Emerging Security Strategies

Part Three: Taking a proactive approach to security

Tuesday September 28th, 2021 | 11am PST

cisco Meraki

George Bentinck
Director of Product Management

openpath

James Segil
President and Co-Founder

PlaceOS

Cam Reeves
Senior Developer

Overview

As threats evolve and business resiliency is a critical initiative for many, it is time to get proactive about a holistic physical and cyber security vision:

- The difference between proactive and reactive security
- Current state of security
- Top proactive security components and technology for your business
- How to use your centralized cloud-based security data for business intelligence and automation
- Considerations for maintaining a healthy and future-proof security infrastructure

Remember to drop any questions into the Q&A box throughout the discussion.

Reactive vs. Proactive Security

Reactive

- An attack happens, and your team responds or reacts, to the breach. The attack is discovered, the attacker repelled, the damage is assessed, and the clean-up begins.

- There is nothing inherently wrong with reactive security — this is part of the reason you've invested in security controls — but this cannot be your entire security culture.

Proactive

- When your culture is proactive, your team is committed to prevention rather than simply to responding to threats.

- This means investing in a strong defensive position, educating your employees about good security practices, and planning for risks your organization hasn't yet encountered

The Current State of Security

Example of Current Security Environment

Infrastructure

- On premises Windows server running in the basement of the building
- Credentials on post-it notes stuck to monitors
- Changes made via email to security team
- Outdated integration methods (XML-RPC, SOAP, etc.) or none at all

Protocols

- Security team receives a new user or CSV file with a list of users
- Manually creates users, assigns relevant access, generates card numbers
- Writes encoded card details to NFC cards by hand
- BMS receives request upon user's card read, verifies access and door/turnstyles/etc are unlocked

On Premises vs Cloud-Based Security

64 PERCENT OF COMPANIES NOW BELIEVE THE CLOUD IS MORE SECURE THAN LEGACY ON-PREMISES SYSTEMS.

- IBM, *"Cost of a Data Breach Report"*

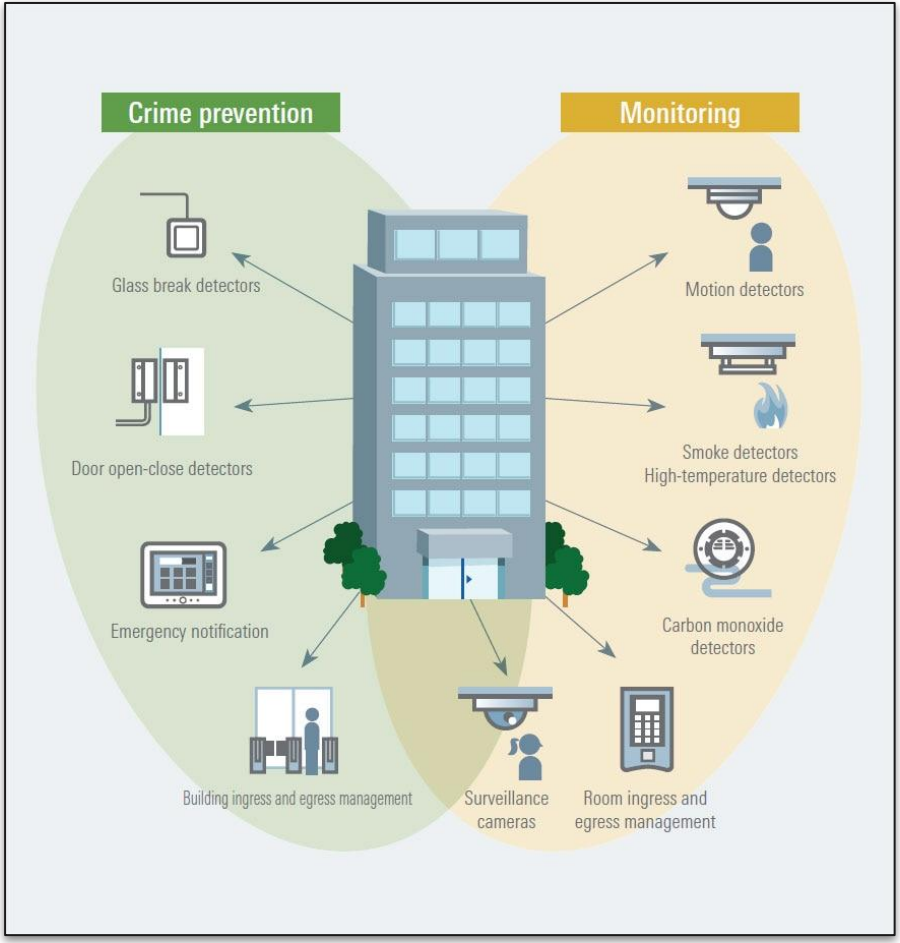
On Premises vs Cloud-Based Security

- Some businesses have an unfounded belief that on-premises security systems are safer than cloud-based solutions
- Physical location of the server provides a false sense of security
- In reality, it’s much like storing your money in a box under your bed vs in a bank
- Cloud based solutions allow proper delegation via multiple users with finer grained permissions compared to many on premises solutions
- No requirement to "roll your own security" for physical (and sometimes non-physical) access
- Security patches and updates are managed by the access control provider
- Cloud providers generally have around-the-clock support for security breaches or other issues which can be prohibitively expensive for a lot of businesses

