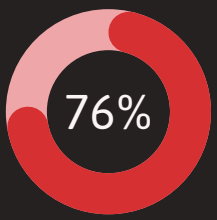
KOLIKO JE SIGURNO VAŠE POSLOVANJE OD NAPADA RANSOMWARE-A?

Odaberite naše napredne usluge **Endpoint Protection**, **Identity Management** i **Data Protection** za ključnu obranu protiv ransomware napada i drugih Cyber prijetnji.

Ne čekajte da postanete žrtva haker napada;
postanite otporni na Cyber prijetnje već danas!

security@qss.ba

U anketi od 1200 organizacija



organizacija je pretrpjelo barem jedan **ransomware napad** prošle godine.

www.qss.ba www.qsscloud.ba prodaja@qss.ba +387 33 563 000

QSS smart it.

NAJČEŠĆI ZLONAMJERNI SOFTVERI

Ransomware
Tip zlonamjernog softvera koji šifrira datoteke korisnika, onemogućavajući pristup do njih dok se ne plati otkupnina

Spyware
Softver koji tajno prikuplja informacije s uređaja korisnika, često bez njihovog znanja ili odobrenja.

Virusi
Programi koji se mogu samokopirati i širiti s jednog na drugi sistem, često korumpirajući ili brišući podatke.

NAJČEŠĆI CYBER NAPADI

Phishing
Napadi koji koriste komunikacijske kanale poput emaila i društvenih mreža za krađu podataka ili širenje malvera.

Napadi na identitet
Eksploatišu autentifikacijske slabosti za neovlašteni pristup i krađu podataka.

Endpoint Protection

Zašto **Endpoint zaštita** za **Cyber otpornost**?

Endpoint zaštita omogućava brzo otkrivanje, blokiranje i zaustavljanje napada koji se u tom trenutku odvija.

Endpoint zaštita ili endpoint sigurnost je praksa osiguravanja krajnjih tačaka ili ulaznih tačaka korisničkih uređaja (kao što su desktop računala, prijenosna računala i mobilni uređaji) od eksploatacije od strane malicioznih vanjskih korisnika.

*Zaštita endpointa je ključna za sprečavanje **ransomware napada** jer endpointi mogu biti početne tačke za ulazak napadača. **Implementiranjem sigurnosti endpointa, organizacije mogu detektovati i blokirati napade prije nego što ugroze mrežu i podatke.***

Zaštita od malwarea
Osigurava zaštitu uređaja od malwarea i drugih zlonamjernih softverskih aplikacija.

Prevencija napada
Pomaže u sprečavanju napada izvana, kao što su DDoS napadi, phishing napadi, i drugi oblici napada na mrežu.

Dijagnostika i analiza
Pruža dijagnostiku i analizu stanja na uređajima, što može pomoći u identifikaciji ranjivosti koje bi se mogle iskoristiti za napad.

Praćenje aktivnosti
Pratiti aktivnosti na uređajima kako bi se otkrile potencijalne prijetnje ili sumnjive aktivnosti.

Automatizacija
Može automatizirati procese zaštite, kao što su automatske zakrpe i ažuriranja, što smanjuje rizik od napada.

Fleksibilnost
Može se prilagoditi specifičnim potrebama organizacije, kao što su vrsta uređaja koji se koriste i vrsta podataka koji se pohranjuju.

Smanjenje rizika
Pomaže u smanjenju rizika od napada, što može smanjiti troškove povezane s obnovom i popravkom sistema nakon napada.

Poboljšajte **Cyber otpornost** implementacijom napredne **Endpoint zaštite** i efikasnim **upravljanjem identitetima** za sveobuhvatnu zaštitu.

security@qss.ba

Identity Management

Zašto **Identity Management** za **Cyber otpornost**?

