cmd.exe /c ipconfig /all
2014-01-01 10:00:02	192.168.1.1	ipconfig /all
2014-01-01 10:00:03	192.168.1.1	Windows IP Configuration
2014-01-01 10:00:04	192.168.1.1	Interface
2014-01-01 10:00:05	192.168.1.1	Media
2014-01-01 10:00:06	192.168.1.1	Physical Address (MAC)
2014-01-01 10:00:07	192.168.1.1	IPv4 Address(es)
2014-01-01 10:00:08	192.168.1.1	Subnet Mask
2014-01-01 10:00:09	192.168.1.1	Default Gateway
2014-01-01 10:00:10	192.168.1.1	DHCP Enabled
2014-01-01 10:00:11	192.168.1.1	IP Address from DHCP
2014-01-01 10:00:12	192.168.1.1	Subnet Mask from DHCP
2014-01-01 10:00:13	192.168.1.1	Default Gateway from DHCP
2014-01-01 10:00:14	192.168.1.1	DHCPv6 Enabled
2014-01-01 10:00:15	192.168.1.1	IPv6 Address(es)
2014-01-01 10:00:16	192.168.1.1	Subnet Mask
2014-01-01 10:00:17	192.168.1.1	Default Gateway
2014-01-01 10:00:18	192.168.1.1	DHCPv6v6 Enabled
2014-01-01 10:00:19	192.168.1.1	IPv6 Address(es) from DHCPv6
2014-01-01 10:00:20	192.168.1.1	Subnet Mask from DHCPv6
2014-01-01 10:00:21	192.168.1.1	Default Gateway from DHCPv6
2014-01-01 10:00:22	192.168.1.1	IPv6 Address(es) from Static Configuration
2014-01-01 10:00:23	192.168.1.1	Subnet Mask from Static Configuration
2014-01-01 10:00:24	192.168.1.1	Default Gateway from Static Configuration
2014-01-01 10:00:25	192.168.1.1	IPv6 Address(es) from DHCPv6
2014-01-01 10:00:26	192.168.1.1	Subnet Mask from DHCPv6
2014-01-01 10:00:27	192.168.1.1	Default Gateway from DHCPv6
2014-01-01 10:00:28	192.168.1.1	IPv6 Address(es) from Static Configuration
2014-01-01 10:00:29	192.168.1.1	Subnet Mask from Static Configuration
2014-01-01 10:00:30	192.168.1.1	Default Gateway from Static Configuration

Interfaccia di Business LOG

**Fino a
5.000 nodi.**



Nessun Agent da installare.

Supporta: **Syslog**

SECURITY OPERATION CENTER (SOC).

Nel mondo digitale odierno, le minacce informatiche sono in costante evoluzione e possono colpire aziende di qualsiasi dimensione.

Oltre alle classiche funzionalità di un Security Operation Center (SOC), la versione integrata in Business LOG offre capacità avanzate di analisi degli eventi, correlazione automatica e monitoraggio continuo del comportamento degli utenti.

Grazie a un monitoraggio costante 24/7 e a strumenti avanzati di analisi comportamentale, è in grado di prevenire incidenti prima che diventino critici, offrendo una sicurezza proattiva e affidabile.

Il SOC aiuta la tua organizzazione a mantenere la conformità con le normative sulla sicurezza dei dati (GDPR, NIS2, ...). Fornisce report che dimostrano l'adesione alle leggi e agli standard del settore.

Attraverso l'uso di strumenti di intelligence, Machine Learning e analisi dei dati basata sull'Intelligenza Artificiale, il SOC può prevedere potenziali attacchi e vulnerabilità.

Questo approccio proattivo consente di implementare misure preventive prima che si verifichino incidenti gravi.

