BITSIGHT *Insights*

Powerhouses and Benchwarmers:

Assessing the Cyber Security Performance of Collegiate Athletic Conferences

BitSight Technologies

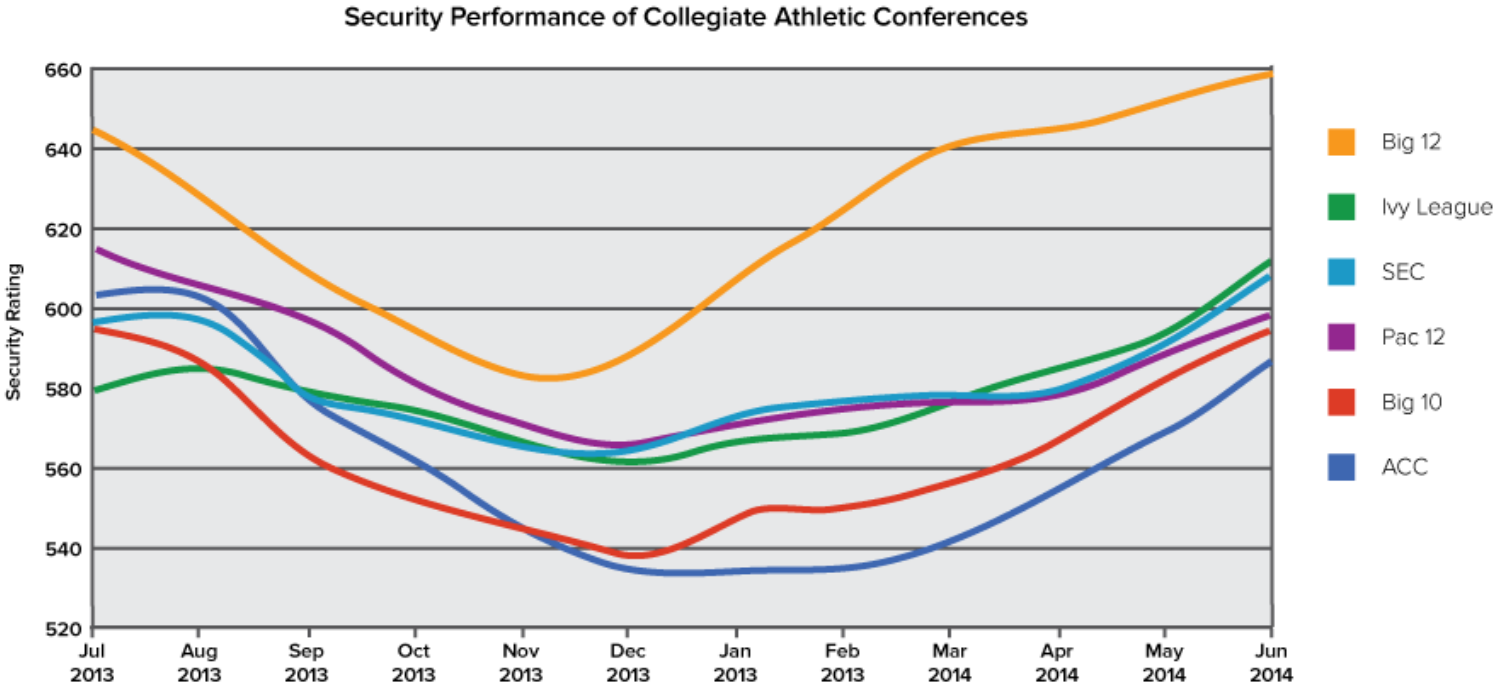
August 2014

BITSIGHT *Insights*

Assessing the Cyber Security Performance of Collegiate Athletic Conferences

It's back to school season for colleges and universities. As students trickle back to campus, schools are preparing for another year of teaching, research, and of course, college sports. No one would deny that American colleges are a treasure trove of knowledge and a bastion of the nation's athletic prowess; yet few know that these institutions are also a gold mine of information, from faculty and student Social Security numbers to football fans' credit card information and sensitive intellectual property. This valuable data, an open network attack surface and Bring Your Own Device (BYOD) culture makes higher education institutions a prime target for cyber attackers.