Efikasno upravljanje identitetima ključno je za cyber otpornost, jer omogućava preciznu kontrolu pristupa i smanjuje rizik od neovlaštenih upada. Strogim autentifikacijskim i autorizacijskim politikama, organizacije ograničavaju pristup samo ovlaštenim korisnicima, **čime jačaju zaštitu od cyber prijetnji i minimiziraju rizik od ransomware napada.**

Primjena principa Zero Trust na sav pristup

Pretpostavka kompromitacije, stroga provjera povjerenja, i ograničen pristup privilegijama.

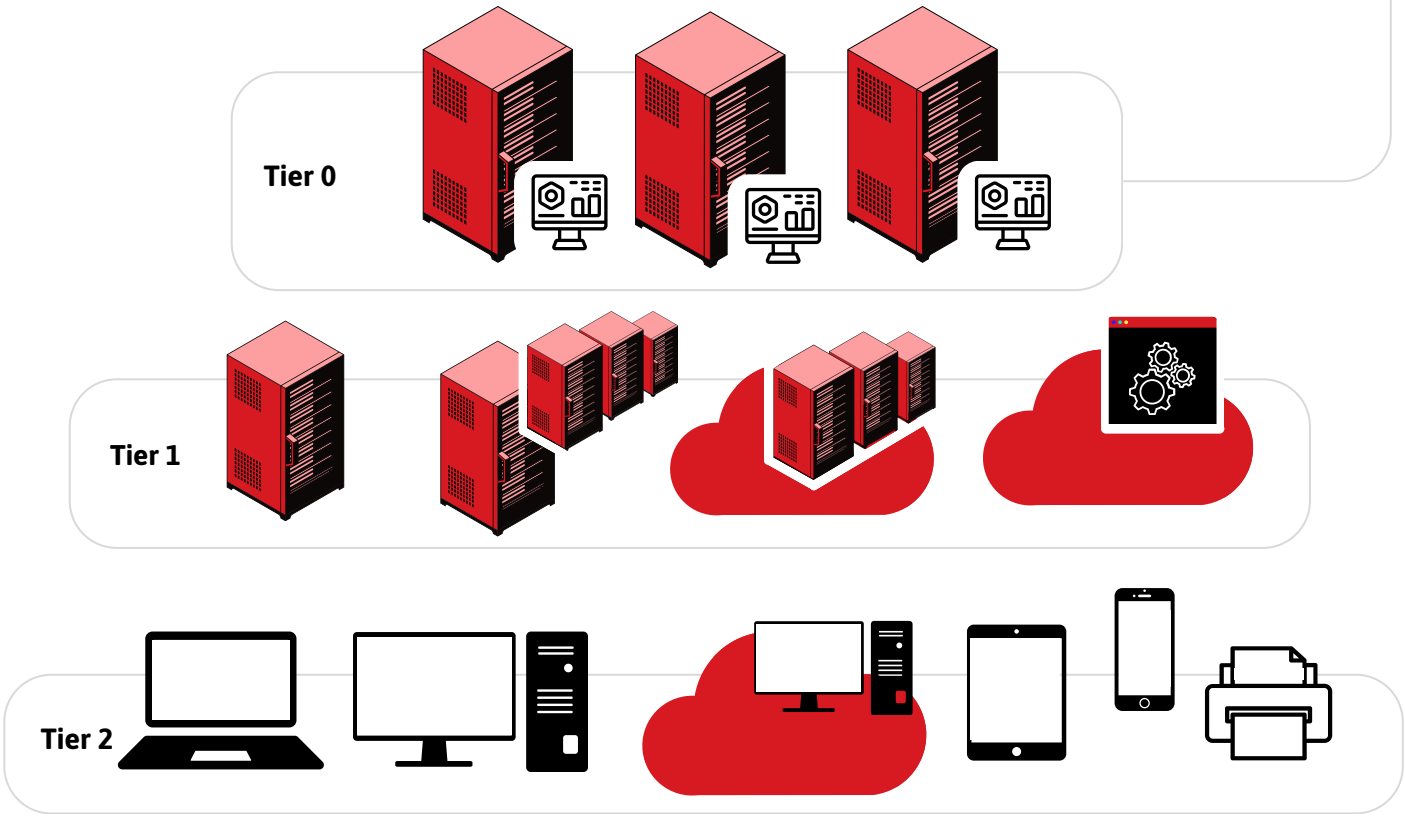
Sprečavanje neovlaštenog eskaliranja privilegija