The screenshot displays the Security Operation Center (SOC) interface. The top navigation bar includes various tool icons such as 'Elenco Macchine', 'Inventario Software', 'Consumi Energetici', 'Aggiornamenti Software', 'Eventi Interni', 'Elenco Log', 'Visualizzatore Archivi', 'Invia Comando', 'Comandi PS', 'Elenco Template PS', 'Log Accessi', 'Log Accessi Files', 'Elenco Accessi USB', 'Log Audit', 'Log Processi', 'Log Stampe', 'Elenco Accessi Falso', 'Elenco Syslog', 'Vista Machine/Utenti', 'Elenco Utenti', 'Elenco Sessioni', and 'Elenco Combinazioni'. Below the navigation bar, there is a dashboard with several active tabs: 'Working Log', 'Elenco Accessi Falso', 'Elenco Syslog', 'Allarmi Eventi', 'Elenco Macchine', 'Consumi Energetici', 'Inventario Hardware', 'Inventario Software', 'Comandi PS multi', and 'Security Operation Center'. The main area is divided into a table of events on the left and a detailed view of a selected event on the right. The event table has columns for 'Livello', 'Data Ora', and 'Oggetto'. The detailed view shows a list of checked items and a message area with text describing the event.

Livello	Data Ora	Oggetto
1	23/02/2025 00:03:48	Controllo IP Estranei
2	23/02/2025 00:03:49	Controllo Installazioni
1	22/02/2025 00:03:29	Controllo IP Estranei
2	22/02/2025 00:03:31	Controllo Installazioni
1	21/02/2025 00:03:30	Controllo IP Estranei
1	20/02/2025 00:03:12	Controllo IP Estranei
1	20/02/2025 00:03:12	Controllo IP Estranei
2	20/02/2025 00:03:13	Controllo Attività di Rete
1	19/02/2025 00:03:56	Controllo IP Estranei
1	18/02/2025 00:03:41	Controllo IP Estranei
2	18/02/2025 00:03:56	Controllo Attività di Rete
1	14/02/2025 00:03:47	Controllo IP Estranei
1	14/02/2025 00:03:46	Accessi di Rete
2	14/02/2025 00:03:46	Controllo Installazioni
2	14/02/2025 00:03:46	Controllo Installazioni
2	14/02/2025 00:03:47	Controllo Attività di Rete
1	13/02/2025 00:03:08	Controllo IP Estranei

Message:

Per la macchina: server-x ha registrato 1 accessi da un IP esterno al range di IP impostato (10.212.134.200). Verificate che questo accesso sia autorizzato.

Durante il controllo, sono stati rilevati 1 tentativi di accesso da grafica ps verso la macchina server-x. Potete verificare, nell'inventario software che questi programmi siano autorizzati.

Per la macchina: server-x ha registrato 4 accessi da un IP esterno al range di IP impostato (fe80:d171:539e:d677:2e79). Verificate che questo accesso sia autorizzato.

Durante il controllo, sono stati rilevati 1 nuovo software installati sulla macchina server-x. Potete verificare, nell'inventario software che questi programmi siano autorizzati.

Per la macchina: server-x ha registrato 4 accessi da un IP esterno al range di IP impostato (fe80:d171:539e:d677:2e79). Verificate che questo accesso sia autorizzato.

Per la macchina: server-x ha registrato 2 accessi da un IP esterno al range di IP impostato (fe80:da57:4d27:d5d6:352a). Verificate che questo accesso sia autorizzato.

Per la macchina: server-x ha registrato 2 accessi da un IP esterno al range di IP impostato (236). Verificate che questo accesso sia autorizzato.

Durante il controllo, sono stati rilevati 2 tentativi di accesso da grafica ps verso la macchina server-x si tratta di accessi a condizioni di rete, verificate che non ci siano errori di configurazione e la natura di tali accessi.

Per la macchina: server-x ha registrato 2 accessi da un IP esterno al range di IP impostato (236). Verificate che questo accesso sia autorizzato.

Per la macchina: server-x ha registrato 2 accessi da un IP esterno al range di IP impostato (236). Verificate che questo accesso sia autorizzato.

