Piattaforma SonicOS

L'architettura SonicOS è al centro di ogni firewall SonicWall fisico e virtuale, incluse le serie TZ, NS*a*, NSv e SuperMassive. SonicOS sfrutta la nostra tecnologia Reassembly-Free Deep Packet Inspection® (RFDPI) a singola fase e bassa latenza brevettata* e Real-Time Deep Memory Inspection™ (RTDMI) con brevetto depositato per fornire soluzioni efficaci ad alta sicurezza, collaudate nel settore, nonché caratteristiche quali SD-WAN, visualizzazione in tempo reale, virtual private networking (VPN) ad alta velocità e altre solide funzionalità di sicurezza.

Funzionalità firewall

Motore Reassembly-Free Deep Packet Inspection (RFDPI)	
Funzionalità	Descrizione
Reassembly-Free Deep Packet Inspection (RFDPI)	Si tratta di un motore di ispezione proprietario, brevettato e ad alte prestazioni, che esegue analisi bidirezionali del traffico basate sui flussi senza proxy o buffering allo scopo di individuare tentativi di intrusione, rilevare malware e identificare il traffico delle applicazioni in qualsiasi porta.
Ispezione bidirezionale	Con la scansione contemporanea del traffico in ingresso e in uscita per il rilevamento delle minacce, questa opzione impedisce l'utilizzo della rete come vettore di malware e come piattaforma per sferrare attacchi qualora venga introdotto un computer infetto.
Ispezione basata sui flussi	La tecnologia di ispezione priva di proxy e buffering genera una latenza estremamente bassa per le attività di ispezione DPI su milioni di flussi di rete simultanei, senza limiti per la dimensione dei flussi e dei file. Inoltre può essere applicata sia a protocolli comuni che a flussi TCP primari.
Architettura altamente parallela e scalabile	L'esclusivo motore RFDPI basato su architettura multi-core offre l'ispezione DPI ad alta velocità e consente di creare nuove sessioni in tempi estremamente brevi, agevolando la gestione dei picchi di traffico in reti complesse.
Ispezione single-pass	Un'architettura DPI single-pass consente di rilevare contemporaneamente malware e intrusioni e identificare le applicazioni, riducendo notevolmente la latenza dell'ispezione DPI e correlando tutte le informazioni sulle minacce in un'unica architettura.
Firewall e connettività di rete	
Funzionalità	Descrizione
Secure SD-WAN	Fungendo da alternativa a tecnologie più costose quali MPLS, Secure SD-WAN consente alle organizzazioni aziendali distribuite di creare, utilizzare e gestire reti protette ad alte prestazioni su vari siti remoti allo scopo di condividere dati, applicazioni e servizi utilizzando servizi Internet pubblici subito disponibili e a basso costo.
REST API	Consente al firewall di ricevere e sfruttare ogni tipo di feed di intelligence proprietario, dei produttori di dispositivi originali e di terze parti per combattere minacce avanzate come zero-day, utenti malintenzionati, credenziali compromesse, ransomware e minacce persistenti avanzate.
Stateful Packet Inspection	Tutto il traffico in transito nella rete viene ispezionato, analizzato e conformato alle policy di accesso del firewall.
Alta disponibilità/clustering	Supporta le modalità ad alte prestazioni Attivo/Passivo (A/P) con sincronizzazione dello stato, DPI Attivo/Attivo (A/A)[2] e clustering Attivo/Attivo.[2] DPI Attivo/Attivo trasferisce il carico di lavoro della Deep Packet Inspection all'appliance passiva per ottimizzare il throughput.
Protezione da attacchi DDoS/DoS	La protezione da flooding SYN offre una difesa dagli attacchi DOS che si basa su tecnologie di blacklist SYN di livello 2 e proxy SYN di livello 3. Inoltre tutela dagli attacchi DOS/DDoS mediante la protezione da flooding UDP/ICMP e la limitazione della frequenza di connessione.
Opzioni di installazione flessibili	Il firewall può essere implementato in modalità su Wire, Network Tap NAT o Layer 2 Bridge[2].
Bilanciamento del carico WAN	Bilancia il carico su più interfacce WAN con metodi basati sulle modalità round robin, percentuale o spill-over. Il routing in base alle policy crea degli instradamenti basati sui protocolli per dirigere il traffico verso una connessione WAN specifica, con possibilità di commutare su una WAN secondaria in caso di caduta dell'alimentazione.
Qualità del servizio (QoS) avanzata	Garantisce l'integrità delle comunicazioni strategiche tramite tagging 802.1p e DSCP e rimappatura del traffico VoIP sulla rete.
Supporto per gatekeeper H.323 e proxy SIP	Blocca le chiamate di spam richiedendo che tutte le chiamate in entrata siano autorizzate e autenticate dal gatekeeper H.323 o dal proxy SIP.