To assess the cyber security performance of American higher education institutions (and in anticipation of the coming college football season), we have focused on the most recognized collegiate athletic conferences: the SEC, ACC, Pac-12, Big 10, Big 12 and Ivy League. The schools in these conferences are large to medium-sized universities, representing a total student population of more than 2.25 million and a network footprint of more than 11 million IP addresses. Conference ratings are calculated using a simple average of the Security Ratings of member schools.



BitSight Technologies uses external data to rate organizations' security performance. Using terabytes of data on observed security events and configuration status, our daily Security Ratings provide a unique view on security risk, all from the outside. Security Ratings range from 250 to 900, with higher ratings equating better security performance. The period of analysis for this report was from July 2013 through June 2014.

Key Findings

BitSight Technologies' latest analysis of Security Ratings in higher education reveals poor performance in the sector. Some of our main findings:

1

Colleges at the Bottom of the Draft

Colleges and universities are failing to adequately address security challenges, with the Security Ratings of athletic conferences averaging around 600. This is considerably below retail and healthcare, two other industries that have faced serious data breaches in the past year.

2

Blitzed by Malware

Higher education institutions experience high levels of malware infections, the most prevalent infection coming from the Flashback malware, which targets Apple computers. Other prominent malware include Adware and Conficker.

3

Homecoming Challenges

Overall security performance declines significantly during the academic school year (September to May). The conferences see an overall 30 point drop in Security Ratings. This is likely due to the influx of students and devices on campus networks.

4

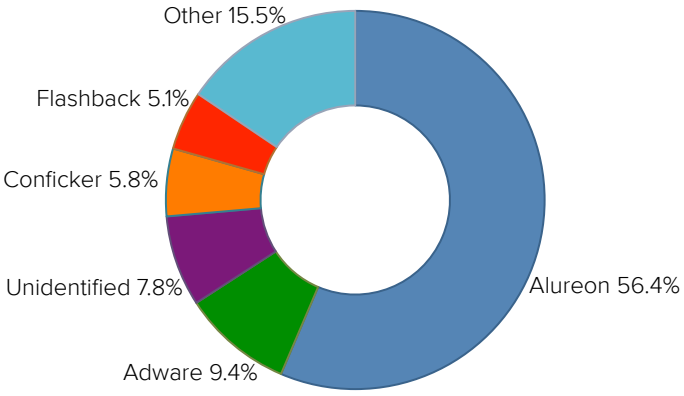
Powerhouses have a Playbook

The schools included in our analysis with a Security Rating of 700 or above all have a dedicated CISO or Director of Information Security on staff. Such prioritization of information security is a key indicator of better security performance.

The Cyber Security Standings

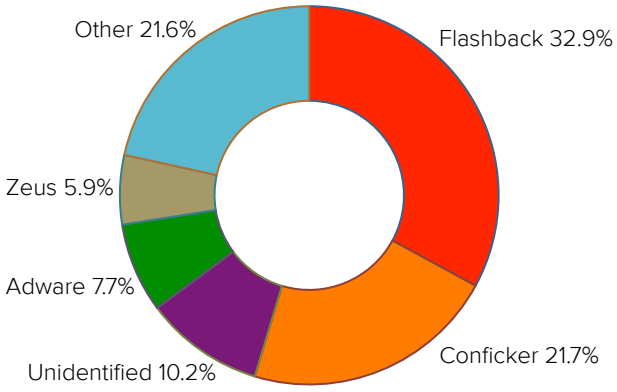
Main Findings:

- The Big Twelve ended the year with the highest Security Rating at 661.
- Alureon, a rootkit that can steal information from an infected device, was the most prominent malware, largely due to a specific and large infection at one member school. It made up more than 56% of observed infections.
- Between September and May, Security Ratings for Big 12 Schools declined 33 points.



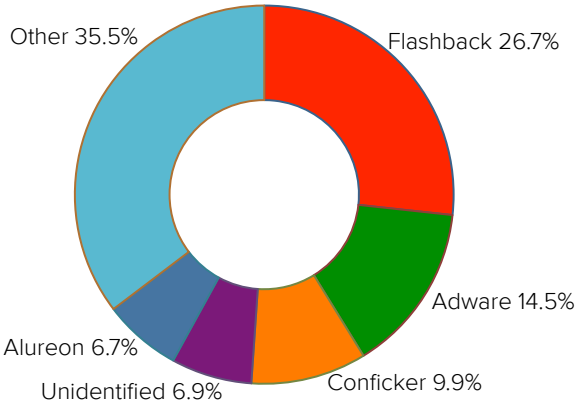
Main Findings:

- The Ivy League ended the year with a 614 rating.
- Flashback takes up a whopping 32.9% of infections observed on the networks of the famed schools of the Ivy League.
- Among the conferences, schools in the Ivy League saw the least change in Security Ratings during the course of the school year, dropping only 20 points.



