# Wireless Transformation
# Security Analysis
# Student Safety

May 8, 2019

Patrick R. Turner, VP & CIO Schoolcraft College
Daniel Heidt, Thought Leader, Access Interactive, Inc.

Schoolcraft College

merit
NETWORK. SECURITY. COMMUNITY.

access interactive
IT solutions for business, education, and government

# Schoolcraft College

- Main campus is located in Livonia Michigan
  - Two satellite sites:
    - Radcliff Center in Garden City
    - Public Safety Training Center in Livonia
- 2 Year College
- 31,183 Traditional and Non-Traditional Enrollment
(Source: 2016-2017 Year End Program Enrollment Report and Non-Program Enrollment Report
- 1 Bachelor Degree Program, 44 Associate Degree Programs and 61 Certificates
- Ellucian® Colleague™ customer for over 34 years

Schoolcraft College

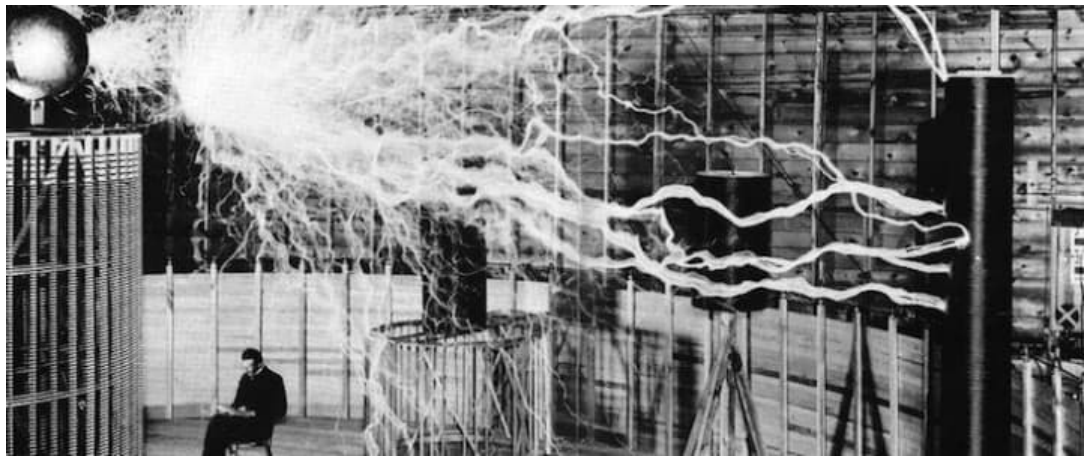
Schoolcraft College

# Access Interactive

- Access Interactive was founded in 1985 and has grown to over 65 employees worldwide with over $25 million in annual revenue.
- A local Michigan consulting company that uses technology to fix, accomplish, or avoid customer critical business initiatives.
- LOGOS
- As Solution Architects, Access Interactive strives to learn the customer's business domain to make the best recommendations with the strongest ROI metrics.

# Key Components of our Presentation

1. Transforming a Wireless Network with the new 802.11ax IEEE standard (the ac replacement)
2. Wireless Security and Vulnerability Testing
3. Capitalizing on Infrastructure Technology to Improve Student Safety on Campus.



Schoolcraft College

# The Problem Statement

- Schoolcraft College's faltering 10+ year old wireless network plagued with dead zones and insufficient capacity for 21st century customer demands.
- Wireless network footprint:15 buildings across 3 locations.

Schoolcraft College

accessinteractive
IT solutions for business, education, and government

# The Solution Process: Next Generation Wireless

1+ yrs. Competitive POC of Aerohive, Meraki, Myst. Aruba ruled out due to price. POC in Student Center and Sports Dome. Focus on ease of management and integration with security system.

