SpriteGuard

By Traffic Observation via Management Limited (TOM Ltd.)

"SpriteGuard - Protecting Open Access Wifi against the ever evolving scourge of cyber crime"

Cybercrime costs[1] the UK economy approximately £27 billion per year, with almost 70% of that threat being against retail operations and establishments. Worldwide these costs scale to almost half a trillion dollars. One of the enabling factors for this risk is the increasing use of mobile devices and services by the general population. With 70% of tablet users and over 50% of smartphone users stating[2] that they use public Wifi hotspots, how can facilities management secure not only payment card infrastructure, but also ensure the security of customers' corporate and personal data?

The Payment Card Industry (PCI) Security Standards Council defines a series of Data Security Standards that aim to protect payment card information transiting over retail networks. These standards do not protect customers using retailer-provided wifi systems for online shopping and banking transactions, nor do they provide any security for personal and corporate information such as social media, work related accounts and other private data.

This vulnerability is particularly acute in open access environments such as cafe's and bars, where enterprise grade security such as pre-assigned key exchanges or backend encryption schemes are simply not appropriate or practical, for a transiting, short-engagement time, customer base.

---

[1] https://www.gov.uk/government/publications/the-cost-of-cyber-crime-joint-government-and-industry-report
[2] http://usa.kaspersky.com/internet-security-center/internet-safety/public-wifi#.VCAm73Wx3UY

This white paper provides

- An overview of current threats against customers and providers in open access networks.
- A review of the current PCI DSS Compliance guidelines for retail operations providing customer-facing WiFi access.
- An introduction to SpriteGuard™, a family of product offerings that provide non-invasive, auditable, wifi area security for both segregated and non-segregated customer and secure wifi networks.

Threats against open access consumers and merchants

With the increasing popularity of open access wifi in 'digital nomad' environments such as cafes, restaurants, hotel lobbies, bars, etc., mobile device usage is an increasing security risk not only for enterprises rolling out bring-your-own-device (BYOD) platforms, but also for individuals. The Wireless Broadband Alliance expects[3] the number of such open hotspots to increase to 5.8m in 2015 from just 800,000 in 2010. The security of such networks is critical to ensure their continued widespread use, and consequently to maintain economic growth and customer satisfaction.

Charlie McMurdie, former head of the UK's Cyber crime unit and a senior security analyst at PWC has been quoted in The Telegraph[4] stating that "A lot of mainstream criminals have identified there are easy opportunities and vulnerabilities just walking down the street and exploiting Wi-Fi networks that exist in every coffee shop".

[3] http://www.wballiance.com/wba/wp-content/uploads/downloads/2013/11/WBA-Industry-Report-2013.pdf

[4] http://www.telegraph.co.uk/sponsored/technology/4g-mobile/data-security/10983100/cyber-security-wifi.html