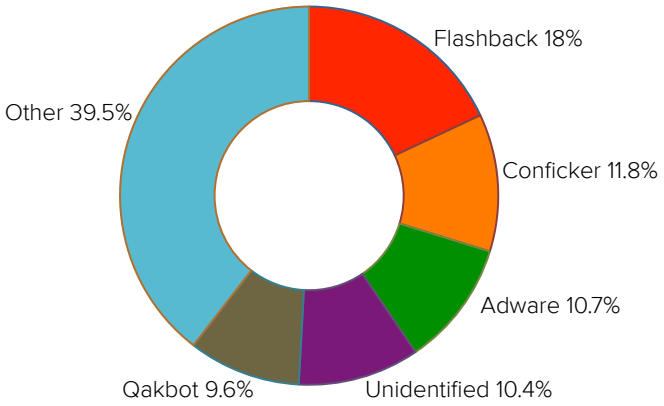
Main Findings:

- The SEC ended the year with a 610 aggregate Security Rating.
- Suggesting the popularity of Macs amongst students, Flashback was the most observed malware in the past year, making up 26.7% of observed infections.
- Security Ratings declined 28 points while students were on campus.



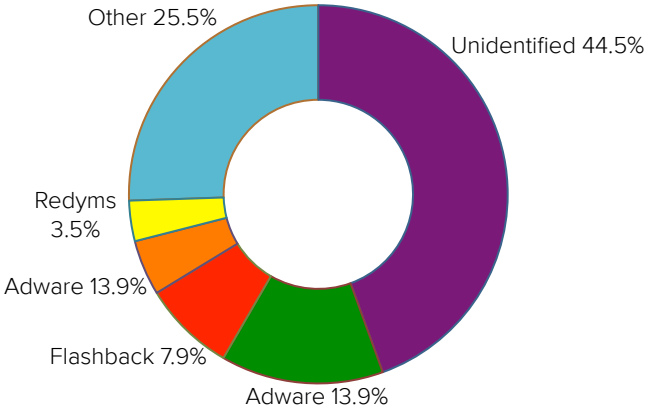
Main Findings:

- The Pac 12 schools ended the year with an average Security Rating of 600.
- Like the SEC, the most commonly observed malware was Flashback, at 18% of infections.
- The conference Security Rating dropped an average of 30 points during the academic school year.



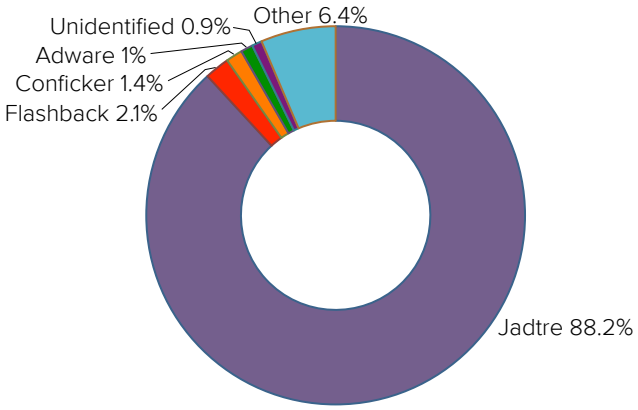
Main Findings:

- The Big Ten finished the year with a Security Rating of 596.
- While the majority of infections observed in Big 10 networks are classified as “unidentified”, Adware made up the highest volume of identifiable infections at 13.9%.
- The Conference Security Rating dropped 40 points during the school months.



Main Findings:

- The ACC ended the year with the lowest aggregate Security Rating at 588.
- An enormous infection of Jadtre, a trojan, at one school skewed the conference’s malware distribution, accounting for 88.2% of activity observed by BitSight.
- There was a 50 point drop in Security Ratings during the school year.