Firewall e connettività di rete (cont.)	
Funzionalità	Descrizione
Gestione di switch Dell N-Series e X-Series singola e a cascata[2]	Gestione delle impostazioni di sicurezza di porte aggiuntive, tra cui Portshield, HA, PoE e PoE+, attraverso un unico pannello di controllo utilizzando il cruscotto di gestione del firewall per gli switch di rete N-Series e X-Series di Dell.
Autenticazione biometrica	Supporto dell'autenticazione per dispositivi mobili come il riconoscimento delle impronte digitali, che non può essere facilmente condivisa o duplicata, per autenticare in modo sicuro l'identità degli utenti che accedono alla rete.
Autenticazione aperta e social login	Consente agli utenti guest di utilizzare le credenziali dei propri servizi di social network come Facebook, Twitter o Google+ per registrarsi e accedere a Internet e ad altri servizi guest attraverso la rete wireless host, la LAN o zone DMZ utilizzando l'autenticazione pass-through.
Autenticazione multidominio	Fornisce un metodo semplice e veloce per amministrare le policy di sicurezza su diversi domini di rete. Possibilità di gestire policy individuali per un singolo dominio o per un gruppo di domini.
Gestione e creazione di rapporti	
Funzionalità	Descrizione
Gestione basata sul cloud e on-premise	La configurazione e la gestione delle appliance SonicWall sono disponibili via cloud attraverso il SonicWall Capture Security Center e in sede tramite il SonicWall Global Management System (GMS).
Gestione avanzata con un unico dispositivo	Configurazione comoda e veloce tramite l'interfaccia Web intuitiva, oltre a un'interfaccia CLI completa e al supporto per SNMPv2/3.
Creazione di rapporti sul flusso delle applicazioni IPFIX/NetFlow	Esporta le analisi del traffico e i dati sull'uso delle applicazioni possono essere esportati tramite i protocolli IPFIX o NetFlow per il monitoraggio e la creazione di report in tempo reale e storici con strumenti come SonicWall Analytics o altri tool che supportano IPFIX e NetFlow con estensioni.
Virtual Private Networking (VPN)	
Funzionalità	Descrizione
Provisioning automatico delle VPN	Semplifica l'installazione dei firewall in ambienti distribuiti complessi automatizzando il provisioning iniziale del gateway VPN site-to-site tra i firewall SonicWall, garantendo l'applicazione istantanea e automatica della sicurezza e della connettività.
VPN IPSec per una connettività Site-to-Site	La VPN IPSec ad alte prestazioni consente al firewall di agire come un concentratore VPN per migliaia di altri grandi ambienti di rete, home office o sedi distaccate.
Accesso remoto tramite VPN SSL o client IPSec	Sfruttando la tecnologia VPN SSL senza client o un client IPSec semplice da gestire, è possibile accedere in tutta semplicità a messaggi e-mail, file, computer, siti Intranet e applicazioni da un'ampia serie di piattaforme.
Gateway VPN ridondante	Se si usano più WAN, è possibile configurare una VPN primaria e secondaria per un failover e un failback automatici di tutte le sessioni VPN.
VPN basato su routing	La possibilità di eseguire il routing dinamico tramite collegamenti VPN garantisce un'operatività continua anche in caso di guasto temporaneo al tunnel VPN, perché il traffico viene instradato senza interruzioni tra gli endpoint attraverso route alternative.
Sensibilità al contesto/al contenuto	
Funzionalità	Descrizione
Tracciamento delle attività degli utenti	L'identificazione degli utenti e il monitoraggio delle loro attività vengono realizzati tramite l'integrazione SSO trasparente con AD/LDAP/Citrix/Terminal Services, combinati a dettagliate informazioni ottenute dall'ispezione DPI.
GeoIP per l'identificazione del traffico da Paesi specifici	Con questa opzione è possibile identificare e controllare il traffico di rete in ingresso o in uscita da Paesi specifici. Lo scopo è proteggere dagli attacchi provenienti da origini note o sospette di attività pericolose o analizzare il traffico sospetto che ha origine nella rete. Possibilità di creare elenchi personalizzati di paesi e botnet per ignorare il tag non corretto di un paese o una botnet associato a un indirizzo IP, eliminando così il filtraggio indesiderato di indirizzi IP a causa di classificazioni errate.
Corrispondenza e filtraggio con espressioni regolari	Questa opzione identifica e controlla i contenuti che attraversano la rete mediante la corrispondenza delle espressioni regolari per impedire perdite di dati.

