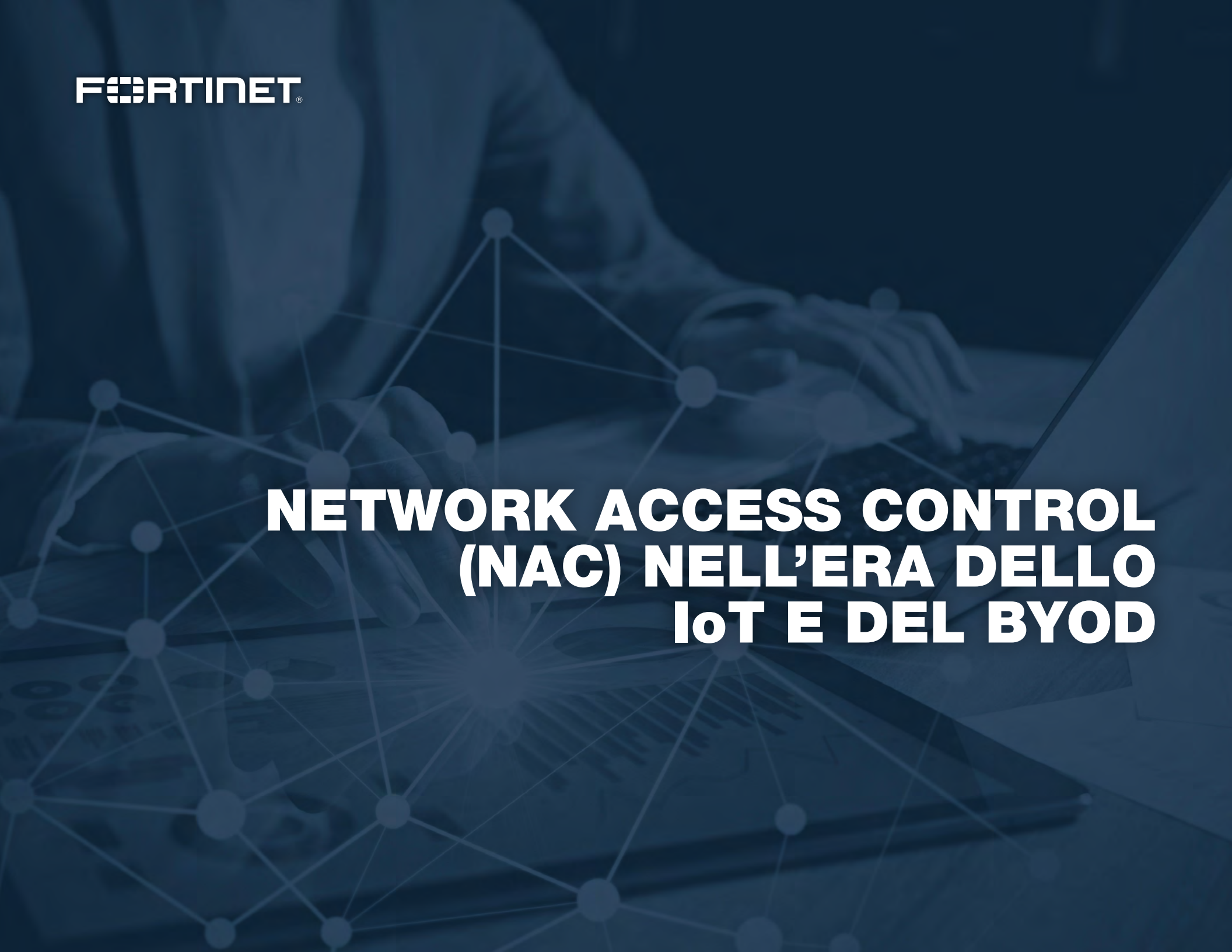


NETWORK ACCESS CONTROL (NAC) NELL'ERA DELLO IoT E DEL BYOD

SOMMARIO

SINTESI PRELIMINARE

Con la continua proliferazione dell'Internet of Things (IoT) e dei dispositivi mobili, si amplia l'infrastruttura informatica aziendale suscettibile ad attacchi e si evidenziano nuove lacune e vulnerabilità nel perimetro della rete. Allo stesso tempo, si fanno sempre più sofisticate le strategie di attacco agli endpoint adottate dagli exploit zero-day e dalle minacce avanzate persistenti. Gli architetti della sicurezza necessitano di migliori controlli di accesso per proteggere dalle minacce i singoli dispositivi e la rete nel suo insieme e per assicurare il rispetto di standard di conformità sempre più rigorosi. Per affrontare queste sfide, le soluzioni di sicurezza NAC (Network Access Control) devono evolversi per fornire funzionalità più robuste, in grado di supportare le esigenze attuali: riconoscimento, contenimento e attenuazione delle minacce.

INTRODUZIONE: L'EVOLUZIONE DEL CONTROLLO DEGLI ACCESSI

L'adozione diffusa in ufficio dei prodotti IoT e delle politiche BYOD (Bring Your Own Device) offre nuove funzionalità aziendali ma, allo stesso tempo, crea nuove sfide. Da un lato, non esiste praticamente alcuna standardizzazione della configurazione dei dispositivi BYOD o IoT. In ogni singola organizzazione, ci sono potenzialmente centinaia di tipi di dispositivi, marchi e sistemi operativi attivamente utilizzati, molti dei quali mancano di funzioni di sicurezza di livello aziendale. Proprio per questo, gli endpoint rimangono un obiettivo preferenziale degli attacchi sofisticati.

Il controllo dell'accesso alla rete da parte dei dispositivi è stato sin dall'inizio, ed è tuttora, un fattore essenziale per la protezione degli endpoint.
Il funzionamento della prima generazione di soluzioni NAC era sostanzialmente basato sull'autenticazione e l'autorizzazione degli endpoint (principalmente PC locali gestiti dall'IT) attraverso una semplice tecnologia di scansione e blocco.