Sprečavanje neovlaštenog eskaliranja privilegija kroz primjenu hijerarhijske zaštite ključnih nivoa - kontrolnog, upravljačkog, i nivoa podataka, zajedno s neprekidnom revizijom konfiguracija i aktivnim nadgledanjem te reagovanjem na anomalije koje signaliziraju moguće napade.

Osiguranje sveobuhvatne sigurnosti i sprovođenje politika na svakom sloju

Primjena sigurnosnih politika na sve, od unutrašnjih do vanjskih pristupa, te kontrola svih oblika pristupa, uključujući korisnike, upravljački kadar, API-je i servisne račune.

*Model prikazuje **podjelu prava i odgovornosti po nivoima sigurnosti,** gdje se viši slojevi štite strožim kontrolama pristupa, a niži slojevi imaju više fleksibilnosti ali manje privilegija.*



Za zaštitu od ransomwarea i jačanje cyber otpornosti, uz **Endpoint** i **Identity Management**, savjetujemo implementaciju **BaaS** i **DRaaS** strategija zaštite podataka.

security@qss.ba

Data Protection

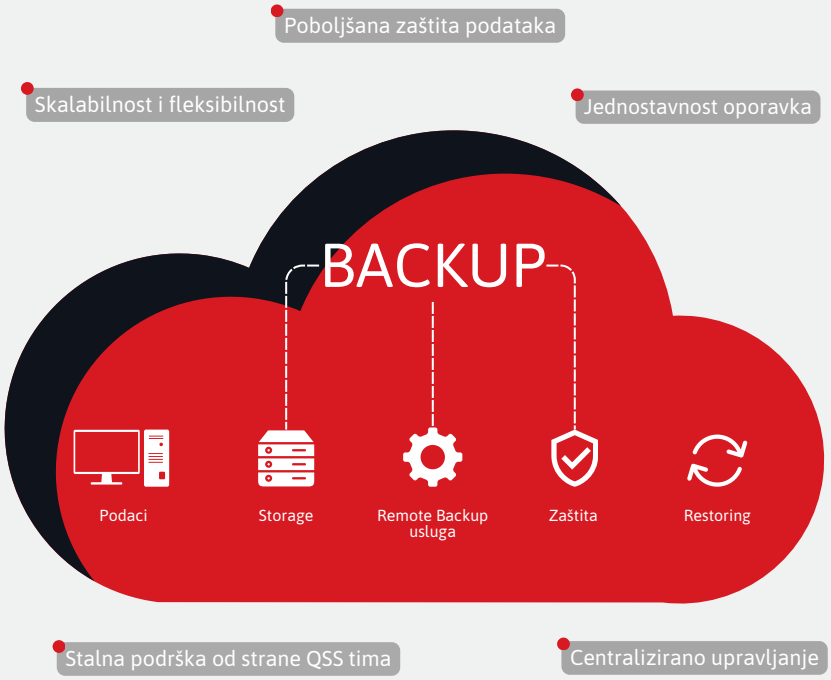
Zašto **Backup kao usluga** (BaaS)?

Poboljšajte sigurnost i dostupnost vaših podataka

Backup as a Service (BaaS) u QSS Data Centru omogućava **automatizirano kopiranje** podataka, eliminirajući potrebu za ručnim backupom koji je često nepouzdan i spor.

Zaštite vrijedne korporativne **podatke** i **osigurajte neprekidnu dostupnost** pouzdanih arhiva, ključnih za kontinuitet poslovanja.

