

RTINET

C,
ELO
UTC
ATA

QUALE STRATEGIA DEVONO METTERE IN ATTO LE IMPRESE PER PROTEGGERSI AL MEGLIO?

L'evoluzione digitale richiede un nuovo approccio alla sicurezza. Serve un cambio di passo, che deve essere sposato sia dal management che dai dipendenti. Per riuscire a contrastare gli sforzi continui dei criminali informatici, le organizzazioni devono includere le strategie di sicurezza nei loro sforzi di digital transformation. Devono inserirla nei piani di sviluppo e di crescita e comprendere che non si tratta solo di una ma di un'im-

che nel cloud. Questo approccio di condividere una threat intelligence utilizzabile in modo rapido riduce le finestre di rilevamento e fornisce una risoluzione necessaria per gli exploit di oggi. Consente quindi più soluzioni per reagire all'unisono alla minaccia. Velocità, integrazione e fondamentali per la per questo Fortinet rivolge alle imprese dimensioni dalle difese, le differenze di investimento

correlata e condivisa su scala. L'intelligence avanzata di sicurezza deve essere automatizzata per ridurre le finestre di rilevamento necessarie e fornire una soluzione rapida. L'integrazione dei singoli prodotti attraverso la rete distribuita, combinata alla segmentazione strategica, contribuirà in modo significativo a combattere la natura sempre più intelligente e automatizzata degli attacchi. I dispositivi di sicurezza di legacy e isolati e una scarsa considerazione della sicurezza continuano a rappresentare un pericolo e aumentano il rischio nel panorama delle minacce odierne, poiché non forniscono visibilità o controllo adeguati. Invece, un "security fabric", un tessuto di sicurezza che copra tutto l'ambiente di rete esteso e integrato tra ogni elemento, è vitale per comprendere il panorama odierno e rispondere in continua crescita e per ridurre la superficie di attacco in

IN QUESTO
SEMPRE
(SOFTWARE)
NETWORK
RETI
INTE
IN S
LA
S

COS'È IL SECURITY FABRIC?

È l'approccio di Fortinet al tema della cyber security, è l'insieme di soluzioni per rispondere alle minacce complesse. Una piattaforma organicamente da zero, che offre un ampio set di funzionalità di sicurezza con automazione eccezionali, e l'implementazione in modo

Fortinet continuano a colpire le minacce. Lo confermano le analisi del team FortiGuard Labs del Global Threat Landscape

avversari continuano a incorporare nuove minacce e a sfruttare tecniche sempre più automatizzate in termini di velocità e scalabilità per le loro attività dannose, segmentazione e integrazione diventano elementi critici di sicurezza strategica per gli ambienti IT e OT odierni. Non esiste una strategia di difesa futura che includa l'automazione o il machine learning senza un mezzo per raccogliere, elaborare e agire sulle informazioni sulle minacce in modo integrato per produrre una risposta intelligente.

informatici crescono e ogni organizzazione sente l'impatto, con rilevazioni di minacce in crescita. Prima, il giorno, ora

ROBOQUATTRO

COLOMBO DESIGN

ROBOQUATTRO

ID 41 Design:
Colombo Design



OL
Oroplus



CM
Cromat
Matt chrome



OM
Oromat
Matt gold



BI RAL 9016
Biancomat
Matt White



CR
Cromo
Chrome



NM RAL 9005
Neromat
Matt Black



DKZERO

ID 41 R-RY Ø50

CD 49 BZG G Ø50

ID 42 IM

ID 42 DK/SM

ID 42 DK0/SM

ID 42 DK Z



OL - OM - CR - CM - BI - NM

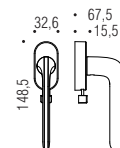
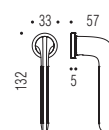
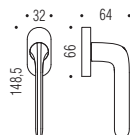
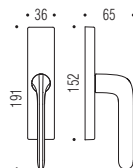
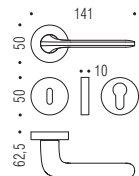
OL - OM - CR - CM - BI - NM

OL - OM - CR - CM - BI - NM

OL - OM - CR - CM - BI - NM

OL - OM - CR - CM

OL - CR - CM





Materiale: Cromall®
Material: Cromall®