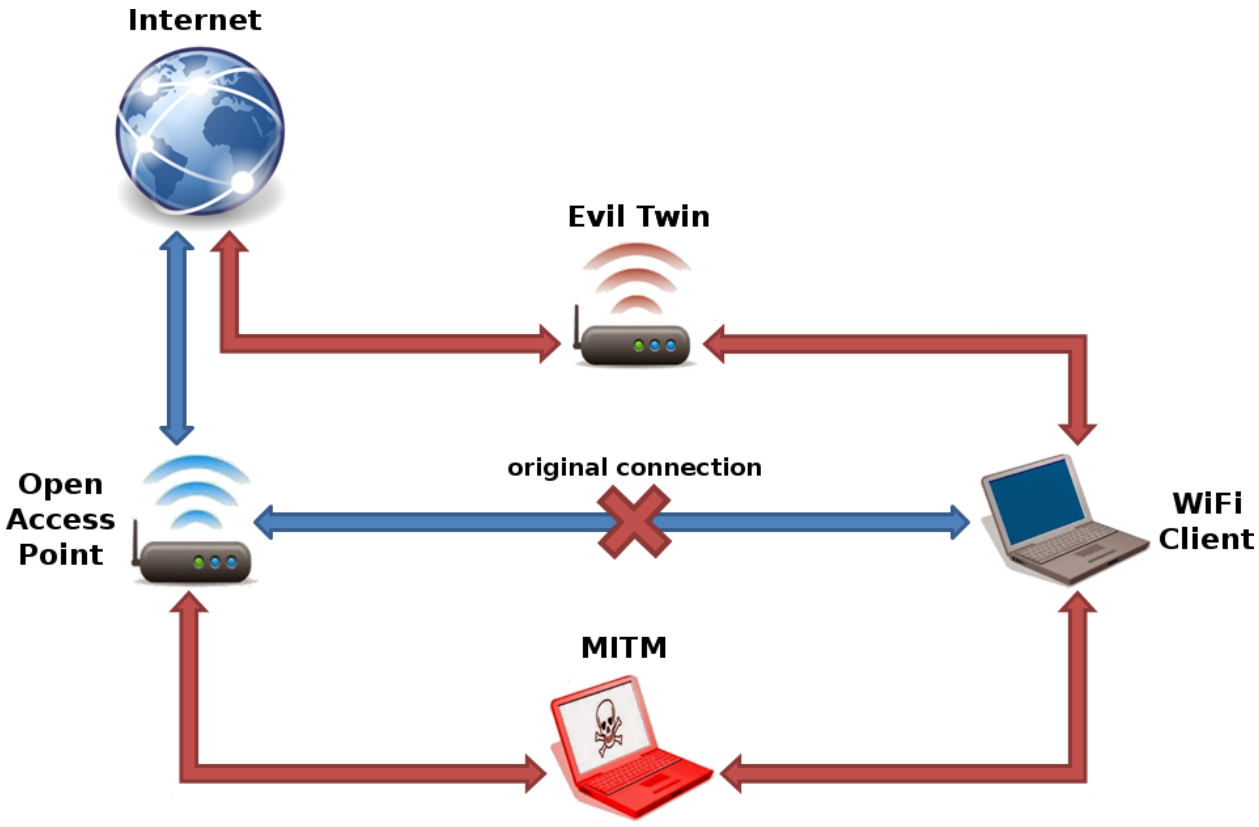


Figure 1: Example of Evil Twin and Man-In-The-Middle attacks

One of the most common form of wireless attack are “Evil Twin” attacks, where an attacker advertises itself as a fake wireless network similar to the legitimate access point except using, in many cases, a separate backhaul connection such as a 3G/4G connection. This opens up customers to having all of their data being transited through, and modifiable by, the attacker. Another common attack that is very similar in operation is called the Man In The Middle (MITM), whereby an attacker temporarily advertises itself as the access point on the same network, and routes the victims traffic through the original, legitimate, router. This attack is particularly worrying as the legitimate access point is still interacting with the victim, with the attacker able to control the data connection.

This data includes but is not limited to, bank and social account login information, emails and their attachments, and data synchronised by applications such as Dropbox and iCloud. Further, through the use of packet injection and browser caching, attackers can inject executable code into a browser's’ session that is held in the victim’s machine even after leaving the wireless network and returning to a secure network, potentially introducing crimeware/malware/spyware to a supposedly secure, internal network.

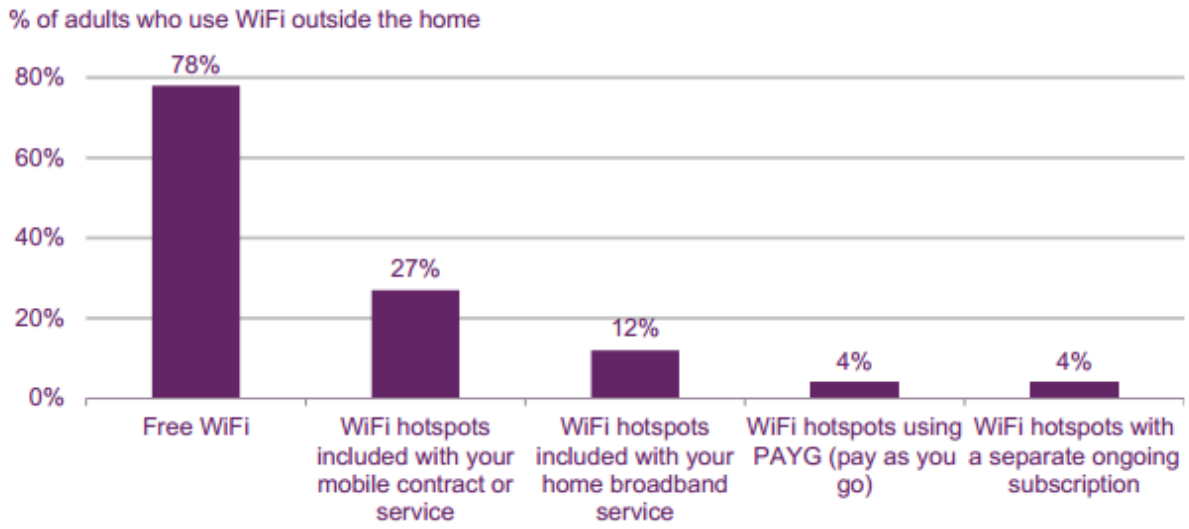
A more simplistic, but nevertheless damaging family of attacks, are Denial of Service attacks. These take on many technical forms but in general are concerned with either totally jamming a wireless network from it’s users, or selective jamming individual users, possibly to coerce them