Tuttavia, quando è sorta l'esigenza di gestire l'accesso di utenti guest alle reti aziendali, si è resa necessaria un'evoluzione delle funzionalità di controllo degli accessi. Le soluzioni NAC di seconda generazione consentivano un accesso limitato a Internet per gli utenti esterni (ad esempio visitatori, collaboratori esterni, partner commerciali).

Ma ora, con i profondi cambiamenti che interessano sia l'interno delle infrastrutture di rete che il panorama delle minacce esterno, sommati alle pressioni di sempre più rigide normative di settore e leggi sulla privacy dei dati, le soluzioni NAC devono evolvere di nuovo. Per proteggere completamente gli endpoint BYOD e IoT, le aziende devono essere in grado di vedere dove si trova ogni dispositivo, cosa fa e come si connette ad altri dispositivi nella topologia di rete. In questo scenario, le soluzioni NAC di terza generazione devono coordinare tutta la visibilità, i controlli e le risposte automatiche degli endpoint.

SEZIONE 1:
VISIBILITÀ DELL'INTERA RETE

Non è possibile proteggere ciò che non si vede. La mancanza di visibilità degli endpoint rende un'organizzazione vulnerabile a rischi invisibili. In un recente sondaggio, il 42% dei professionisti IT afferma di aver subito una violazione dagli endpoint, mentre un altro 20% riferisce di non sapere se una violazione subita sia stata causata da un endpoint compromesso.[1]

I team addetti alla sicurezza devono poter monitorare tutti i componenti dell'infrastruttura di rete in molti luoghi diversi, compreso l'estremo perimetro della rete. Per approntare difese forti, è necessario iniziare da una visione completa dei dispositivi interni (computer, smartphone, laptop, server, dispositivi IoT, dispositivi medici, terminali POS) e di qualsiasi altro dispositivo basato su IP attraverso un'unica vista integrata della topologia di rete.