Servizi in abbonamento per la prevenzione delle violazioni

Capture Advanced Threat Protection[1]	
Funzionalità	Descrizione
Sandboxing multi-engine	La piattaforma sandbox multi-engine, che include la piena emulazione di sistema e tecnologie di analisi a livelli hypervisor, esegue il codice sospetto nell'ambiente sandbox virtualizzato, ne analizza il comportamento e fornisce visibilità sulle attività malevole.
Blocco fino al verdetto	Per impedire l'ingresso di file potenzialmente dannosi nella rete, i file inviati al cloud per l'analisi possono essere trattenuti al gateway finché non viene determinata la loro natura.
Analisi di un'ampia varietà di tipi di file	Supporta l'analisi di un'ampia gamma di tipi di file, tra cui programmi eseguibili (PE), DLL, documenti PDF e MS Office, archivi, JAR e APK, su diversi sistemi operativi come Windows, Android, Mac OS e ambienti multi-browser.
Rapida distribuzione delle firme	Quando un file viene identificato come dannoso, una signature viene inviata immediatamente ai firewall con abbonamento al servizio SonicWall Capture, ai database con le firme per l'antivirus a livello gateway e l'ispezione IPS e ai database di reputazione degli URL, degli IP e dei domini entro 48 ore.
Capture Client	Capture Client utilizza un motore statico di intelligenza artificiale (AI) per determinare le minacce prima che possano essere eseguite e permette di ripristinare uno stato precedente non infetto.
Prevenzione delle minacce crittografate	
Funzionalità	Descrizione
Decrittazione e ispezione TLS/SSL	Decifra e ispeziona in tempo reale il traffico crittografato TLS/SSL senza proxy alla ricerca di malware, intrusioni e fughe di dati, applicando le policy di controllo delle applicazioni, degli URL e dei contenuti per proteggere la rete dalle minacce nascoste all'interno del traffico crittografato. L'opzione è inclusa negli abbonamenti di sicurezza di tutti i modelli, tranne SOHO. Per quest'ultimo è venduta come licenza a parte.
Ispezione DPI-SSH	L'ispezione approfondita dei pacchetti del protocollo SSH (DPI-SSH) decripta e ispeziona i dati che attraversano i tunnel SSH, per prevenire attacchi basati su SSH.
Prevenzione delle intrusioni[1]	
Funzionalità	Descrizione
Protezione basata su contromisure	Il sistema di prevenzione delle intrusioni (IPS) integrato utilizza le firme e altre contromisure per eseguire la scansione dei payload dei pacchetti in cerca di exploit e vulnerabilità, coprendo un'ampia serie di vulnerabilità e attacchi.
Aggiornamenti automatici delle firme	Il team del SonicWall Threat Research ricerca continuamente nuovi aggiornamenti e li installa in numerose contromisure IPS, che interessano oltre 50 categorie di attacchi. Gli aggiornamenti sono subito attivi senza la necessità di riavvii o interruzioni del servizio.
Protezione IPS interna alle zone	La segmentazione della rete in varie zone di sicurezza, protette dalle intrusioni, consente di potenziare la sicurezza interna poiché impedisce alle minacce di propagarsi oltre i confini di una zona.
Rilevamento e blocco di comando e controllo Botnet (CnC)	Questa opzione consente di individuare e bloccare il traffico di comando e controllo proveniente dai bot nella rete locale e diretto ai domini e agli indirizzi IP che sono stati identificati come fonte di propagazione di malware o punti CnC noti.
Anomalia/abuso di protocolli	Questa opzione individua e blocca gli attacchi che abusano dei protocolli per tentare di aggirare l'IPS.
Protezione zero-day	Per proteggere la rete dagli attacchi zero-day, questa opzione assicura aggiornamenti costanti a fronte delle tecniche e dei metodi di exploit più recenti, coprendo migliaia di singoli exploit.
Tecnologia antievasione	La normalizzazione estesa dei flussi, la decodifica e altre tecniche impediscono l'ingresso non rilevato delle minacce nella rete, grazie all'uso di tecniche di evasione nei livelli da 2 a 7.
Prevenzione delle minacce[1]	
Funzionalità	Descrizione
Antimalware a livello gateway	Il motore RFDPI scansiona tutto il traffico in entrata, in uscita e tra le zone interne della rete alla ricerca di virus, trojan, key logger e altro malware in file di qualsiasi lunghezza e dimensione, su tutte le porte e tutti i flussi TCP.
Protezione contro il malware Capture Cloud	Un database residente sui server cloud SonicWall, costantemente aggiornato con decine di milioni di firme delle minacce, viene consultato per ottimizzare le capacità del database di firme integrato nel dispositivo, garantendo così un'ampia copertura delle minacce da parte del motore RFDPI.
Aggiornamenti di sicurezza costanti	I nuovi aggiornamenti sulle minacce vengono inviati automaticamente ai firewall sul campo con servizi di sicurezza attivi e sono subito attivi senza riavvii o interruzioni.
Ispezione bidirezionale dei TCP primari	Il motore RFDPI esegue l'analisi bidirezionale dei flussi TCP primari su tutte le porte per rilevare e prevenire le minacce in ingresso e in uscita.
Ampio supporto di protocolli	Identifica protocolli comuni come HTTP/S, FTP, SMTP, SMBv1/v2 e altri che non inviano dati nel formato TCP grezzo. Decodifica i payload per eseguire l'ispezione anti-malware anche se questi non utilizzano porte standard e ben note.