onto previously discussed Evil Twin platforms. A related attack that has had little empirical research performed in public wifi is the use of selective denial to inflict reputational damage on the provider, potentially losing customers who go to a competitor for their 'better' wifi.

These factors combine to cause an open access dilemma, where two competing forces are at loggerheads; security and usability.

Merchants providing wireless want to provide an easy to use, accessible, secure, performant wireless environment for their customers to use while paying for their services, while protecting their own infrastructure through the use of segregating firewalls that fall under PCI DSS Scope. The Wireless Broadband Alliance report[5] highlights 'Increasing Customer Satisfaction and reducing churn' as being the joint-first most important factors for investing in hotspot systems, along with encouraging users to offload from their cellular carriers.

Meanwhile, consumers are overwhelmingly unconcerned about the security of their wifi connections, despite continuing to use such networks for private correspondence. In OfCom's 2014 Communications Market Report[6], 77% of respondents said that they were not concerned about how secure their connection was, while 78% of adults said they use free public wifi when not at home over Pay-for hotspot schemes. 72% of respondents said that they used public wifi at least once a week, over 50% said they used such networks for social networking, browsing the Internet, and both personal and business email. Over 20% also said they performed shopping and banking transactions on such networks.



Source: Kantar Media Omnibus
Base: All who use WiFi outside the home or while travelling (N=348)

Figure 2: Types of WiFi used in public places outside the home or while travelling

[5] http://www.wballiance.com/wba/wp-content/uploads/downloads/2013/11/WBA-Industry-Report-2013.pdf
[6] http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr14/2014_UK_CMR.pdf

This clearly demonstrates that consumers put themselves at the mercy of service providers, are perfectly willing to expose their personal data, and will happily take the path-of-least-resistance when it comes to accessing wifi. This attitude precludes the ability for merchants to impose enterprise-style security measures to authenticate users, chiefly because those users will quickly move on to an easier to use, but potentially less secure, provider.

The same report indicates that over 60% of public wireless users do so at low-loyalty, short-engagement locations such as cafe's and bars, where users have a plethora of similar offerings, and the difference between a customer and a passer by could be the provision of wifi.

Current estimates[7] put the price of consumer-facing cybercrime, such as Identify Theft and Online Fraud, at over £3bn per annum. It's clear that there is a need to defend not only customers, but also to defend merchant-provided wireless systems. Legislative gray areas, such as the Digital Economy Act 2010 which blurred the line of responsibility[8] for criminal acts performed via public wifi, could potentially leave such providers culpable of malpractice for not protecting their customers. This could leave many providers with no option but to shut down their open access systems, incurring reputational and revenue costs from lost custom.

Current provisions for security of Customer Data in PCI DSS 3.0

The PCI Compliance provides retailers with a globally recognised mark of security in dealing with payment card data. While not currently mandated across the world, compliance is required by many payment card providers and insurers, reducing total operating costs for merchants by satisfying insurers and payment card service providers as to the supposed security of the merchant's operations.

Under the current PCI DSS 3.0[9] (DSS) released in 2013 and enacted at the beginning of 2014, and the supplemental PCI DSS Wireless Guideline[10] (WG) released in 2009, any wireless access points connected outside the Card Data Environment (CDE) are 'not within scope' of assessment. Regardless, under DSS 11.1 there is a requirement to monitor for, and notify in the event of detection of, unauthorised wireless access points that could be connected to the CDE as part of a quarterly site assessment, or an ongoing WIDS/IPS infrastructure.