Elevating Security via Integration and Automation

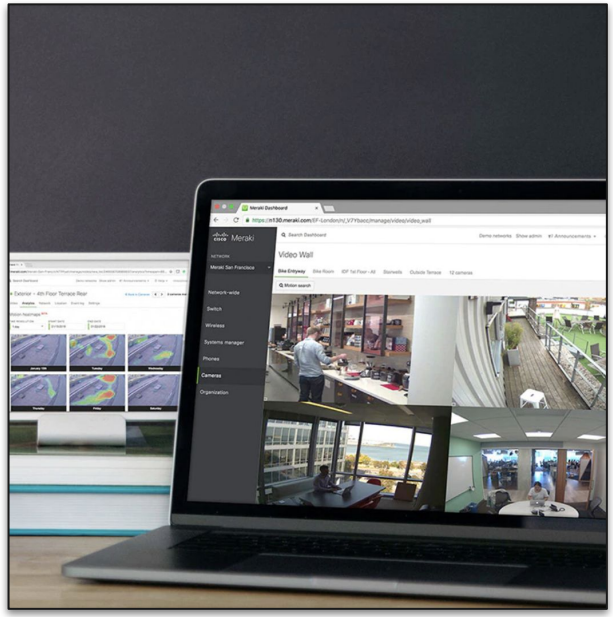
Top Proactive Security Technology for Your Business

- Access Control
- Smart Video Surveillance
- Visitor / Guest Management
- Identity Management
- Building / Office Management Systems
- Occupancy Management & People Tracking
- Smart Security Sensors



Unified Access Control & Video Security

Centralized Security Monitoring



Video Reader

Smart Video Surveillance

Unified Access Control & Video Security

- **Efficiency**
  With an integrated system, all operations can become streamlined. Surveillance and access control information can be viewed from a single interface at a workstation or even on your smartphone with a simple app.

- **Real-Time Monitoring & Entry / Exit Validation**
  You can view access control information on the same interface as the video, rather than linking events and reports later.

- **Data Collection & Centralization**
  A centralized system allows for more actionable data collection, as well as improved security measures.

- **Improved Safety**
  You can also have alarms or a PA linked through the same system as video surveillance. Tailgating can be addressed immediately.

Example 1: Automated Onboarding and Access Grants

- The environment:
  - Users already exist in Office 365
  - Group membership defines level of access control
  - Calendar events retrieved have an organiser, meeting time and location
- The flow: Fully automated user onboarding:
  - Add users to access control system via Graph API integration
  - Set building access based on user groups or job title field
  - Retrieve calendar events periodically and grant room access for the duration of each event

Example 2: Automated Lock Opening with Geolocation

- The environment:
  - Staff can be located via AP triangulation using Meraki
  - Locks (generally doors/entrances) using access control are mapped
- The flow: Fully automated door unlocking:
  - Distance between X,Y coordinates of the user and the room are calculated
  - If distance is within some threshold, check the access rights of the user
  - Assuming access is sufficient, open the lock for a specified period of time or until distance is greater than the previous threshold

Example 3: External Visitor Management

- The environment:
  - Calendar events can be retrieved from G Suite API
  - External event attendees can be identified by email
  - QR readers exist at the building entrance connected to turnstiles
- The flow: Visitor access without front of house interaction:
  - Grab all calendar events for the day and record any external attendees details
  - Create a new cardholder and card for the external user in the access control system
  - Grant access to the building for the day of the attendee's arrival
  - Encode the card in a QR code and email it to the external attendees
  - External attendees then scan their QR code and are granted access through the turnstiles

Planning & Maintaining Security

Top Considerations for a Future-Proof Security Strategy

1. 24/7 visibility of all your assets from anywhere
2. Smart technology that you can leverage to help automate alerts, discoveries, and tasks
3. Integrate and connect your security solutions
4. Ensure that your systems are adaptable, and can be easily updated to defend against evolving threats
5. Adopt comprehensive and consistent training methods
6. Implement and document response procedures to mitigate risk
7. Adopt Security-By-Design principles

Top Considerations for Planning Your Security Infrastructure

1. Identify the scope of your physical security plans. This should include the types of employees the policies apply to, and how records will be collected and documented.
2. Determine who is responsible for implementing your physical security plans, as well as the key decision-makers for making adjustments or changes to the plan.
3. Include the different physical security technology components your policy will cover.
4. State the types of physical security controls your policy will employ. Include any physical access control systems, permission levels, and types of credentials you plan on using.
5. List out key access points, and how you plan to keep them secure.
6. Define your monitoring and detection systems. What types of video surveillance, sensors, and alarms will your physical security policies include? Identify who will be responsible for monitoring the systems, and which processes will be automated.
7. Outline all incident response policies. Your physical security planning needs to address how your teams will respond to different threats and emergencies.
8. Scope out how to handle visitors, vendors, and contractors to ensure your physical security policies are not violated.
9. Create a cybersecurity policy for handling physical security technology data and records. Include your policies for encryption, vulnerability testing, hardware security, and employee training.
10. Address how physical security policies are communicated to the team, and who requires access to the plan.

Thank you for joining the series

Get more information and free resources to help with your security planning today

- https://meraki.cisco.com/webinars/
- https://www.openpath.com/physical-security-guide
- https://place.technology/podcast