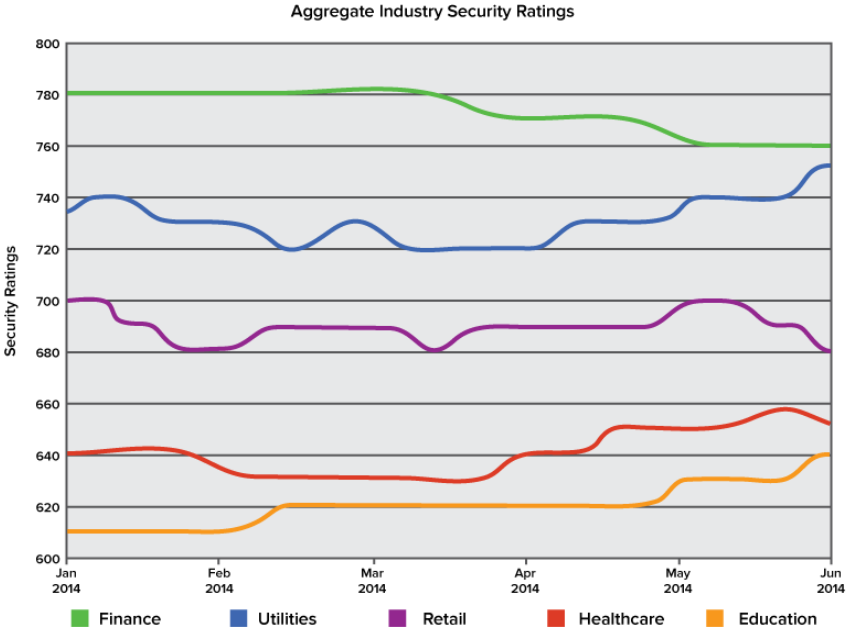
Malware Definitions

Other: All other infections that we have seen on the network of the rated conference.

Unidentified: Behavior indicative of a malware infection has been observed, although we cannot identify the exact infection. This can occur for a number of reasons, such as when behaviors common to many different types of malware are observed or when a piece of malware has not yet been named.

Powerhouses and Benchwarmers in Higher Education Security Performance

The aggregate Security Ratings of these institutions reveal a lot of weaknesses on the cyber security playing field. In comparison to the industries we analyzed in our last BitSight Insights industry report, these schools (and higher education in general) fall significantly behind in cyber security performance. The overall Security Rating of the education sector is lower than even retail and healthcare -- two industries that have struggled with protecting credit, personal and patient information. So why are higher education institutions failing to secure their networks from frequent security events?



One of the primary reasons arises from the clear differences between the information technology infrastructure in a corporate and university setting. University cyber security is a complex game that involves juggling a high volume of open network access points, diverse technology needs, multiple compliance and regulatory measures and the protection of high value information, such as student and faculty data or even sensitive intellectual property. It is no wonder that these organizations often drop the ball. Whereas businesses often have dedicated security teams that can work in conjunction with IT groups to create manageable network access points and maintain certain restrictions, security teams at schools are often left playing catch up. With thousands of users connecting on multiple devices, universities have limited control over student activities online. In our BitSight analysis, this became apparent by looking at the security performance of these universities during the school year versus the summer months. From September through May, the months when the majority of students are connected to

Are colleges getting sacked by compliance requirements?

Colleges and Universities face a daunting number of compliance regulations. In addition to filling stadium seats, many schools have on-campus healthcare systems, restaurants, book stores, conference centers, research labs and more - meaning their networks house much more than just student records. Because of this, Education has become a nexus for diverse data, and multiple consumer cyber protection regulations are applicable. Below is a list of the regulations impacting cyber security in higher education:

- PCI-DSS (The Payment Card Industry Data Security Standards)
- HIPAA (The Health Insurance Portability and Accountability Act)
- GLBA (Gramm-Leach-Bliley Act)
- FERPA (Family Education Rights and Privacy Act)
- Red Flags Rule
- FISMA (The Federal Information Security Management Act)

As our ratings data suggests, being compliant does not necessarily mean you are secure. Meeting compliance standards is an on-going effort for schools, and with limited funds and resources, it's sad to see that regulatory efforts are not driving better security performance for these colleges and universities. In many cases, both security and compliance can be achieved with continuous monitoring technologies, that can help alert teams to malicious activity on networks before damage is caused.

