ZERO TRUST 및 N²SF 대응 보안 솔루션

Future Systems

WeGuardia™ ITU Z-Series

ITUz는 인가된 사용자의 내부망 접속을 안전하게 제어하는 **제로트러스트 기반 SDP 솔루션**으로
DNS 기반 통신(실제 서버 정보 숨김)과 애플리케이션 단위 접근제어, 서버간 횡적 이동 제어,
C/S/O 서버 별 정책 경고 기능 등을 통해 운영자의 안전한 설정을 돕습니다.

ZTNA 보안의 패러다임

기존 **경계형 시큐리티**와 **제로트러스트 시큐리티**가 합쳐진 제품으로
외부로부터의 공격, 신뢰할 수 있는 것 만이 존재하게 하였다면,
외부/내부 구별없이 의심하여 다양한 공격 위협으로부터 원천 차단합니다.



제품 이미지

WeGuardia™ ITUz-series

경계형 시큐리티 (Perimeter Security)

'경계형 시큐리티'는 네트워크 경계선을 기준으로 내부와 외부를
구분해, 외부 공격과 내부 정보 유출을 막기 위한 개념입니다.
내부는 '신뢰할 수 있는 영역', 외부는 '신뢰할 수 없는 영역'
으로 나누어 접근을 통제합니다.

따라서 **방어의 초점은 네트워크 전체**에 맞춰져 있습니다.



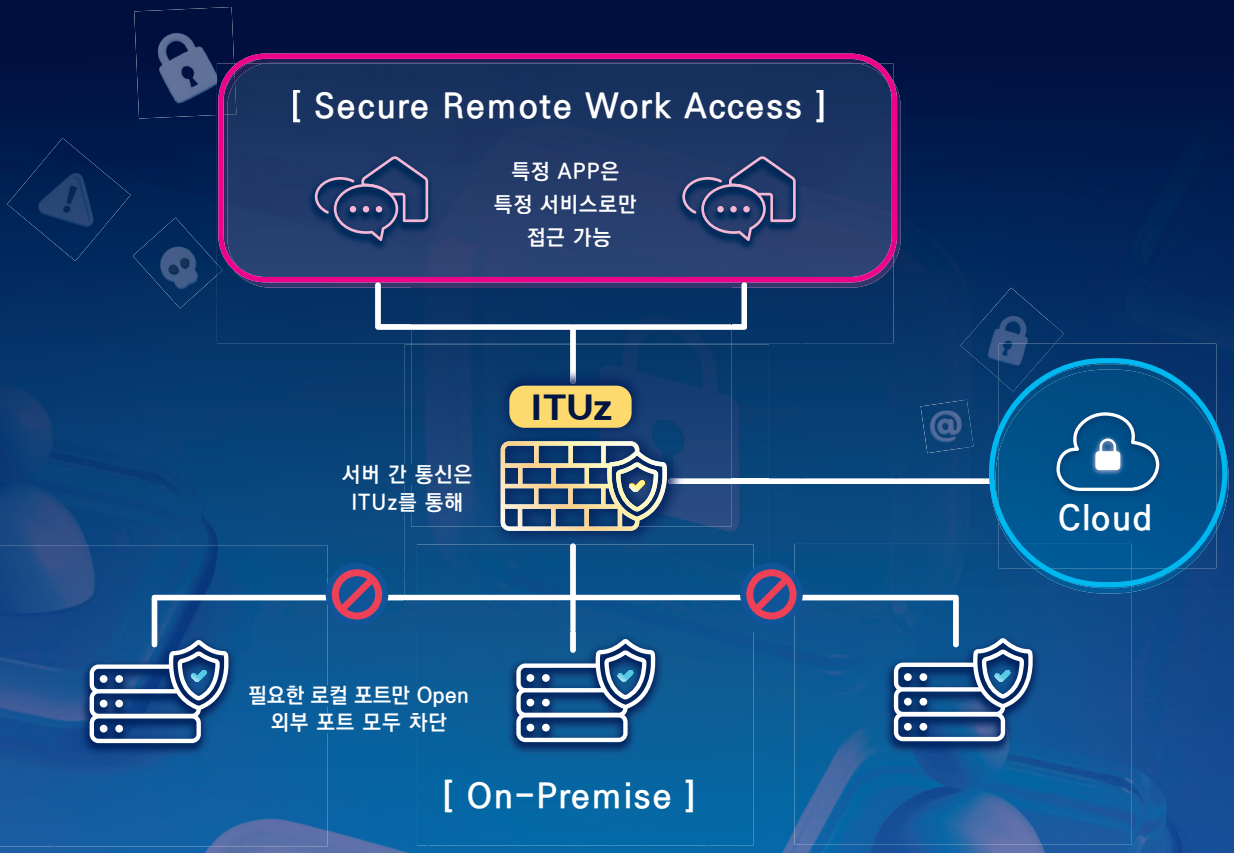
제로트러스트 시큐리티 (Zero Trust Security)

'제로트러스트 시큐리티'는 어떤 것도 신뢰하지 않고,
서비스 단위로만 안전하게 연결을 허용하는 보안 모델입니다.

ITUz는 **모든 접속을 암호화된 터널로 보호하고 승인된
사용자만 자원에 접근 가능**하도록 설계되어 있습니다.

이는 기업 내부망을 외부 공격자에게 완전히 감추는 것이며,
서버 간 이동까지 제어해 침투 확산을 원천 차단합니다.

[ZTNA 방화벽 구성도]



ZTNA 방화벽 주요기능



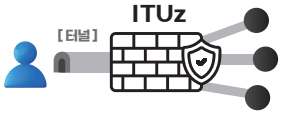
DNS 기반 통신 (접속 경로 추상화)

접속은 DNS 정보로만 이루어지며,
사용자 측에서 실제 서버 IP/포트는 알 수 없음
이를 통해 공격 표면을 크게 줄임



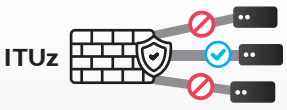
애플리케이션별·서비스별 접근 제어
(마이크로 세그멘테이션)

특정 앱/서비스에 대해서만 접근을 허용하는 정책을
적용할 수 있어, 불필요한 권한 노출 원천 차단



터널링을 통한 세분화된 연결 (중계 터널링)

클라이언트와 내부 서비스 간의 트래픽은
ITUz 터널을 통해 전달되어 세션·경로 제어가 용이



서버 간 횡적 이동 제어

내부 서버들 간의 통신도 ITUz 정책으로
제어 가능해 침투 시 횡적 확산을 사전에 차단



C/S/O 등급 기반 정책 경고

Classified/Sensitive/Open 등급 분류에 따라
서버 간 정책 충돌·위험을 자동으로 감지해
운영자에게 경고를 제공, 안전한 정책 설정을 도움



NAC

IP와 MAC 기반으로 단말을 관리하며,
필수 프로그램 설치 여부를 확인해
안전한 네트워크 접속을 보장

Future Systems

서울특별시 구로구 디지털로 26길 61 (에이스하이엔드타워 2차), 1902호
070-8853-6327 02-837-2986 www.future.co.kr
영업문의 business@future.co.kr(사업본부)