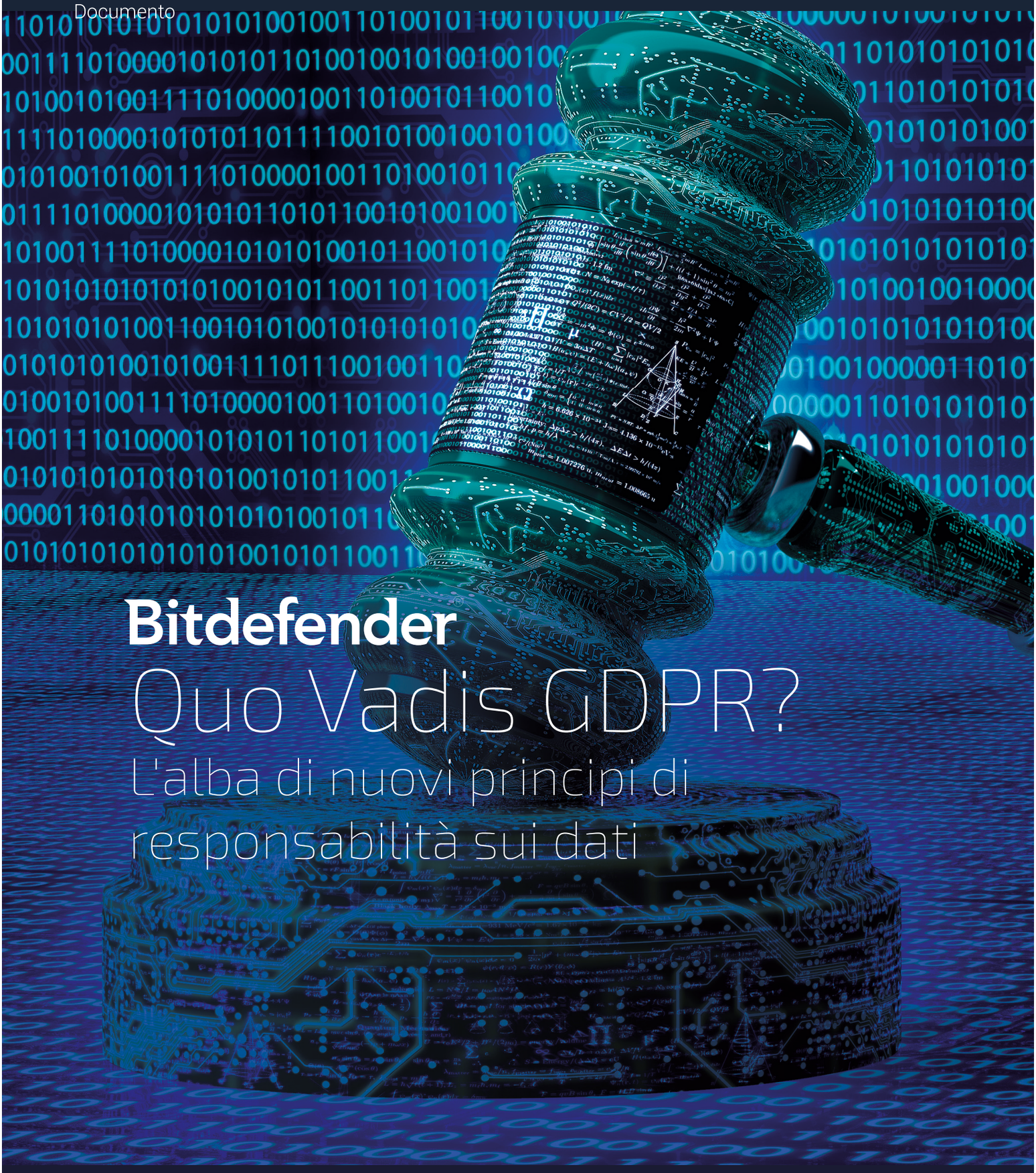
Documento



Bitdefender

Quo Vadis GDPR?

L'alba di nuovi principi di responsabilità sui dati

Panoramica della situazione

Dopo anni di dibattiti, preparativi e sforzi per allinearsi con le nuove sfide e trasformazioni digitali, il GDPR (Regolamento generale sulla protezione dei dati) è stato finalmente approvato dal Parlamento europeo il 14 aprile 2016. Il regolamento è entrato in vigore 20 giorni dopo la sua pubblicazione sulla Gazzetta ufficiale dell'UE, e la sua data attuale di applicazione è stata fissata per il 25 maggio 2018.