# Wireless Network Requirements Traceability Matrix (a.k.a. R&V Plan)

| Date: | | Project Name: | Wireless Network Overhaul | | Project Number: | R&V Lead: | Jeff Borton |
|---|---|---|---|---|---|---|---|
| **ID** | **Date Received** | **Source** | **Type (e.g., Business, GUI, etc.** | **Requirement (Shall Statement)** | **Work Product/Use Case** | **Validation Method** | **Validation Date** | **Validated By Whom** |
| 1 | 6/16/2017 | JT/JCB | Connectivity | The network shall be a Layer 3 network separated per building. Outside can be treated as one Layer 3 Network. | AI will create one to two L3 wireless networks | AI will demonstrate application connectivity via wireless on an SC issued laptop using SC credentials using L3 | | |
| 2 | 12/11/2017 | PRT | Architecture | The Wireless Network AP's used shall use, and be based on, a Cloud Controller architecture. | Aerohive HiveManager NG is a cloud based controller. | Connection validation to HiveManager NG offsite | | |
| 3 | 12/11/2017 | PRT | Acceptance | This R&V Plan (Requirements Traceability Matrix) shall be singularly controlling regarding the acceptance and completion of this Project. | AI acknowledges and agrees to adhere to the R&V Plan and validation | AI will pass 100% of use cases | | |
| 4 | 6/16/2017 | JT/JCB | Connectivity | The Wireless network shall allow for continuous connectivity when walking from building to building. | Locations with the proper amount of outdoor AP coverage will seamlessly maintain user connections between AP's | Demonstrate a client device maintaining connection during handoff from one AP to another via ping from laptop and through HiveManager GUI | | |
| 5 | 6/16/2017 | SC/TD | Connectivity | The wireless network shall allow for uninterrupted wireless connectivity via Layer 3 roaming across APs | The solution will be configured for L3 roaming between AP's where proper coverage is provided. | Demonstrate a client device maintaining connection during handoff from one AP to another via ping from laptop and through HiveManager GUI | | |
| 7 | 11/18/2017 | PT/JCB | Survey | The wireless network design (model, configuration, number, and placement of AP's) shall be based on the results of a campus wide wireless survey using **signal strength** | Site survey will be performed using signal strength (as one criteria) to assist with wireless network design | Survey documentation will define signal strength and define AP starting placement | | |

# Proof Of Concept Details


- Hardware Tested
  - Aerohive AP650 802.11ac
  - Meraki
  - Myst
- Test Location: Schoolcraft Student Center & Sports Dome
- Evaluation Criteria: From R&V Plan.
- Selection based on Eval. Criteria, Ease of Use, Ease of Configuration, Ease of System Management Etc.

Aerohive

DELL

# Selection Criteria/ Rationale

Why the Selection of Aerohive was made:

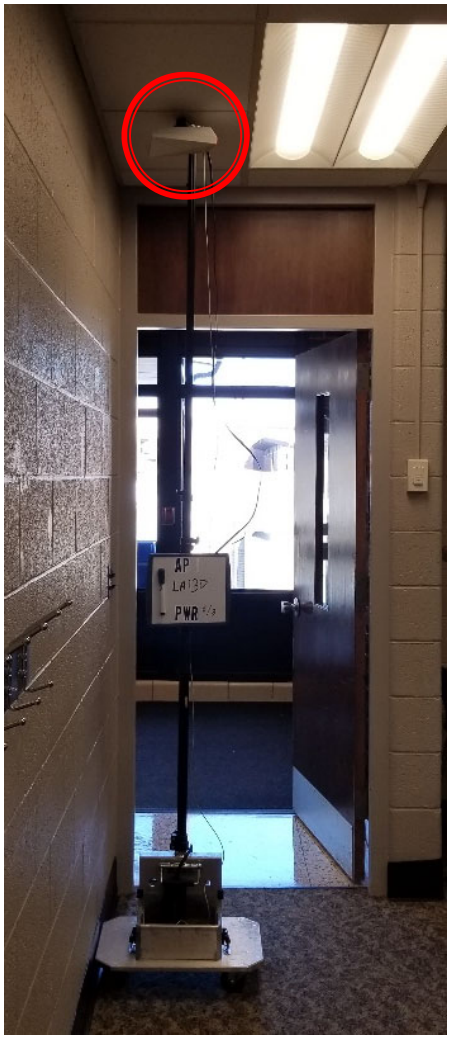
Notes,: Both Aerohive and Cisco provided a vendor to assist us in learning their respective technologies, which assisted in the decision making process, in addition we also took into account our technician's ability to learn the product on their own.