The WG (while being superseded by DSS 3.0) goes into great detail about the different architectures and topologies that are in, and out of scope with the PCI requirements, the most relevant to the above described scenarios being that of a segmented wireless network, whereby open access traffic is physically or virtually separated from the Card Data Environment (CDE).

---

[7] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

[8] http://www.itpro.co.uk/641650/the-piracy-pitfalls-of-offering-public-wi-fi

[9] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

[10] https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

As shown in Fig <REF>, all POS information is protected within the CDE, and DSS 3.0 goes to great lengths to secure and audit the transit of that data through to Internet Based Card Processing backends.

However, the vulnerability in this case is where a customer using the open access wifi, which we've demonstrated is almost completely insecure, to perform some 'secure' transaction, as we've established that they are extremely likely to. That transaction may even be to the same merchant's internet-based store while they're currently operating from the physical store. Regardless, the transaction is taking place on the merchant's premises, using the merchant's network infrastructure, where there is a reasonable expectation of security on the part of a loyal (or opportunistic) customer.

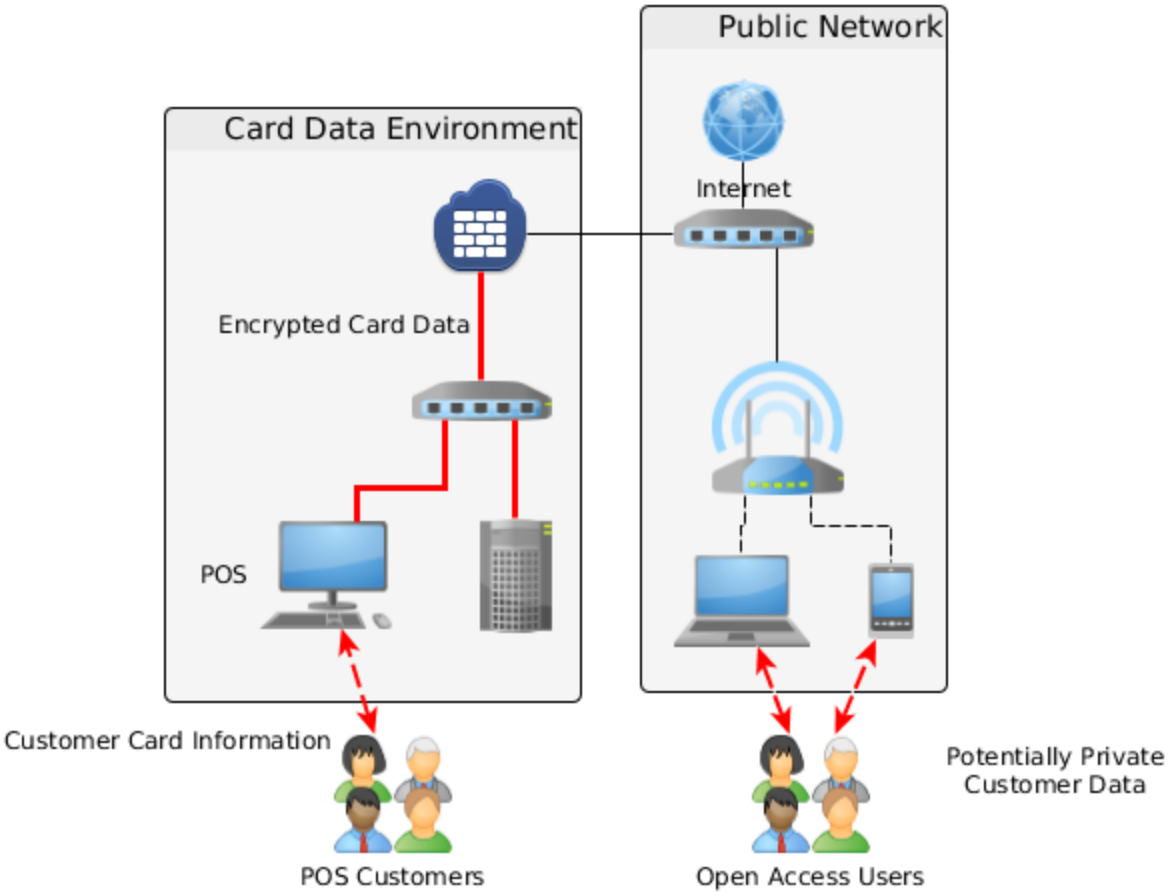


Figure 3: Architecture of a common CDE/Public Wifi Deployment

The DSS mandates a quarterly scan for Unauthorized Wireless Devices, however the DSS's definition of an "unauthorized access point" does not include access points that are not connected to the CDE, a specification for protection that does not cover any of the aforementioned attacks on customers.

Even if the DSS was expanded to include 'Evil Twin' style access points, quarterly assessment cycles are rendered irrelevant considering the sporadic and short lived nature of these style of

attacks. Verizon's Data Breach Investigations Report 2014[11] found that nearly 100% of cyber crime attacks take less than a day to accomplish, whereas only 20% of attacks were discovered within several days of a breach. Together with 'drive-by-wi-fi' hijacking, the likelihood of an attack being detected whilst a scan is being performed is almost impossible within currently mandated requirements.