Controllo e intelligence delle applicazioni[1]	
Funzionalità	Descrizione
Controllo delle applicazioni	Verifica delle applicazioni o di singole funzionalità rilevate dal motore RFDPI a fronte di un database in crescita, contenente migliaia di firme di applicazioni. Questo controllo potenzia la sicurezza e la produttività della rete.
Identificazione di applicazioni personalizzate	Per verificare le applicazioni personalizzate è possibile creare firme basate su schemi o parametri specifici, che risultano univoci per un'applicazione nelle relative comunicazioni di rete. In questo modo si ottiene ulteriore controllo sulla rete.
Gestione della larghezza di banda delle applicazioni	La gestione della larghezza di banda delle applicazioni esegue l'allocazione granulare e la regolazione della larghezza di banda disponibile per applicazioni (o categorie di applicazioni), inibendo al tempo stesso il traffico di applicazioni non essenziali.
Controllo granulare	Questa opzione consente di controllare le applicazioni o componenti specifici di un'applicazione in base a pianificazioni, gruppi di utenti, elenchi di esclusione e una serie di attività con identificazione SSO degli utenti completa, mediante l'integrazione di LDAP/AD/servizi Terminal/Citrix.
Filtraggio dei contenuti[1]	
Funzionalità	Descrizione
Filtraggio dei contenuti interno/esterno	Mette in atto le policy di utilizzo accettabili e blocca l'accesso a siti web HTTP/HTTPS contenenti informazioni o immagini discutibili o non produttive con Content Filtering Service e Content Filtering Client.
Content Filtering Client	Consente di applicare policy che bloccano contenuti Internet specifici per i dispositivi Windows, Mac OS, Android e Chrome situati all'esterno del perimetro del firewall.
Controlli granulari	Mediante combinazioni di categorie è possibile bloccare determinati contenuti. Il filtraggio può essere pianificato in base all'ora del giorno, ad esempio durante l'orario scolastico o lavorativo, e applicato a gruppi o singoli utenti.
Cache Web	Le classificazioni degli URL sono memorizzate nella cache locale del firewall SonicWall, in modo che il tempo di risposta per l'accesso successivo ai siti Web visitati con maggior frequenza sia inferiore a un secondo.
Local CFS Responder	Local CFS Responder può essere implementato come appliance virtuale in cloud privati basati su VMWare o Microsoft Hyper-V. Questa soluzione costituisce un'opzione per la flessibilità di implementazione (Light weight VM) del database di rating CFS in vari casi d'uso sulla rete del cliente che richiedono una soluzione dedicata in loco in grado di velocizzare la richiesta di rating CFS e i tempi di riposta, oltre ad offrire un gran numero di elenchi di URL autorizzati/bloccati (+100.000) e si somma ai 1000 firewall SonicWall per le ricerche di rating CFS.
Antivirus e antispyware applicati[1]	
Funzionalità	Descrizione
Protezione su più livelli	Le funzionalità del firewall sono utilizzate come primo livello di difesa presso il perimetro, insieme alla protezione degli endpoint che impedisce l'ingresso di virus nella rete attraverso notebook, unità USB e altri sistemi non protetti.
Opzione di applicazione automatizzata	Assicura che ogni computer che accede alla rete abbia installato e attivato il software antivirus appropriato e/o il certificato DPI-SSL, eliminando i costi comunemente associati alla gestione dell'antivirus desktop.
Distribuzione e implementazione automatizzate	Per ridurre il carico amministrativo, l'installazione dei client per antivirus e antispyware avviene automaticamente, computer per computer, in tutta la rete.
Antivirus di nuova generazione	Capture Client utilizza un motore statico di intelligenza artificiale (AI) per determinare le minacce prima che possano essere eseguite e per ripristinare uno stato precedente non infetto.
Protezione antispyware	Grazie all'opzione di protezione avanzata contro gli spyware, è possibile eseguire scansioni e bloccare l'installazione di una serie completa di programmi spyware su desktop e notebook prima che vengano trasmessi dati riservati. Questo potenzia le prestazioni e la sicurezza dei computer desktop.