Durante il controllo, sono stati rilevati 2 tentativi di accesso da grafica ps verso la macchina server-x si tratta di accessi a condizioni di rete, verificate che non ci siano errori di configurazione e la natura di tali accessi.

Per la macchina: server-x ha registrato 4 accessi da un IP esterno al range di IP impostato (721). Verificate che questo accesso sia autorizzato.

Per la macchina: WindowsServer2025 ha registrato 90 tentativi di accesso alle risorse di rete, eseguiti con l'utente . Questo, solitamente, può essere determinato da problemi di configurazione delle share di rete, unità di rete con credenziali obsolete o attività schedate con utente o password errate.

Durante il controllo, sono stati rilevati 1 nuovo software installati sulla macchina: WindowsServer2025. Potete verificare, nell'inventario software che questi programmi siano autorizzati.

Durante il controllo, sono stati rilevati 6 nuovi software installati sulla macchina server-x. Potete verificare, nell'inventario software che questi programmi siano autorizzati.

Durante il controllo, sono stati rilevati 2 tentativi di accesso da grafica ps verso la macchina server-x si tratta di accessi a condizioni di rete, verificate che non ci siano errori di configurazione e la natura di tali accessi.

Per la macchina: server-x ha registrato 2 accessi da un IP esterno al range di IP impostato (721). Verificate che questo accesso sia autorizzato.

Per la macchina: WindowsServer2025 ha registrato 15 tentativi di accesso alle risorse di rete, eseguiti con l'utente . Questo, solitamente, può essere determinato da problemi di configurazione delle share di rete, unità di rete con credenziali obsolete o attività schedate con utente o password errate.

SysProcessor - Allarme rilevato ! - Synology Nas Login, BloggyProcessor - Allarme rilevato ! - SysLog: Accesso Falso, Check Session, Modifica File

LE PRINCIPALI FUNZIONI.

Allarmi personalizzati.

Ricevi un allarme ad una mail specifica e/o lancia un comando tramite Power Shell al verificarsi di un'azione specifica definita in fase di configurazione dall'utente.

Monitora dispositivi USB.

Monitora facilmente tutte le operazioni fatte su dispositivi esterni (inserimento, scritture, copie ed eliminazioni).

Inventario automatico.

Business LOG inventaria e storicizza tutte le operazioni in tutta la rete riguardanti software e hardware.

Syslog integrato.

Syslog integrato per la registrazione da macchine Linux, Unix e Mac o da dispositivi compatibili Syslog, come Router, Firewall, Nas, ecc.

LE PRINCIPALI FUNZIONI.

Archiviazione crittografata.

Oltre al DB presente in Business LOG, è possibile creare in automatico un backup di tutte le informazioni raccolte in una Path a scelta (nas, server, storage cloud).

Log da software assistenza remota.

Business LOG raccoglie i log da applicativi di assistenza remota, come TeamViewer, Supremo, AnyDesk, NoMachine e tanti altri.

Registrazione eventi accesso file.

In una tabella dedicata è possibile monitorare chi apre, elimina o copia i file presenti in una determinata cartella di rete.

Firma digitale su ogni log raccolto.

In Real Time, nel momento della raccolta log viene apposta in automatico una firma tecnica di coerenza su ogni log.

IL SOC DI BUSINESS LOG – NOVITÀ 2025

Rilevamento in tempo reale.

Il SOC (Security Operation Center) di Business LOG rileva e risponde a minacce informatiche in tempo reale, garantendo protezione continua contro attacchi, vulnerabilità e attività sospette, con azioni immediate di mitigazione.

Risposta rapida agli incidenti.

In caso di problematiche, il SOC di Business LOG è in grado di attivare immediatamente procedure di risposta per contenere e mitigare l'impatto.

Analisi proattiva delle minacce.

Attraverso l'uso di strumenti di intelligence, Machine Learning e analisi dei dati basata sull'Intelligenza Artificiale, il SOC può prevedere potenziali attacchi e vulnerabilità.