Le basi e i principi fondamentali del Regolamento generale sulla protezione dei dati dell'UE risalgono al 1995, quando è entrata in vigore la direttiva sulla protezione dei dati 95/46/EC con l'obiettivo di armonizzare le leggi e i regolamenti sulla privacy dei dati in tutta Europa. Tuttavia, il lancio del nuovo GDPR dell'UE comporterà delle modifiche alla politica di regolamentazione per riflettere meglio l'attuale trasformazione digitale molte organizzazioni, e la società in generale, stanno attraversando.

Le modifiche hanno portato responsabilità e obblighi aggiuntivi per aziende, istituzioni, enti governativi e altre entità che trattano dati personali, ma garantiscono anche nuovi diritti ai cittadini, come il diritto di ottenere dai responsabili del trattamento dei dati la conferma del trattamento effettivo dei dati personali , dove vengano elaborati e per quale scopo.

Questo White Paper analizza i problemi da affrontare da parte delle organizzazioni che gestiscono grandi volumi di dati personali, le side organizzative interne che dovranno superare nel loro cammino per ottenere la conformità, oltre ai processi aziendali e tecnologici necessari per soddisfare i nuovi obblighi imposti dal GDPR.

Inoltre, questo documento delinea come Bitdefender possa aiutare le aziende a ottenere la conformità con il GDPR, includendo un approccio graduale per proteggersi dalla perdita, il furto e le violazioni dei dati.

Implicazioni per le aziende

L'applicazione del GDPR avrà un impatto importante sulle aziende, poiché dovranno prestare maggiore attenzione al modo in cui gestiranno i dati personali. In base al http://www.eugdpr.org/, i punti fondamentali del GDPR, oltre alle informazioni sul suo impatto sulle aziende, sono evidenziati in basso:

- **Maggiore campo di applicazione territoriale (applicabilità extra-territoriale))** - Senza dubbio, il maggiore cambiamento al quadro regolamentare della privacy dei dati deriva dalla maggiore giurisdizione del GDPR, in quanto si applica a tutte le aziende che gestiscono dati personali di persone interessate residenti nell'Unione, indipendentemente dalla posizione dell'azienda. In precedenza, l'applicabilità territoriale della direttiva era ambigua e riferita alla gestione di dati "nell'ambito di un'elaborazione".

- **Sanzioni** - Le organizzazioni che infrangono il GDPR possono essere sanzionate fino al 4% del loro fatturato annuale globale, o 20 milioni di euro (se superiore). Queste regole si applicano sia ai responsabili del trattamento che dell'elaborazione dei dati, quindi i "cloud" non potranno essere esentati dall'applicazione del GDPR.

- **Consenso** - Le condizioni per il consenso sono state rinforzate e le aziende non potranno più utilizzare termini e condizioni lunghi e illeggibili, caratterizzati da un gergo giuridico, in quanto la richiesta di consenso deve essere fornita tramite un modulo comprensibile e facilmente accessibile, con lo scopo per il trattamento dei dati allegato a tale consenso.

Come indicato in precedenza, il Regolamento generale sulla protezione dei dati serve anche a rinforzare i diritti dei cittadini i cui dati personali vengano raccolti, ospitati ed elaborati da fornitori di terze parti. Questi diritti includono, ma non sono limitati a:

- **Notifica delle violazioni** - Ai sensi del GDPR, la notifica delle violazioni diventerà obbligatoria in tutti gli stati membri, laddove una violazione dei dati potrebbe "comportare un rischio per i diritti e le libertà dei cittadini." Ciò deve essere fatto entro 72 ore dalla prima presa di coscienza della violazione.

- **Diritto di accesso** - Parte dei maggiori diritti delle persone interessate indicati dal GDPR è proprio il diritto per le persone interessate di ottenere dal responsabile del trattamento dei dati la conferma del trattamento effettivo dei dati personali, dove vengano elaborati e per quale scopo.

- **Portabilità dei dati** - Il GDPR introduce la portabilità dei dati, ovvero il diritto per una persona interessata di ricevere i propri dati personali, che in precedenza hanno fornito in un "formato utilizzato comunemente e suscettibile di una lettura elettronica", e il diritto di trasmettere tali dati a un altro responsabile del trattamento.

- **Privacy by Design** - Il concetto di Privacy by design esiste da alcuni anni, ma solo ora è diventate parte dei requisiti legali con il GDPR. In pratica, Privacy by design riguarda l'incorporazione della protezione dei dati a partire dall'inizio della progettazione di un sistema, piuttosto che una semplice aggiunta.