[1] Lee Neely, "Endpoint Protection and Response: A SANS Survey," SANS Institute, 12 giugno 2018.

Le funzionalità di valutazione dei rischi di una soluzione NAC di terza generazione devono identificare il tipo di dispositivo e la configurazione del software (compreso lo stato di aggiornamento della protezione antivirus e antimalware). Questa valutazione della vulnerabilità degli endpoint deve riguardare anche i dispositivi headless (che non possono supportare la sicurezza integrata a causa delle loro limitate capacità), una categoria in cui ricadono molti dispositivi IoT.

Le organizzazioni devono inoltre essere in grado di rilevare e classificare automaticamente tutti gli utenti potenziali associati ai dispositivi prima di concedere l'accesso alla rete: ad esempio, quali dispositivi hanno registrato in rete e persino il luogo e l'ora della richiesta di connessione. Inoltre, le funzioni di visibilità e valutazione dei rischi della soluzione NAC devono effettuare scansioni continue per individuare comportamenti anomali degli utenti o segni di compromissione degli endpoint dopo la connessione.

63%

Il delle organizzazioni non è in grado di monitorare i dispositivi mobili quando lasciano la rete aziendale.

"The Cost of Insecure Endpoints," Ponemon Institute, giugno 2017.

SEZIONE 2:
CONTROLLI BASATI SU POLICY

Dopo l'identificazione di utente e dispositivo, una soluzione NAC di terza generazione deve essere in grado di implementare controlli di accesso granulari, basati su policy, attraverso una segmentazione dinamica della rete. La segmentazione della rete crea livelli di sicurezza più profondi, isolando i dati sensibili e creando barriere per impedire che le minacce si diffondano in direzione est-ovest all'interno dell'organizzazione.

Per rendere possibile tutto ciò, le soluzioni NAC devono integrarsi con altre soluzioni di sicurezza top di gamma, compresi prodotti di sicurezza di fornitori terzi. Questa capacità è critica per la protezione delle moderne reti multi-vendor. La soluzione deve essere in grado di sfruttare gli switch, i router e i punti di accesso esistenti nell'infrastruttura per stabilire un inventario in tempo reale delle connessioni e imporre un controllo dell'accesso alla rete basato sulla segmentazione.

La soluzione NAC deve regolare dinamicamente a quali parti della rete e a quali risorse i dispositivi e gli utenti possono accedere e quando possono accedervi, il tutto sulla base di policy di controllo predefinite.

Le organizzazioni spendono una media di 1.156 ore e 3,4 MILIONI DI DOLLARI ogni settimana per fronteggiare i rischi connessi agli endpoint.