Blitzed by Flashback

Flashback was the most prevalent malware observed by BitSight in the conferences over the past year. Out of the six conferences we analyzed, this malware was the most prevalent in three of them. Flashback is a malware that began infecting Apple computers through a Java vulnerability. This malware can run malicious code on a device, although Apple has tried to mitigate its effects by buying the Command and Control domains propagating the infection. In our previous analysis of different industries, from retail to finance, we have never encountered such a high number of Flashback events. So why are universities feeling the brunt of these attacks?

The answer may lie in the devices present in corporate and educational settings. Forrester recently forecasted that Apple only captures a mere 8% of the corporate computer and tablet market.[4] On the other hand, Mac computers are ubiquitous on college campuses. According to a 2010 study by research firm Student Monitor, Apple computers account for 27% of personal computers on campus, which are constantly connecting to the school networks. The study also noted that of students who anticipated making a computer purchase, 47% were planning to buy an Apple computer.[5] Another possible explanation is that students are failing to apply important security updates, such as the XProtect patch to defend against Flashback. While businesses are known to apply strict protocols on updating company software, universities often have little control over the actions of college students who bring their own devices to campus.

campus networks, we observed an average 30-point drop in the overall security ratings of the athletic conferences.

Higher education's network security problems aren't just apparent in our data; they have become front-page news over the past year. Despite meeting diverse compliance regulations, universities are failing to take some basic steps to prevent major data breaches that expose the personal information of students, alumni and staff. A recent Educause report noted that Privacy Rights Clearinghouse recorded 551 breach reports from colleges and universities from 2005 to 2013, which amounts to roughly a breach per week.[1] In 2014 alone there have been multiple high profile breaches leading to massive amounts of records being exposed through cyber attacks. Some recent examples include The University of Maryland (309,079 records), Indiana University (146,000 records) and the University of Delaware (74,000 records). To put this into financial perspective, the 2014 Ponemon Cost of a Data Breach report put the financial cost in the wake of a data breach at a whopping $237 per record for Education.[2] This per record cost is second only to financial institutions, which hold valuable credit information. As higher education institutions focus on cutting costs to increase affordability, these incidents end up being a major financial and reputational blow to the nation's colleges and universities.

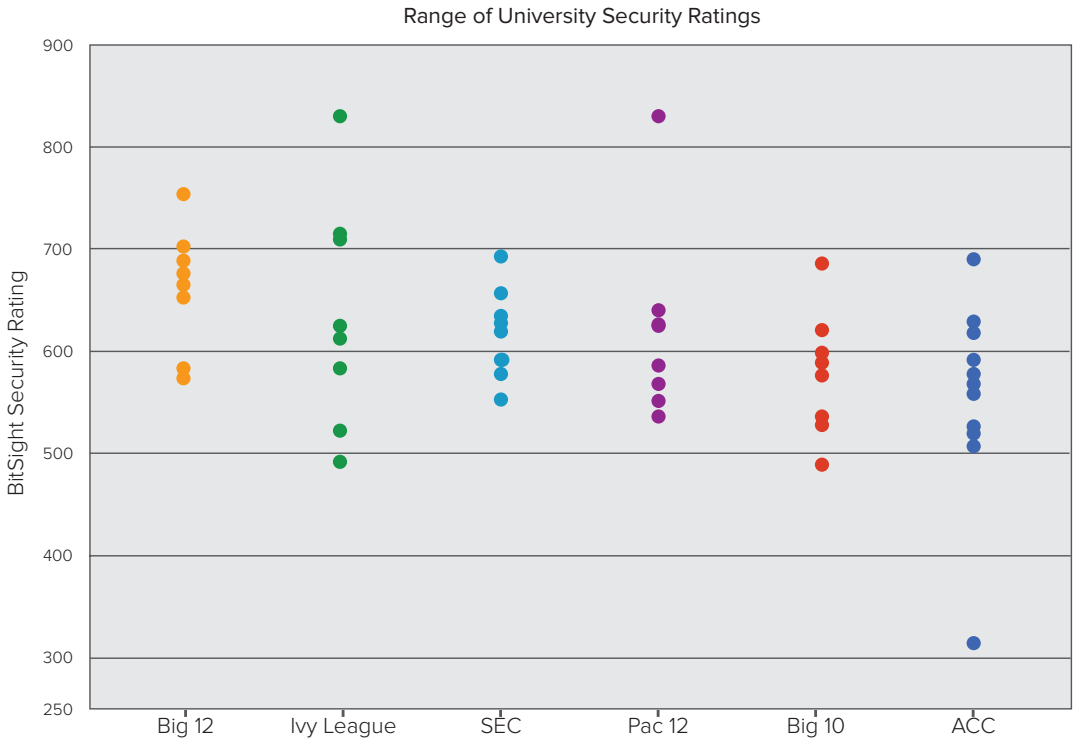
With public breaches and intense regulatory oversight, it would seem that these information security issues would prompt schools to create a strategic plan to tackle these problems. After all, poor cyber security practices leading to a data breach can have severe financial impacts: it can alienate future and current alumni donors, affect ticket and apparel purchases at sporting events, and even devalue important intellectual property that serves as a revenue stream for many large institutions. Some schools recognize this challenge and are rising to the occasion. Confirming the results of our data analysis, higher rated schools also demonstrated a commitment to information security. Perhaps most revealing, all universities with a Security Rating of a 700 or above employ a Chief Information Security Officer or Director of Information Security. Many of these schools also have online resources for faculty and staff and active information security awareness programs. Yet, for other schools, research indicates that strategic cyber plans fail to exist; a recent SANS survey revealed that fewer than half of higher education organizations have a formal risk program to assess and remediate cyber threats.[3] While patching antivirus and firewall systems is an important part of a security team's job, these employees also need to advocate placing information security as a key strategic issue for their institutions.