1. Aerohive was a much easier product to learn, required much less interaction with vendor for SC techs to understand the product.
2. Aerohive management page is similar to the pages we use to manage our current network. Not only can we monitor the type of traffic but can easily navigate to the exact device and its location on campus. This is useful for both security and monitoring of network usage. The Meraki management page is not as user friendly. You can access user information but you have to know exactly what you are looking for and where to go look.
3. Aerohive has a superior console for both feature troubleshooting and managing SSIDs for the technicians. Meraki requires tags to manage the SSIDs, which is not as simplistic. Aerohive can easily add a new SSID per AP as compared to Meraki.
4. Details in the Aerohive heat maps are superior to that of Meraki, which had limited information on the range and strength, as compared during the proof of concept (POC). In addition, adding the campus maps was much more simplistic and easily configurable in the Aerohive interface.
5. The Aerohive dashboard was more feature rich from our usage as compared to that of Meraki.
6. In our testing, when available, 95% of the users used social media to log in. Social media is an option as a part of the Aerohive solution. Aerohive allows for Facebook, Linkedin, Google, and Twitter logs in. Meraki can be configured to use a local Facebook page but will require a 3rd party vendor for more platforms. Both of Aerohive and Meraki are using 3rd parties for social media but Aerohive includes it where Meraki will require a separate agreement.
7. Aerohive has nice built in Client ID manager. It shows the type of client and retains information for monitoring. It also gives you the option to set up certain clients or locations for monitoring.
8. Range on APs appears to be better on Aerohive but this is not necessarily an apple to apples comparison, but worth mentioning.
9. Had some difficulties with the ISE wireless portal, which has been hard to work on do to hardwire ISE also being in place, so separation of ISE from WIFI is desired. Aerohive has its own network access control, where the portal page is built in directly to the Aerohive management page and is enforced at the AP itself. With Meraki you are using ISE so the page is managed in the Cisco ISE page and relies on conditions to display it.
10. Meraki requires more work to move Aps around (Nature of ISE as we use it).
11. Meraki has delays in reporting connections and showing changes in the cloud environment, Aerohive is very responsive.
12. Aerohive will continue to function even if your license expires. Meraki APs stop working the moment the license expires. Not that we intend on running in an expired state, however human failure on this would result in an outage condition with Meraki that would not be a factor in Aerohive.