While no current system can totally prevent fraudulent or malicious wireless usage, there are research-backed methodologies that can greatly limit the freedom that cybercriminals have to operate within a merchant's premises.

Introducing the SpriteGuard family

SpriteGuard™ is a wireless intrusion detection and prevention (WIDS/WIPS) system based on next generation network security technologies designed to perform cross-layer attack detection and prevention. It can work either alongside the existing infrastructure, or as part of a fully managed offering, in order to detect and prevent WiFi threats.

Together, they provide significant security for merchants; preventing cyber criminals even beginning their attacks on clients by blocking the basic malicious behaviours common to many wifi attacks.

The product portfolio comprises a range of physical devices (SG-Devices) that scan for unauthorised/malicious activity in Wi-Fi networks and protect the clients and access points (APs) in those networks; the portfolio also comprises a central management console (SG-MC) that can control the SG-Devices (SG-Scanner, SG-Sniper and SG-AP) and receive status updates from them.

The SG-MC is a cloud-based security management system that receives reports from the physical SG-Devices about the security status of the wireless environment. SG-MC provides a web-based display of important information such as the MAC and IP addresses of the clients connected to a Wi-Fi access point, and whether or not any attacks have been perpetrated, updated in real-time. It also has the facility to whitelist and blacklist specific clients; if they have been caught attempting an attack before, they will automatically be blocked from the next facility or franchise that they attempt to move to. SG-MC also provides trends of attacks over time, as well as logs for every SG-Device that connects to it. These logs may be used for further forensics, or for certification purposes (e.g. PCI-DSS reports). A monthly report, about the status and attacks, is available for each SG-Device connected to the SG-MC.