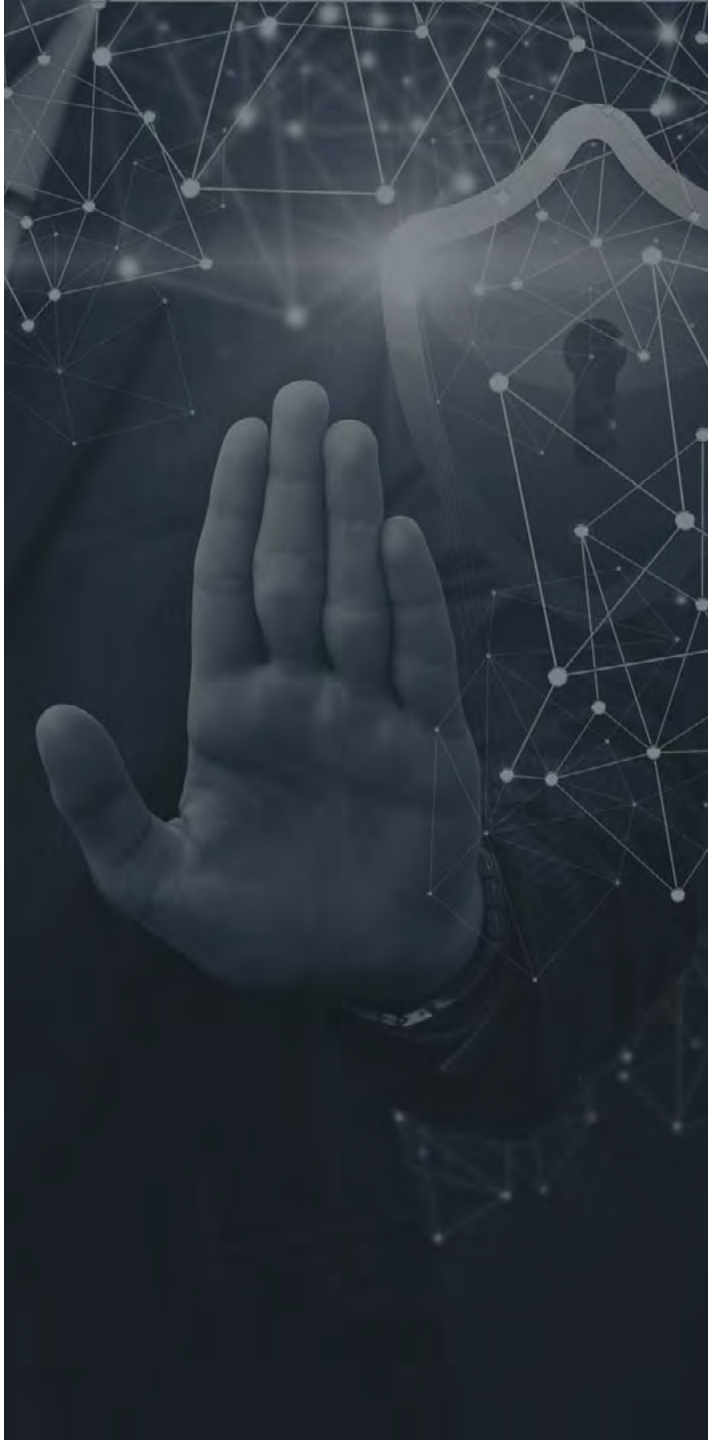
"The Cost of Insecure Endpoints," Ponemon Institute, giugno 2017.

SEZIONE 3:
RISPOSTE AUTOMATIZZATE ALLE MINACCE

Secondo uno studio recente, il tempo medio per rilevare una violazione rimane elevato (197 giorni), così come il tempo medio per contenerla (69 giorni).[2] L'integrazione supporta anche la capacità delle soluzioni di sicurezza di inviare e ricevere threat intelligence in tempo reale per coordinare le azioni nell'intera organizzazione. Questo tipo di automazione è il "Santo Graal" di un'architettura di sicurezza connessa. Le soluzioni NAC di terza generazione devono includere un livello di orchestrazione che aggreghi tutti i dati di sicurezza, al fine di classificare automaticamente le minacce in base alla loro priorità e definire quindi risposte di attenuazione coordinate in modo dinamico.

I dispositivi o gli utenti che violano una determinata policy di rete devono attivare immediatamente una risposta di contenimento unificata in tutta l'architettura di sicurezza. Tale risposta può prevedere la terminazione automatica di una connessione, restrizioni all'accesso alla rete, isolamento in quarantena e/o una serie di azioni di notifica.

Questi tipi di risposte automatizzate alle minacce possono ridurre i tempi di contenimento da diversi giorni a pochi secondi, proteggere le informazioni sensibili e l'IP e, allo stesso tempo, supportare la conformità a norme, standard e leggi sulla privacy dei dati sempre più severe.



[2] Larry Ponemon, "Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT," SecurityIntelligence, 11 luglio 2018.