# Wireless Survey Process

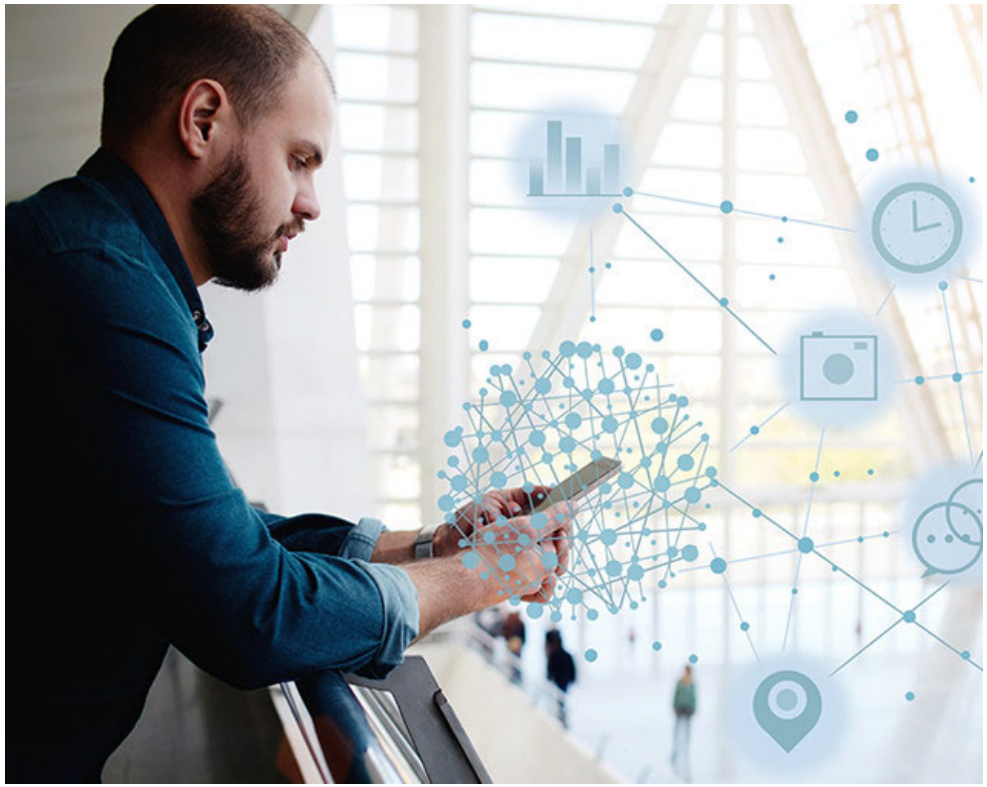
- Air Magnet SurveyPro™
- Design & Deploy Wireless LANs For Optimal Performance, Security & Compliance
- Collect real-world data by performing unique true end-user experience (wireless LAN throughput, data rates, retries, losses) measurements

NETSCOUT®



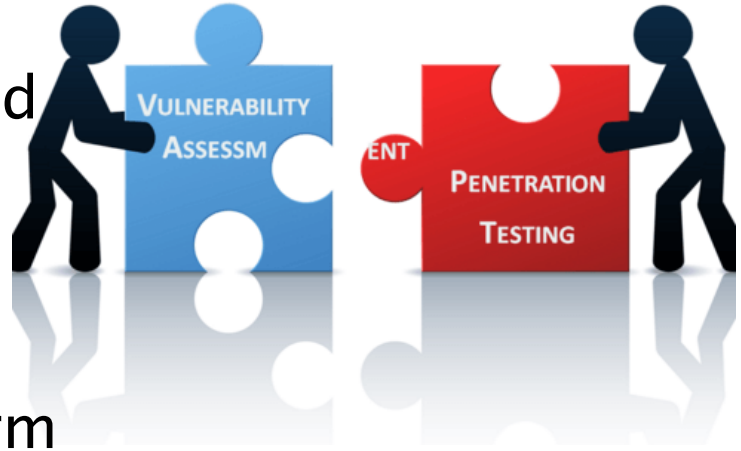
# Deployment Process

- Building-by-building phased approach
- Leveraging existing switching infrastructure
- Aerohive™ uses push deployment
- Schoolcraft Facilities partnered with wiring vendor to pull cabling and mount APs.
- Aerohive™ has it own heat map calculation with tuning and optimization.



# Security and Vulnerability Testing

- Goal is to dramatically increased speed and coverage requiring security due diligence.
- In addition to our stringent security practices we have invested in wireless and application pen testing to close any vulnerabilities to protect the increases capacity / coverage.
- Will leverage Access Interactive as a 3rd party independent penetration testing firm to allow us to validate and to comply with recent audit requirements.