Uštedite vrijeme i resurse uz poboljšanu zaštitu podataka, koristeći redovne analize temeljene na umjetnoj inteligenciji. Dodatno, BaaS uvodi **air gap** među vašim lokalnim podacima i backup-ovima u oblaku, čime se efikasno **štiti od ransomware napada** i **osigurava siguran i pouzdan oporavak**.



Zašto **Disaster Recovery as a Service** (DRaaS) ?

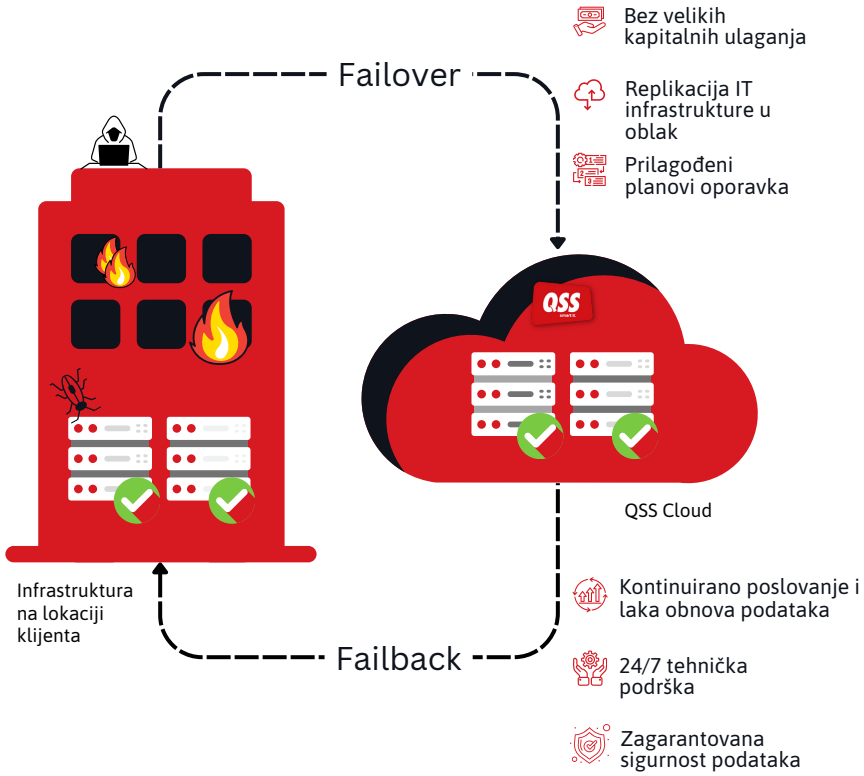
Oporavak od katastrofe i kontinuitet poslovanja

Disaster Recovery-as-a-Service (DRaaS) nudi **replikaciju IT infrastrukture u Cloud**, smanjujući rizik od gubitka podataka. Ovu uslugu plaćate mjesečno što je dodatan benefit jer nema kapitalnih ulaganja.

Održivost poslovanja ovisi o **kontinuiranoj** ponudi rješenja i usluga vašim klijentima. Međutim, ometajući događaj poput **prirodnih katastrofa** ili **cyber napada** može zaustaviti vaše poslovanje. Odabirom DRaaS osigurat ćete da bez smetnji nastavite pružati usluge klijentima.

Upotrebom **strategije air gap** između vaše produkcijske infrastrukture i DR okruženja u oblaku, DRaaS sprečava da **ransomware** kompromituje vaše **replikovane podatke**, čime osigurava brz i efikasan oporavak.

Korištenje DRaaS-a eliminira potrebu i za ulaganjem u vlastitu infrastrukturu za obnovu nakon katastrofe što dovodi do **smanjenja troškova** i **pojednostavljenja IT infrastrukture**.



Za potpunu **zaštitu**, **efikasnost** i **inovativnost** poslovanja snažno **preporučujemo kombinovanje** Disaster Recovery as a Service s Backup-as-a-Service rješenjem!

security@qss.ba