- **Responsabili della protezione dei dati** - Per aziende le cui attività principali consistono in operazioni di elaborazione che richiedono un costante e sistematico monitoraggio delle persone interessate su larga scala o categorie speciali di dati oppure dati relativi a condanne e reati penali, la nomina dei responsabili della protezione dei dati è obbligatoria.

Tra molte aziende regna ancora la confusione

Una recente ricerca di IDC mostra che molte organizzazioni hanno una minima conoscenza o addirittura non conoscono il regolamento o il suo obiettivo, le sue tempistiche o il suo impatto, malgrado il rischio di sanzioni molto elevate, fino al 4% del fatturato annuo globale o 20 milioni di euro, (se superiore), oltre alle potenziali azioni legali, la sospensione dell'elaborazione dei dati personali e il danno in termini di reputazione.

Ciò è sorprendente, soprattutto a causa delle possibili conseguenze che le aziende dovranno affrontare in caso di non conformità. Attualmente, i costi delle violazioni di dati sembrano restare nella fascia inferiore a numeri a sei cifre, almeno in base all'indagine di IDC..

Le aziende che hanno già iniziato a prepararsi per la conformità hanno indicato le sfide principali poste dal GDPR, in ordine di importanza:

- Cifratura e/o pseudonimizzazione dei dati
- Notifica delle violazioni dei dati entro 72 ore
- Protezione dei dati da progettazione e in via predefinita
- Portabilità dei dati
- Definire processi e tecnologie "all'avanguardia"

Malgrado queste sfide, alcune organizzazioni utilizzeranno questa opportunità per migliorare servizi e reputazione, riconoscendo che la protezione dei dati è diventata una questione sempre più importante perdipendenti, clienti e fornitori.

Mentre gestione e responsabilità saranno critici per l'effettiva conformità al GDPR, la responsabilità definitiva ricadrà sui vertici aziendali, con un'alta implicazione a livello di consiglio di amministrazione. Le aziende dovranno valutare i rischi dei propri sistemi di gestione dei dati, assicurarsi che i diritti dei soggetti siano protetti investendo in controlli e sistemi appropriati, controllare i consensi per capire quale tipo di dati possono e non possono elaborare e assicurarsi che sia in atto un processo di gestione delle violazioni.

La risposta di Bitdefender al GDPR

IDC raccomanda il seguente approccio a cinque passi nel cammino verso la conformità al GDPR supportati dalla piattaforma integrata di gestione dei dati e un team di governance dei dati multifunzionale.

- **Comprendere lo scopo e minimizzare le assunzioni di dati personali.**

- Mentre molte società di consulenza consigliano di iniziare i preparativi al GDPR dalla mappatura e scoperta dei dati, cominciare da un tale sforzo gravoso potrebbe rallentare significativamente l'intero progetto GDPR, specialmente quando si prendono in considerazione dati oscuri e non strutturati. IDC consiglia di iniziare a lavorare con i soggetti economici la cui assunzione dei dati personali è vitale per la propria attività e lavorare per ridurre al minimo l'assunzione di dati personali. Ciò semplificherà notevolmente il prossimo passaggio.

- **Definire la propria "avanguardia"**

- Definire controlli procedurali e tecnologici che si ritengono sufficienti per proteggere i dati personali (consultare l'articolo 32 del GDPR). Prestare particolare attenzione nel proteggere i dati non strutturati, ad esempio cifrandoli. Un'altra area di attenzione è la capacità di rilevamento delle violazioni, incluso l'accesso non autorizzato/insolito ai dati personali.

- **Sviluppare e verificare accuratamente il processo di risposta agli incidenti.**

- Includere partner e terze parti (ad esempio fornitori di servizi cloud) nei propri test e piani di risposta agli incidenti. Ricordarsi che determinate violazioni di dati richiedono la notifica ai soggetti interessati oltre alla segnalazione all'Autorità di protezione dei dati (DPA) (consultare l'articolo 34 del GDPR).

- **Stabilire una corretta gestione dei dati**

- La gestione dei dati dovrebbe essere il risultato della cooperazione delle funzioni aziendali con la propria architettura di sicurezza di informazioni e dati, facilitata dal Responsabile della protezione dei dati. Quando si scelgono controlli tecnici e procedurali, deve essere prestata una particolare attenzione ai prodotti e ai servizi che migliorano la postura della sicurezza dei dati, introducendo nuove o migliori capacità in più discipline. Una maggiore visibilità e una gestione centrale sono ottimi esempi di tali capacità.

