CYPRESSCOM

GIẢI PHÁP BẢO MẬT
THIẾT BỊ VÀ HỆ THỐNG VEDA





CYPRESSCOM

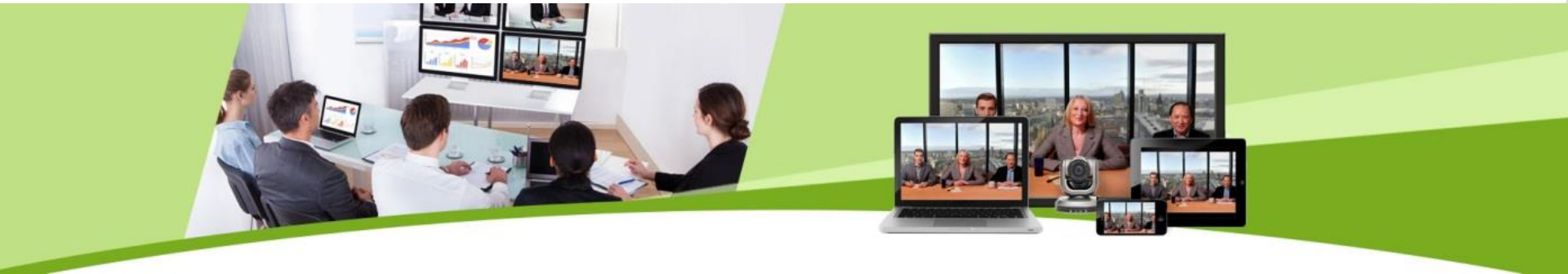
NỘI DUNG

1. BẢO MẬT THIẾT BỊ
2. BẢO MẬT DỮ LIỆU
3. BẢO MẬT QUẢN TRỊ
4. BẢO MẬT HỆ THỐNG MẠNG HỘI NGHỊ

CYPRESSCOM

BẢO MẬT THIẾT BỊ

- Thiết bị vận hành chỉ mở các cổng phục vụ dịch vụ hội nghị truyền hình, đóng tất cả các cổng không liên quan
- Mật khẩu truy cập hệ thống, bảo mật mật khẩu AES 256 bit
- Mã hóa dữ liệu trên ổ flash trong hệ thống đầu cuối và MCU



BẢO MẬT DỮ LIỆU

- Dữ liệu lưu trữ trên ổ cứng được mã hóa, chỉ giải mã khi chạy thiết bị

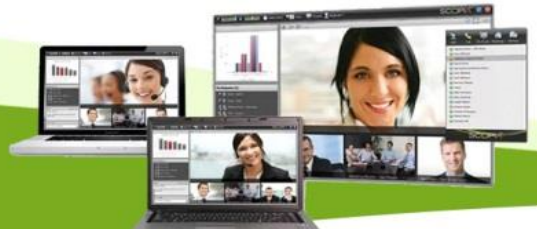
- Dữ liệu video/Audio/Content truyền trên mạng được mã hóa chuẩn Flowfish hoặc AES 256 bit

- Hỗ trợ giao thức bảo mật ITU-T H.235 trong trao đổi mã khóa trong cuộc gọi

CYPRESSCOM

BẢO MẬT QUẢN TRỊ

- Bảo mật bằng giao thức HTTPS khi truy cập hệ thống MCU và đầu cuối vận hành
- Mật khẩu truy cập, bảo mật mật khẩu AES 256
- Chống tấn công quét mật khẩu bằng phép thử: Mật khẩu sai tăng thời gian được phép truy cập đăng nhập
- Phân quyền trong điều hành: Nhiều cấp độ được truy cập các quyền quản trị hệ thống



CYPRESSCOM

BẢO MẬT HỆ THỐNG MẠNG

- Các thiết bị trong mạng không kết nối trực tiếp mà khởi tạo hệ thống mạng VPN riêng khi thiết lập cuộc gọi
- Không cho phép thiết bị bên ngoài mạng VPN truy cập vào mạng lưới
- Các thiết bị trong hệ thống được cấp Certificate riêng để truy cập qua mạng
- Các giao thức kết nối hỗ trợ TLS, mã hóa AES 256 bit

Thank You !