[11] http://www.verizonenterprise.com/DBIR/2014/

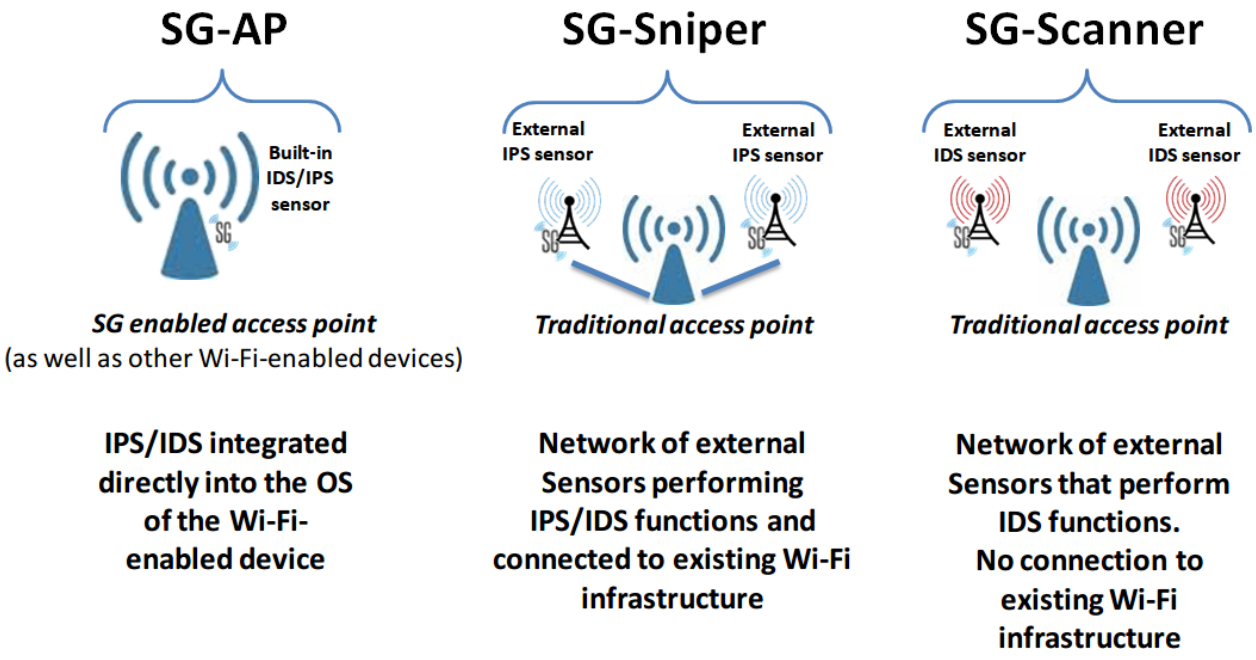


Figure 4: SG-Devices portfolio

The SG-Scanner provides the most basic level of security whereby small low-cost sensors are deployed alongside existing access points to monitor the Wi-Fi airspace in a customer's premises, but do not need to be integrated into the existing Wi-Fi infrastructure. SG-Scanners behave as additional radios that can be deployed throughout a customer's premises to cover the entire area that needs to be monitored. They remove the burden of scanning the airwaves from the access point so that it remains free to operate exclusively as an access point. They report information such as the ID and MAC address of every client connected to the Wi-Fi network, as well as the details about every other access point operating in the area. SG-Scanner also monitors for abnormal network activity such as floods of authentications or de-authentications, and reports all this information back to SG-MC. In the case of larger premises, individual scanners can either protect the 'home channel' of the in-place access point, or to hunt through other Wi-Fi channels looking for off-channel evil-twin attacks, or other potential threats that would normally be missed by a single channel solution.

The SG-Sniper also operates alongside the existing Wi-Fi network and equipment, but provides enhanced protection for the existing access point as well as for the clients. SG-Sniper has the ability to disconnect selected clients from selected access points, e.g. should they unwittingly connect to rogue or unauthorised APs. They can also connect to the existing Wi-Fi access point in order to implement and dynamically configure client blacklists and whitelists, upon command from SG-MC. In this way the existing AP is protected against attacks design to exhaust its resources (e.g. Deauth floods and "ping-of-death") and the clients are automatically disconnected from any unauthorised APs.

The SG-Scanner and SG-Sniper collect and report information about APs (ESSID, BSSID, channel, type of encryption, RSSI, clients connected) and clients (MAC address) in the neighbourhood area. They collect also other information for the AP that needs to be protected such as IP addresses of both AP and clients connected. Moreover, they provide statistical information about number of total packets analysed subdivided by type of frame (management, data and control), with more details for beacon and data types. All information are collected without compromising the users' privacy as the data inside the packets is not analysed or collected.

The SG-AP provides the highest level of security for Wi-Fi networks. SG-AP is embedded within Wi-Fi-enabled access points in order to prevent hacker attacks against the clients in Wi-Fi. Networks, and also protection for the APs. The software consists of a sub layer – termed the Attacked Resilient Sub Layer (ARSL) – that is integrated into the operating system of the device between the driver and the MAC layer. All data traffic passes through the proprietary algorithms within the ARSL where malicious packets are detected and destroyed. Importantly, this is accomplished without inspecting the contents of the traffic, meaning that data integrity is maintained at all times.

Conclusion

SpriteGuard provides a level of security and peace of mind not currently available, targeted at the problems inherent in open access wifi markets. These markets make up a significant amount of public wifi browsing time and are currently left out of PCI DSS Compliance considerations. With low cost of entry and a subscription based SaaS notification and monitoring solution, SpriteGuard is an essential measure for facilities managers that value their clients and end users data as well as their own liability.