- **Eseguire attività di mappatura e scoperta dei dati**

- Per eliminare i dati inutilizzati (oscuri) ottenuti e allineare la resistenza e l'efficienza dei relativi controlli di protezione dei dati, condurre una scoperta dei dati. Lo scopo principale di questa attività è assicurare che non manchi alcuna capacità di elaborazione e raccolta dei dati nella fase iniziale di minimizzazione dell'assunzione.

Il secondo passaggio di questo approccio si riferisce all'utilizzo della migliore tecnologia a propria disposizione e nell'ambito di un budget accessibile per allinearsi con i requisiti del GDPR.

Bitdefender è ben posizionata per offrire alle aziende i migliori strumenti tecnologici in grado di aiutarle a ottenere la conformità al GDPR. A tale proposito, l'approccio di Bitdefender alla protezione dei dati personali consiste in un cammino di quattro passaggi:

- Identificare quali dati personali si memorizzano ed elaborano
- Valutare a quali rischi sono esposti i propri dati
- Impostare controlli procedurali e tecnici per mitigare i rischi
- Migliorare la visibilità e la capacità di rilevare e rispondere agli incidenti

In quanto a tecnologia, la risposta multilivello di Bitdefender aiuta le aziende a ottenere la conformità ai requisiti di sicurezza del GDPR, offrendo protezione da perdita e furto di dati, tra cui attacchi mirati, e una migliore visibilità nelle violazioni di dati.

Protezione da perdite di dati – Dispositivi persi/rubati

Aspetti chiave: Secondo il Data Breach Investigation Report (DBIR) di Verizon del 2016, solo nella prima metà dell'anno si sono registrate perdite per 554 milioni di dati. Il rapporto ha anche svelato che questo tipo di violazioni dei dati sono piuttosto comuni per gli enti sanitari, andando a rappresentare quasi la metà (45%) delle violazioni di dati sanitari, con molte perdite di dati provocate da dispositivi smarriti o rubati.

Risposta di Bitdefender: GravityZone Full-Disk Encryption

GravityZone Full Disk Encryption utilizza i meccanismi di cifratura forniti da Windows (BitLocker) e Mac (FileVault), sfruttando la cifratura nativa dei dispositivi, per assicurare la massima compatibilità e le migliori prestazioni. Non ci sarà alcun agente aggiuntivo da impiegare e nessun server di gestione da installare. La soluzione offre:

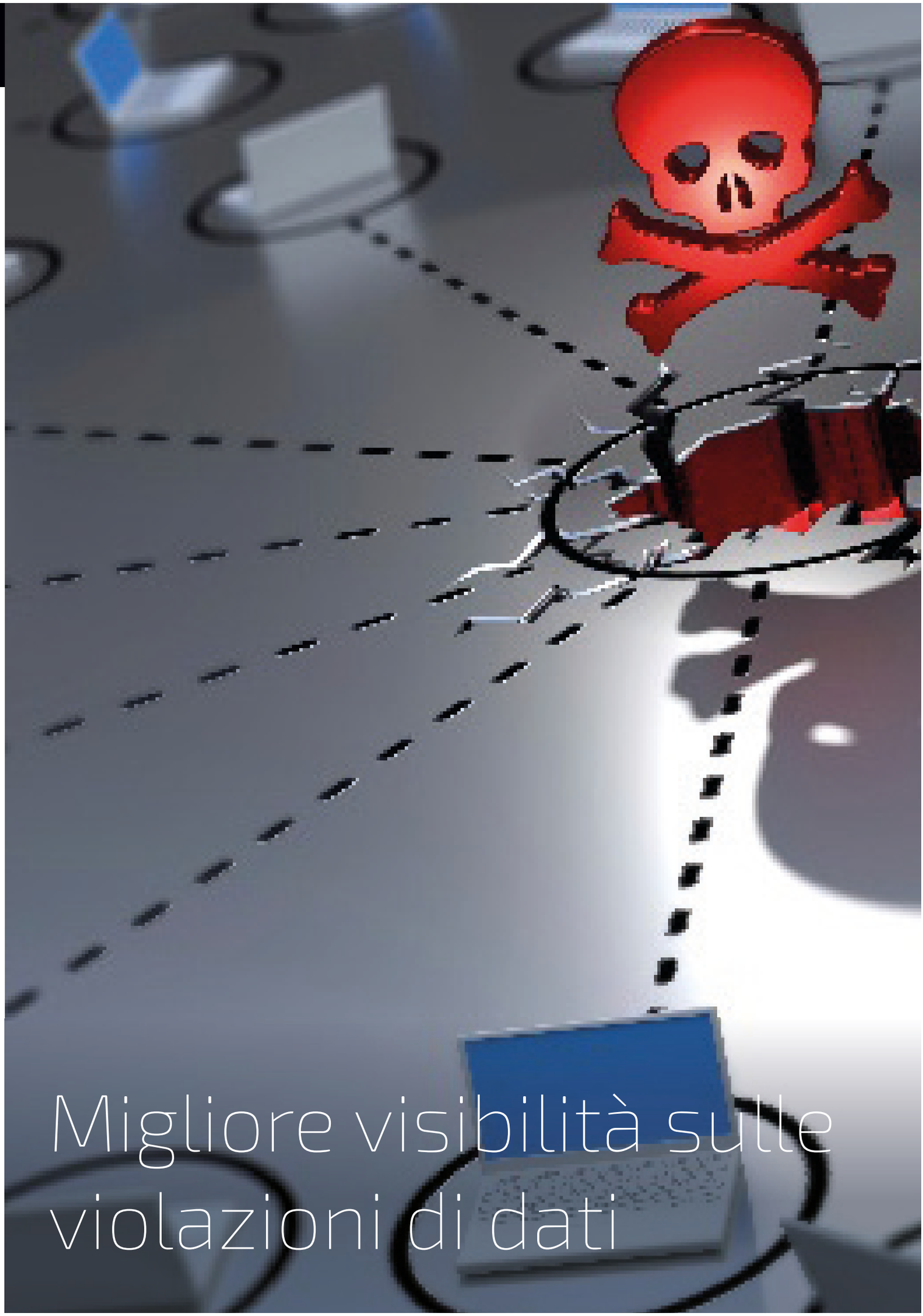
- Gestione della cifratura dalla stessa console cloud o locale utilizzata per la protezione degli endpoint
- La cifratura nativa per Windows (BitLocker) e Mac (FileVault), evitando problemi di prestazioni e non richiedendo alcun agente
- Impiego immediato di Full Disk Encryption negli endpoint e gestione delle chiavi di ripristino dalla console
- Rapporti specifici sulla cifratura che aiutano le aziende a dimostrare la conformità
- Controllo di autenticazione prima dell'avvio

Protezione dal furto di dati – Attacchi mirati

Aspetti chiave: in base allo stesso rapporto di Verizon, nel 2016 ci sono stati 1.616 attacchi social, di cui circa la metà (828) con una violazione dei dati confermata. Nel 95% dei casi, gli aggressori hanno poi attivato con successo un phishing con l'installazione di software. Il che è prevedibile, considerando le motivazioni e i bersagli della maggior parte degli aggressori sui social. Due terzi di tali soggetti puntano a guadagni finanziari, mentre un terzo a condurre vere e proprie operazioni di spionaggio. Entrambe queste motivazioni implicano il furto di credenziali, informazioni personali e segreti aziendali.

La risposta di Bitdefender: La piattaforma di protezione degli endpoint multilivello e di nuova generazione di Bitdefender è stata progettata e sviluppata da zero per proteggere dagli attacchi mirati più elusivi e avanzati. Più livelli di sicurezza offrono una protezione in fase di pre-esecuzione (Hyperdetect, Sandbox Analyzer) ed esecuzione (Anti-exploit avanzato e Application Control), oltre a una tecnologia innovativa specifica per la protezione dei Data Center (HVI- Hypervisor Introspection).

Hyperdetect	**Sandbox Analyzer**
• Offre prevenzione in fase di pre-esecuzione • Sfrutta l'apprendimento automatico più l'euristica avanzata • Blocca minacce sofisticate (PowerShell, attacchi privi di file, attacchi schermati, ransomware sconosciuti) • Fornisce la massima accuratezza di rilevamento senza falsi positivi • Offre impostazioni flessibili per ottimizzare una protezione aggressiva con una quantità minima di falsi positivi • Fornisce una totale visibilità sulle attività sospette	• Offre l'invio automatico dei file sospetti dagli endpoint per un'analisi nel sandbox • Fornisce opzioni per la modalità blocco o monitoraggio • Verdetto in tempo reale • Fornisce informazioni sul comportamento di file sconosciuti • Assicura una protezione totale a livello aziendale
Anti-exploit	**Controllo applicazioni**
• Protegge le applicazioni di terze parti e le applicazioni Microsoft usate più comunemente • Si concentra su strumenti e tecniche di attacco • Funziona come un livello aggiuntivo di sicurezza per vulnerabilità note non risolte da patch e zero-day • Funziona con un approccio fuori dagli schemi ed è progettato per garantire la massima precisione	• Convalida le applicazioni in esecuzione sull'endpoint • Aiuta a bloccare ransomware, attacchi mirati avanzati o malware zero-day