Conformità normativa.

Il SOC aiuta la tua organizzazione a mantenere la conformità con le normative sulla sicurezza dei dati (GDPR, NIS2, ecc.).

BUSINESS LOG SERVER

LE VERSIONI DISPONIBILI.

Business LOG One | NOVITÀ 2025

Registra i log da 1 computer + Audit dal File Server.

La soluzione ideale per uso personale, piccoli studi e aziende che vogliono monitorare la sicurezza e gli accessi di singoli PC. Facile da installare, include IA, dashboard SOC, controllo file, USB, tracking e stampa. Non include scansioni remote, inventario, Powershell, RT, Azure e Syslog.

Business LOG Auditor | NOVITÀ 2025

Registra i log da 1 computer + fino a 20 nodi con Plugin RT.

Pensato per server o piccole reti aziendali, anche senza dominio Active Directory. Facile da installare, è ideale dove si vuole limitare la configurazione, usando l'agente RT. Include IA, dashboard SOC, controllo file, USB, tracking, stampa, Syslog e supporto Azure (con licenza). Esclude scansioni remote e inventario.

BUSINESS LOG SERVER

LE VERSIONI DISPONIBILI.

Business LOG Plus | 1-39 nodi

Registra da 1 a 39 nodi (client e server).

Business LOG Enterprise80 | 40-80 nodi

Registra da 40 a 80 nodi (client e server).

Business LOG Enterprise150 | 81-150 nodi

Registra da 81 a 150 nodi (client e server).

Business LOG Enterprise250 | 151-250 nodi

Registra da 151 a 250 nodi (client e server).

BUSINESS LOG SERVER

LE VERSIONI DISPONIBILI.

Business LOG Enterprise500 | 251-500 nodi

Registra da 251 a 500 nodi (client e server).

Business LOG Enterprise750 | 501-750 nodi

Registra da 501 a 750 nodi (client e server).

Business LOG Enterprise1000 | 751-1000 nodi

Registra da 751 a 1000 nodi (client e server).

Business LOG EnterpriseX | nodi illimitati

Nodi illimitati (client e server) e tutti i plugin inclusi.

I PLUGIN DISPONIBILI.

Plugin RT (Real Time)

Permette di acquisire i log di macchine Windows anche per le macchine fuori dominio o per quelle macchine per cui si rende necessario avere una registrazione in Real Time.

Plugin Backup Log in Cloud

Permette di esportare i log raccolti su uno storage cloud privato (consultabile tramite web in Microsoft Azure o tramite l'applicazione dedicata).

Plugin USB e Dischi removibili

Permette di monitorare gli inserimenti, le letture e le scritture dei dischi removibili (chiavette USB, dischi esterni o SD/microSD).

Plugin As400

Permette di raccogliere i log da macchine IBM As400 direttamente all'interno di Business LOG Server.

I PLUGIN DISPONIBILI.

Plugin SQL

Permette di acquisire i log dall'audit avanzato di SQL server ed ottenere informazioni sulla query in uso nelle tabelle del database.

Plugin Stampanti

Consente di monitorare tutte le stampanti all'interno della rete aziendale e di consultare, nell'apposita tabella, tutti gli ordini di stampa eseguiti.

Plugin Azure

Permette di registrare i log access degli Account Azure.
Consente inoltre di ricevere log anche da Microsoft 365 (per avere i log di Sharepoint è necessario avere una licenza E5).

Plugin Aggiornamenti

Le macchine controllate ricevono, in un apposito elenco all'interno di Business LOG, tutti gli aggiornamenti di Windows Update (e gli HotFix applicati) elencati, scaricati e installati .

I PLUGIN DISPONIBILI.

Plugin SOC Stream – Novità 2025

Mediante il Plugin SOC Stream è possibile consultare le informazioni raccolte dal SOC (installato on-premise) su un sito web dedicato, garantendo così una visione completa, sempre disponibile ed in tempo reale delle attività di sicurezza e conformità.