# High Level Security Penetration Approach

| Scope, Plan and Pre-requisites | | |
|---|---|---|
| **Foot Printing & Reconnaissance** | | |
| Active Reconnaissance from User LAN | Open Ports, Vulnerability Scanning, Out od Date Patches, Default Credentials | Understand network segmentation |
| **Network Exploration** | | |
| Subnet, VLAN, Server Zone Identification | Network Segmentation Checks & Exploitation | Identify Attack Vectors |
| **Penetration Testing** | | |
| Exploit known vulnerability & misconfigurations | Privilege Escalation | Target Domain Admin Account |
| **Reporting** | | |
| Attack Foothold | Executive Summary | Finding, Risk & Recommendations |

# Security Testing Process

- Access Interactive will utilize tools and tactics to exploit vulnerabilities in the Schoolcraft College infrastructure.
- Schoolcrafts challenge is great due to several key investments like Cisco® ISE, Checkpoint® IPS, ForcePoint™ DLP, Trend Micro® Deep Security & Deep Discovery, Qualsys Vulnerability testing, AI will attempt access and control of the system.
- With this knowledge we will collaborate with AI to increase our security posture to close vulnerabilities and secure our school and student population.

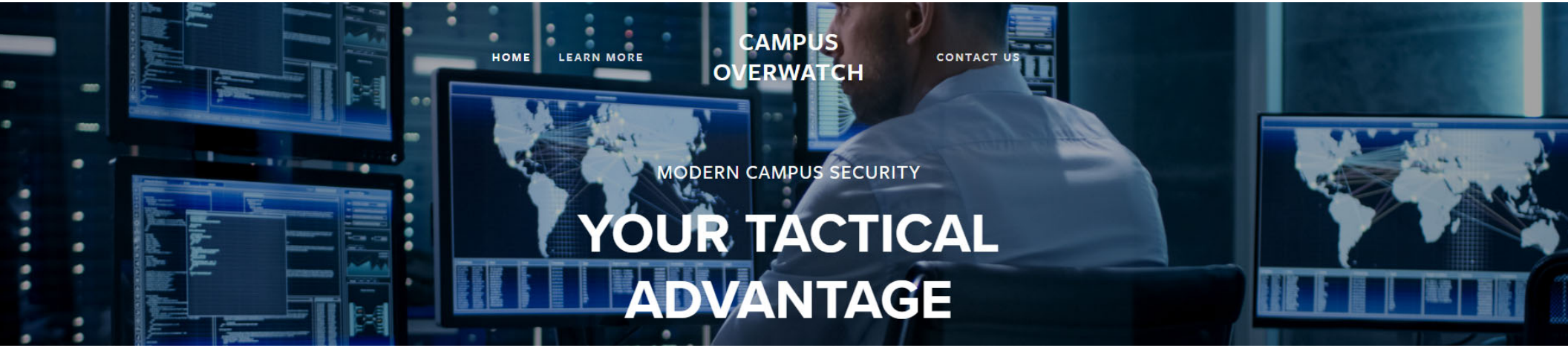
# Protecting Key Areas of Compliance

- PII
- FERPA
- HIPAA
- PCI
- GDPR
- IRS Pub 1075
- Title IX
- CJIS
- Gramm-Leach-Bliley Act (GLB Act)

# Next Generation Wireless Networking Enables Technology Advances

Wayfinding, Location Based Services, e.g. Marketing, Emergence of Fusion Centers, Cross Domain Data Sharing, Unstructured/Structured Data Analytics

# Advanced Wireless Inspired Student Safety




Technology for Campus Police Departments to identify Persons of Interest and Witnesses.