Migliore visibilità sulle violazioni di dati

Aspetti chiave: uno studio condotto nel 2017 dal Ponemon Institute sul costo delle violazioni di dati ha mostrato che il tempo medio per identificare una violazione è 191 giorni, , mentre quello per contenere la violazione è 66 giorni. Nel caso di Equifaxq, la violazione di dati si è verificata da metà maggio a luglio 2017, è stata scoperta al termine di luglio ed è stata resa pubblica solo a inizio settembre.

La risposta di Bitdefender: la visibilità è fondamentale per affrontare le minacce e le violazioni di dati. Se scoperta abbastanza presto, gli sforzi e i relativi costi richiesti per affrontare e mitigare le minacce interne risultanti dalle violazioni di dati potrebbero essere sostanzialmente ridotti. La piattaforma di protezione per endpoint multilivello e di nuova generazione di Bitdefender è stata sviluppata da zero in base a un principio di sicurezza flessibile, in pratica, oltre alle tecnologie di previsione, prevenzione e rilevamento, la suite di sicurezza include strumenti di visibilità dedicati, come Endpoint Security HD Insight e Security Analytics for EDR.

Endpoint Security HD Insight	Security Analytics planned for EDR
• Consente un'esecuzione in remoto (Sandbox) • Fornisce un miglior contesto sulle minacce • Connette le minacce con le azioni delle minacce • Offre una visione migliore sugli endpoint per future analisi e ulteriori azioni • Svela le minacce sospette (rapporti HD)	• Rileva picchi nelle attività dei malware • Rileva connessionibotnet/C&C • Rileva download di file sospetti (attacchi mirati) • Rileva l'esecuzione di processi sospetti (attacchi privi di file) • Rileva comportamenti anomali di applicazioni / sistema (estrazione dati e movimento laterale) • Rileva minacce interne (utenti dannosi / account utente compromesso)

Sintesi

Il GDPR è diventato una realtà e presto ogni azienda dovrà implementare tutte misure necessarie per ottenere la conformità. Tale processo è piuttosto complesso, in quanto comprende diversi passaggi come una valutazione e un'analisi accurata della maturità della privacy dei dati, un percorso dettagliato per affrontare i nuovi requisiti legislativi, una mappa completa per test di sicurezza, verifica e valutazione dei processi, oltre a un ciclo di comunicazione continuo per una costante osservanza e miglioramento.

Tra tutte queste iniziative, le aziende dovranno investire nella tecnologia come agevolatore principale per ottenere la conformità. Il GDPR intende definire gli attributi tecnologici più moderni per gestire dati strutturati e non strutturati con un forte accento sulla privacy e la protezione dei dati.

Attraverso la sua soluzione di sicurezza integrata, multilivello e di nuova generazione, Bitdefender è in posizione perfetta per aiutare le aziende a ottenere la conformità offrendo un set di tecnologie che rispondono senza problemi ai requisiti più rigorosi del GDPR.

Bitdefender è un fornitore globale di tecnologie di sicurezza che offre soluzioni in oltre 100 paesi attraverso una rete di collaborazioni a valore aggiunto, distributori e rivenditori. Dal 2001, Bitdefender produce costantemente tecnologie di sicurezza aziendali e consumer pluripremiate, ed è un fornitore di sicurezza leader nelle tecnologie cloud e di virtualizzazione. Attraverso Ricerca e Sviluppo, partnership e collaborazioni, Bitdefender ha migliorato i più alti standard nell'eccellenza della sicurezza, sia nella sua tecnologia numero uno sia nelle sue partnership strategiche con i migliori fornitori al mondo di tecnologie cloud e di virtualizzazione. Maggiori informazioni sono disponibili alla pagina http://www.bitdefender.it/

BD-Business-Nov.13.2017-Tk#: crea1826
Bitdefender-Whitepaper-GDPR-crea2140-A4-it_IT