[1]Richiede un abbonamento aggiuntivo
[2] Serie firewall NSv non supportata

Informazioni su SonicWall

Da oltre 27 anni SonicWall combatte il crimine informatico proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di rilevamento e prevenzione automatizzata delle violazioni in tempo reale ottimizzata per le esigenze specifiche di oltre 500.000 organizzazioni in più di 215 paesi e regioni, per consentire loro di fare più affari con maggior sicurezza. Per maggiori informazioni visita **www.sonicwall.com** o seguici su Twitter, LinkedIn, Facebook e Instagram.

Partner Enabled Services
Serve aiuto per pianificare, ottimizzare o implementare una soluzione SonicWall? Gli Advanced Services Partner di SonicWall sono qualificati per fornire servizi professionali di altissimo livello. Per maggiori informazioni: www.sonicwall.com/PES.

SONICWALL®

Riepilogo delle funzionalità di SonicOS

Firewall

- Ispezione Stateful Packet
- Reassembly-Free Deep Packet Inspection
- Protezione dagli attacchi DDoS (UDP/ICMP/SYN flood)
- Supporto di IPv4/IPv6
- Autenticazione biometrica per accesso remoto
- Proxy DNS
- API REST

Decrittazione e ispezione TLS/SSL/SSH[2]

- Deep packet inspection per TLS/SSL/SSH
- Inclusione/esclusione di oggetti, gruppi o nomi di host
- Controllo SSL
- Controlli DPI SSL granulari per zona o regola

Capture Advanced Threat Protection[2]

- Real-Time Deep Memory Inspection
- Analisi multi-engine basata sul cloud
- Sandbox virtuale
- Analisi a livello hypervisor
- Emulazione di sistema completa
- Ispezione di un'ampia varietà di file
- Invio automatico e manuale
- Aggiornamenti in tempo reale dell'intelligence contro le minacce
- Blocco fino al verdetto
- Capture Client

Prevenzione delle intrusioni[2]

- Scansione basata sulle firme
- Aggiornamenti automatici delle firme
- Motore di ispezione bidirezionale
- Funzionalità per regole IPS granulari
- Identificazione tramite GeoIP
- Filtraggio botnet con elenco dinamico
- Corrispondenza con espressioni regolari

Anti-malware[2]

- Scansione anti-malware basata sui flussi
- Antivirus per gateway
- Antispyware per gateway
- Ispezione bidirezionale
- Nessun limite alle dimensioni dei file
- Database dei malware cloud