1. Grama, J. (2014). Just In Time Research: Data Breaches in Higher Education. *EDUCAUSE*. Retrieved August 1, 2014.
2. Ponemon Institute. 2014 Cost of a Data Breach Study: United States. (2014, May). Retrieved August 3, 2014.
3. Marchany, R. (2014, June 1). Higher Education: Open and Secure? *SANS Institute*. Retrieved July 1, 2014.
4. Wakabayashi, D. (2014, January 19). Apple Devices Flow Into Corporate World. *The New York Times*. Retrieved August 6, 2014.
5. Elmer-DeWitt, P. (2010, August 7). Big Macs on campus. *Fortune*.

Conclusions

Overall, our data shows that the security performance of higher education institutions is failing to make the grade. With limited resources, university security teams are often falling behind. One way that security teams can better communicate and monitor security is through benchmarking performance. By tracking changes over time and comparing internal security performance against peer and competitor schools, security professionals can more efficiently use the resources on hand, and better advocate for increased budget and resources to improve their performance. While information sharing should be prioritized through organizations such as the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC), having insight into malicious activity on peer networks can greatly expand the visibility of potential and current threats facing these institutions. This becomes more evident in our data: many schools face similar threats, such as Flashback, Conficker and Adware. With this information, schools can take proactive steps to mitigate common threats.

It is important to note that while the aggregate conference ratings indicate overall poor security performance, there are schools that stand above the rest. In each conference, there was at least one school with a rating of 680 or above. These schools, in general, have fewer security events on their networks and lower event duration. For universities, this insight is invaluable. Schools that need accessible metrics and comparison tools to advocate for resources and budget can use Security Ratings as an evidence based measurement of overall security. This empowers schools to communicate meaningful and accessible metrics to decision makers, and integrate information security into the overall strategic goals of colleges and universities.



Each point represents one university's Security Rating.

Open campus networks and the BYOD campus culture are not likely to change any time soon. Students and faculty have diverse IT needs that require multiple access points and large often unrestricted networks. In order to effectively prioritize security on campus networks, security teams need expanded visibility into their current network vulnerabilities and quantitative benchmarks for comparison. Only when information security moves out of the IT department and becomes an institutional strategic priority will higher education organizations effectively create an environment that secures sensitive personally identifiable information (PII) and intellectual property (IP) data. For many of these institutions, benchmarking and monitoring security performance is a good place to start.

BITSIGHT®
The Standard in SECURITY RATINGS

About BitSight Technologies:
BitSight Technologies is transforming how companies manage information security risk with objective, evidence-based security ratings. The company's Security Rating Platform continuously analyzes vast amounts of external data on security behaviors in order to help organizations make timely risk management decisions.

125 CambridgePark Drive, Cambridge, MA | www.bitsighttech.com | info@bitsighttech.com | 1.617.245.0469
Follow us on Twitter: @BitSight