L’AUTOMAZIONE DELLE SOLUZIONI DI RILEVAMENTO DEGLI ENDPOINT E DI RISPOSTA È LA MASSIMA PRIORITÀ PER I PROFESSIONISTI DELLA SICUREZZA INFORMATICA CHE INTENDONO APPLICARE CONTROLLI SUGLI ENDPOINT. SOLO IL 45% RIFERISCE CHE QUESTI PROCESSI SONO COMPLETAMENTE AUTOMATIZZATI.

Lee Neely, “Endpoint Protection and Response: A SANS Survey,” SANS Institute, 12 giugno 2018.

RIEPILOGO: ASPETTI DA CONSIDERARE

Di fronte ai cambiamenti dell'infrastruttura di rete, ad attacchi sofisticati agli endpoint e ai requisiti di conformità sempre più rigidi, le organizzazioni necessitano di controlli di accesso alla rete di terza generazione, che contribuiscano a proteggere i dispositivi mobili e intelligenti connessi. Una soluzione NAC per questo scenario deve soddisfare i criteri seguenti:

- ☐ **Visibilità.** Una soluzione NAC deve essere in grado di vedere e valutare una serie completa di endpoint (inclusi i dispositivi IoT) prima che si connettano alla rete. Deve inoltre essere in grado di classificare l'eventuale utente del dispositivo. Il riconoscimento dei rischi del dispositivo e dell'utente deve proseguire dopo la connessione.
- ☐ **Valutazione delle vulnerabilità degli endpoint.** La soluzione deve anche essere in grado di determinare le vulnerabilità critiche dei dispositivi, come versioni software obsolete o patch non installate.
- ☐ **Policy di controllo granulari.** Una volta identificati il dispositivo e l'utente, la soluzione deve essere in grado di automatizzare le policy e i controlli di sicurezza, nonché la condivisione della threat intelligence.
- ☐ **Integrazione.** Una soluzione NAC deve integrarsi perfettamente con le altre soluzioni presenti nell'intera architettura di sicurezza, compresi i prodotti di terze parti, per condividere attivamente le informazioni pertinenti sulle potenziali minacce e applicare controlli in tutta l'organizzazione estesa.
- ☐ **Risposte alle minacce in tempo reale.** Per gli endpoint che potrebbero essere compromessi, le organizzazioni necessitano di una soluzione NAC che faciliti risposte automatiche in tempo reale alle minacce e contribuisca a contenere immediatamente i dispositivi sospetti prima che si verifichino infezioni o danni gravi.
- ☐ **Automazione dei flussi di lavoro.** La soluzione deve consentire il provisioning self-service degli utenti, l'ingresso automatizzato dei nuovi dispositivi e la visualizzazione di messaggi per interventi di auto-correzione nel caso in cui un dispositivo non soddisfi gli standard minimi di sicurezza.
- ☐ **Scalabilità e flessibilità.** Una soluzione NAC di terza generazione deve implementare un'architettura scalabile, in grado di supportare in modo conveniente più sedi aziendali e un numero illimitato di dispositivi. Deve offrire modalità di distribuzione flessibili, con opzioni fisiche, virtuali e cloud.

FORTINET®

www.fortinet.com

ITALIA - ROMA
Via del Casale Solaro, 119
00143 Roma
Italia
Vendite: +39 06-51573-330

ITALIA - MILANO
Centro Torri Bianche
Palazzo Tiglio
20871 Vimercate (MB)
Italia
Tel: +39 039 687211

SEDE GLOBALE
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
Stati Uniti
Tel: +1.408.235.7700
www.fortinet.com/sales

UFFICIO VENDITE EMEA
905 rue Albert Einstein
06560 Valbonne
Francia
Tel: +33,4.8987,0500

UFFICIO VENDITE APAC
8 Temasek Boulevard #12-01
Suntec Tower Three
Singapore 038988
Tel: +65-6395-7899
Fax: +65-6295-0015

AMERICA LATINA SEDE CENTRALE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

275502-0-0-IT aprile 12, 2019 7:53 AM

ebook-nac-in-the-era-of-iot-and-byod_IT