Identificazione delle applicazioni[2]

- Controllo delle applicazioni
- Gestione della larghezza di banda delle applicazioni
- Creazione di firme personalizzate per le applicazioni
- Prevenzione di eventuali perdite di dati
- Creazione di report sulle applicazioni tramite NetFlow/IPFIX
- Ampio database di firme delle applicazioni

Visualizzazione e analisi del traffico

- Attività degli utenti
- Utilizzo per applicazione/larghezza di banda/minaccia
- Analisi basate su cloud

Filtraggio dei contenuti Web HTTP/HTTPS[2]

- Filtraggio degli URL
- Proxy avoidance
- Blocco in base a parole chiave
- Filtraggio basato su policy (esclusione/inclusione)
- Inserimento intestazione HTTP
- Gestione della banda secondo categorie di valutazione CFS
- Modello di policy unificato con controllo delle applicazioni
- Content Filtering Client

VPN

- Secure SD-WAN
- Provisioning automatico delle VPN
- VPN IPSec per connettività site-to-site
- Accesso remoto tramite VPN SSL e client IPSec
- Gateway per la rete VPN ridondante
- Mobile Connect per iOS, Mac OS X, Windows, Chrome, Android e Kindle Fire
- VPN basato su routing (RIP/OSPF/BGP)

Connettività di rete

- PortShield
- Frame Jumbo
- Indagine del percorso MTU
- Registrazione avanzata
- VLAN trunking
- Port mirroring (NS*a* 2650 e superiori)
- QoS livello 2
- Sicurezza delle porte
- Routing dinamico (RIP/OSPF/BGP)
- Controller wireless SonicWall[1]
- Routing basato sulle policy (ToS/metrica ed ECMP)
- NAT
- Server DHCP
- Gestione della larghezza di banda
- Aggregazione dei link[1] (statica e dinamica)
- Ridondanza delle porte[1]
- Alta disponibilità A/P con State Sync
- Clustering A/A[1]
- Bilanciamento del carico in entrata/in uscita
- Bridge L2,[1] modalità Wire/Virtual Wire, modalità Tap, modalità NAT
- Failover WAN 3G/4G[1]
- Routing asimmetrico
- Supporto CAC (Common Access Card)

VoIP

- Controllo QoS granulare
- Gestione della larghezza di banda
- DPI per il traffico VoIP
- Supporto per gatekeeper H.323 e proxy SIP

Gestione e monitoraggio

- GUI Web
- Interfaccia a riga di comando (CLI)
- SNMPv2/v3
- Gestione e reporting centralizzati con SonicWall Global Management System (GMS)[2]
- Accesso
- Esportazione per Netflow/IPFix
- Backup della configurazione basato su cloud
- BlueCoat Security Analytics Platform
- Visualizzazione della larghezza di banda e delle applicazioni
- Gestione IPv4 e IPv6
- Creazione di report su altri tool (Scrutinizer)
- Display di gestione LCD[1]
- Gestione degli switch Dell N-Series e X-Series inclusi gli switch a cascata[1]

Wireless[1]

- WIDS/WIPS
- Prevenzione di access point non autorizzati
- Fast roaming (802.11k/r/v)
- Selezione canale automatica
- Analisi dello spettro RF
- Visualizzazione in pianta
- Visualizzazione della topologia
- Cambio automatico di banda
- Beamforming
- Equità di accesso alla rete (AirTime fairness)
- Estensore MiFi
- Quote cicliche guest
- Portale ospite LHM

Wireless integrato (solo serie TZ)

- Dual-band (2,4 GHz e 5,0 GHz)
- Standard wireless 802.11 a/b/g/n/ac
- Rilevamento e prevenzione delle intrusioni wireless
- Servizi guest wireless
- Lightweight hotspot messaging
- Segmentazione degli access point virtuali
- Captive portal
- ACL cloud

[1] Non supportato su firewall serie NSv
[2] Richiede un abbonamento aggiuntivo.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

© 2018 SonicWall Inc. TUTTI I DIRITTI RISERVATI. SonicWall è un marchio o marchio registrato di SonicWall Inc. e/o delle sue affiliate negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi e marchi registrati appartengono ai rispettivi proprietari.
Datasheet-SonicOSplatform-US-VG-MKTG4136