# History of the Cleary Act

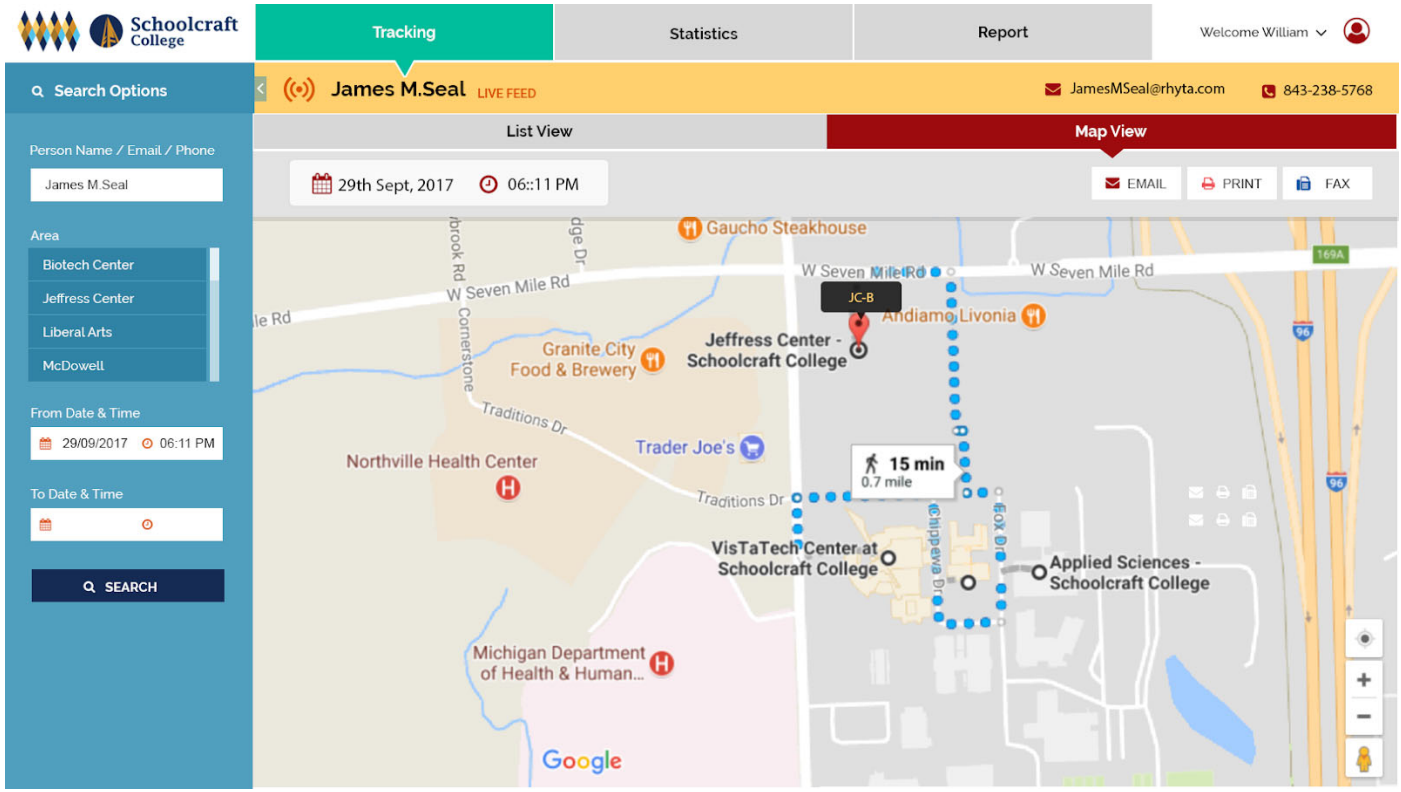
- The need for such public participation became very real in the aftermath of the unreported 1986 murder of Jeanne Cleary, a student at Lehigh University

- Cleary Act – the passage of the Student Right-to-Know and Campus Security Act of 1990. The Act mandates regular crime reporting for colleges participating in federal student loan programs as amended by the Higher Education Amendments Act of 1998.