Plugin AI – Novità 2025

Il Plugin porta l'intelligenza artificiale al centro della tua sicurezza IT. Analizza gruppi di log con l'engine AI 2.0 e scopri in pochi istanti il reale impatto organizzativo e le criticità di sicurezza. Uno strumento potente per anticipare i rischi, prendere decisioni consapevoli e rafforzare la tua strategia di protezione.

Plugin Energy 5.0 – Novità 2025

Con il Plugin hai il pieno controllo sui consumi energetici dei tuoi dispositivi. Grazie alla visualizzazione storica e in tempo reale, puoi identificare sprechi e ottimizzare l'utilizzo delle risorse. Puoi attivare comandi intelligenti per ridurre l'impatto energetico, migliorare l'efficienza e contribuire alla sostenibilità aziendale.

LE OPZIONI AGGIUNTIVE.

Supporto Sistemistico.

Supporto alla configurazione iniziale dell'infrastruttura da parte di un nostro tecnico specializzato in attività sistemistiche.

Formazione al personale (2h).

Il servizio viene erogato per fornire tutte le informazioni necessarie al personale incaricato per la gestione e l'uso del software.

Il servizio viene erogato da remoto tramite un Webinar interattivo in diretta dedicato al personale dell'organizzazione.

Installazione di Business LOG

Il servizio prevede l'affiancamento di un tecnico di Business LOG ai tecnici dell'organizzazione nella fase di installazione e configurazione del software per configurarlo correttamente (ed essere compliance alle normative). Il servizio può essere erogato da remoto o in presenza ed è caldamente consigliato.

BUSINESS LOG SERVER

I REQUISITI MINIMI.

VERSIONE PLUS.

RAM

12 GB

**8 GB di RAM richiesti
(consigliati 12 GB).**

SPAZIO

50 GB

**25 GB di spazio su disco per
database e archivi.**

VCORE

4

**CPU Intel o AMD di classe
Pentium (almeno 2 vCore per
VM).**

WINDOWS

10

**Sistema operativo: Windows 10,
Windows 11, Windows Server
2016, Windows Server 2019,
Windows Server 2022 Windows
Server 2025.**

.net
FRAMEWORK

4.8

**.net Framework 4.8 (compreso
nel setup).**



B U S I N E S S L O G C L O U D

REPARTO COMMERCIALE

Business LOG è prodotto e distribuito da Enterprise Srl.

Enterprise Srl è un'azienda italiana impegnata nella consulenza strategica e nello sviluppo software, con una forte specializzazione nella progettazione e realizzazione di soluzioni a support della riorganizzazione di tutti i processi aziendali e professionali.

info@mirium.it

<https://mirium.it/contatti>

BUSINESS LOG SERVER

I REQUISITI MINIMI.

VERSIONE ENTERPRISE.

RAM

12 GB

**12 GB di RAM richiesti
(consigliati 16 GB).**

SPAZIO

100 GB

**50 GB di spazio su disco per
database e archivi.**

VCORE

6

**CPU Intel o AMD di classe i7 o
superiore (almeno 6 vCore per
VM).**

WINDOWS

10

**Sistema operativo: Windows 10,
Windows 11, Windows Server
2016, Windows Server 2019,
Windows Server 2022,
Windows Server 2025.**

.net
FRAMEWORK

4.8

**.net Framework 4.8 (compreso
nel setup).**

**È richiesto l'utilizzo di dischi SSD o M2
o, in caso di Macchina virtuale, l'utilizzo
del controller disco Paravirtual.*

PROUDLY POWERED BY
ENTERPRISE SRL

BUSINESS LOG AI POWERED

— Suite di Log Management per gestire al meglio la normativa riguardante gli Amministratori di Sistema e le disposizioni in materia di Privacy Europea (GDPR 2016/679), NIS2 e ISO 27001.

MIRIUM

