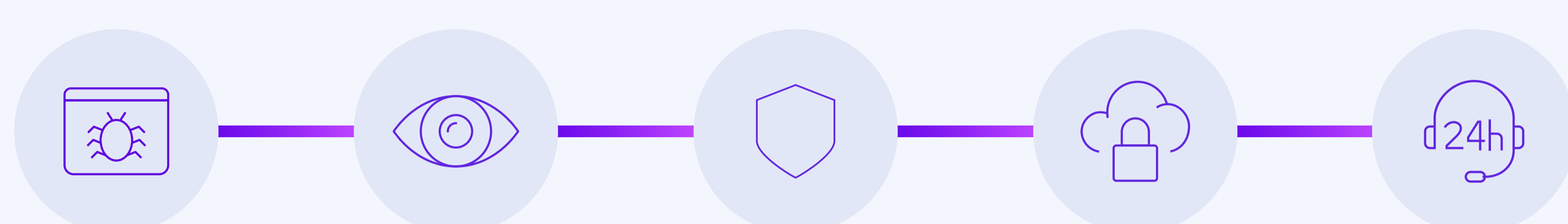


Come scegliere la soluzione ottimale per la tua azienda

Le aziende si trovano ad affrontare sempre più minacce informatiche e obblighi normativi con poche risorse e budget limitati. Ecco perché è fondamentale sfruttare gli investimenti di sicurezza esistenti per ottimizzare il ritorno sull'investimento grazie a endpoint, accesso al cloud, VPN, sistemi di sicurezza perimetrale e sistemi di registrazione.

Questa tabella illustra tre servizi di gestione delle minacce principali: Managed Detection and Response (MDR), Extended Detection and Response (XDR) e N-able MDR. Metti a confronto i dati di ogni servizi per decidere dove investire il budget a disposizione e come ottimizzare la protezione informatica.



	MDR	XDR	N-able MDR
Responsabile gestione	Servizio gestito	Servizio gestito o gestione del cliente	Servizio gestito o gestione del cliente
Origini dati	<ul style="list-style-type: none"> Endpoint Traffico di rete Servizi cloud 	<ul style="list-style-type: none"> Endpoint Traffico di rete Perimetro Servizi cloud Active Directory Posta elettronica 	<ul style="list-style-type: none"> Endpoint Traffico di rete Perimetro Servizi cloud Active Directory Posta elettronica
Rilevamenti	<ul style="list-style-type: none"> Malware/loC Attacchi senza file 	<ul style="list-style-type: none"> Malware/loC Attacchi senza file Anomalie comportamentali Machine learning 	<ul style="list-style-type: none"> Malware/loC Attacchi senza file Anomalie comportamentali Machine learning
Indagine	Inclusa nel servizio SOC (variabile)	<ul style="list-style-type: none"> Richiede servizio SOC gestito Il SOC esegue le indagini 	<ul style="list-style-type: none"> Inclusa nel servizio SOC Inclusa nel servizio SOC
Risposta	Servizio SOC servizio gestito di rilevamento e risposta: gestione autonoma	Richiede servizio SOC gestito	Servizio SOC: team di sicurezza esteso
Riparazione	<ul style="list-style-type: none"> Isolamento e blocco endpoint Blocco traffico (IP/DNS sorgente) Reimpostazione o disattivazione accesso al cloud 	<ul style="list-style-type: none"> Isolamento e blocco endpoint Blocco traffico (IP/DNS sorgente) Reimpostazione o disattivazione account/gruppo Reimpostazione o disattivazione accesso al cloud 	<ul style="list-style-type: none"> Isolamento e blocco endpoint Blocco traffico (IP/DNS sorgente) Reimpostazione o disattivazione account/gruppo Reimpostazione o disattivazione accesso al cloud
Reportistica	Basata su capacità SOC	<ul style="list-style-type: none"> Richiede servizio SOC gestito Reportistica cogestita 	<ul style="list-style-type: none"> Rilevamenti Indagini Report personalizzati Info sulla conformità Report di ispettori sulla conformità Prospetti riassuntivi
Intelligence delle minacce	Di base	Di base	<ul style="list-style-type: none"> Team e ricercatori dedicati all'intelligence minacce Feed intelligence minacce Monitoraggio del dark web Tecnologia antifrode gestita
Velocità di distribuzione	<ul style="list-style-type: none"> Richiede prima di tutto licenze per servizi Settimane per configurazione e messa a punto 	<ul style="list-style-type: none"> Richiede prima di tutto licenze per servizi Settimane per configurazione e messa a punto 	<ul style="list-style-type: none"> Implementazione in pochi giorni Distribuzioni agent tramite criteri di gruppo (GPO)
Visibilità	Il SOC richiede report o informazioni sulle indagini	Cogestione variabile	<ul style="list-style-type: none"> Visibilità completa per i clienti che vedono e hanno accesso allo stesso portale del SOC Reportistica clienti in tempo reale
Contesto	<ul style="list-style-type: none"> Il SOC richiede report o informazioni su indagini Reportistica conformità limitata 	Cogestione variabile	<ul style="list-style-type: none"> Vista semplificata: i clienti vedono e hanno accesso allo stesso portale del SOC Minacce e rilevamenti Programmi in caso di rischi Violazioni criteri di integrità rete Informazioni sulla conformità

Individua le minacce ed elimina i rischi

Scopri di più su come i servizi Managed Detection and Response e la Security Operations Platform di N-able possono aiutare il tuo team a individuare minacce, ridurre i rischi informatici e ad assumere il controllo di ogni aspetto.