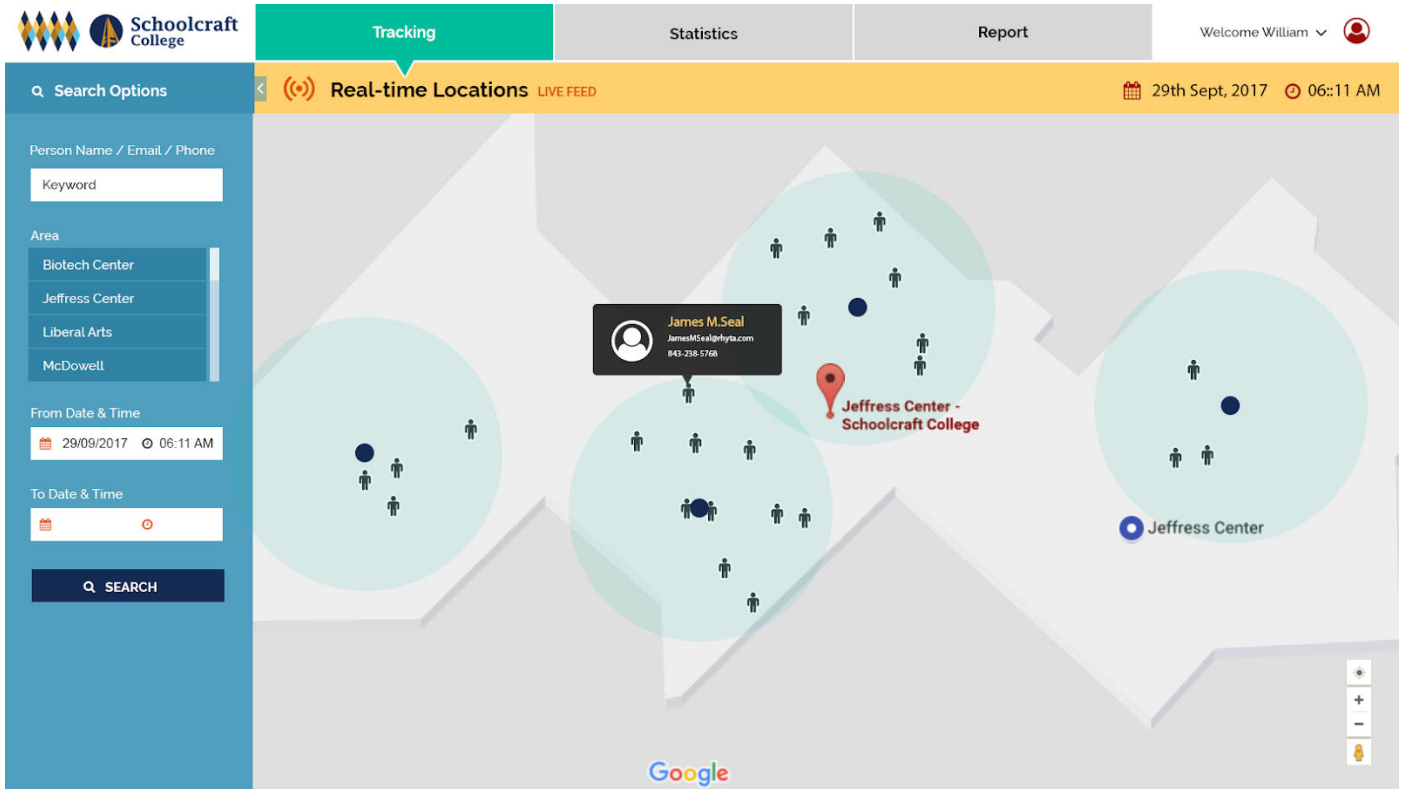
# Problem Statement

- Police investigation methods include incident area canvassing, security camera review, database searching, but suspect identification can still remain a challenge.
- Supplementing police investigation by improving the timeliness, accuracy, and success in identifying those who are in proximity to a suspected incident will improve safety.

# The Solution = Campus Overwatch™



# Tactical Visibility (Individual)



# Student Safety Evolution

- This is just the beginning…
- To be part of the Student Safety Evolution contact us to learn more about Campus Overwatch™

Thank you, Pat & Daniel

Schoolcraft College

accessinteractive
IT solutions for business, education, and government

# Thank you for your kind attention!
# Questions…?