Delivering Secure, High-Performance CCTV Networks with Always On Internet Connectivity

CCTV networks have evolved dramatically in recent years, with the global CCTV camera market expected to reach an impressive $16.1 billion valuation by 2029. Surveillance activity is rising on a consumer, business, and government level – and the UK is no exception. In fact, the UK has more surveillance activity per capita than any other European country: one security camera for every 13 people, according to CCTV statistics.

As the scale of CCTV networks increases, so does the number of threats. Low-level passwords getting compromised, internet-facing networks used to spam other networks, IP spoofing as a way to carry out malicious activity… The CCTV safety battle is ongoing. Incidents in recent years have thrust the topic of CCTV safety into the spotlight, one of the most notable being the 2016 Mirai malware attack. The event left much of the Internet inaccessible on the US east coast after turning CCTV cameras into bots via a DDoS attack.

Many operators are switching to IPVPN-based private CCTV networks to address the complex, ever-growing security issues. However, these alternatives are not an option for everyone; a significant number of organisations still have CCTV networks using consumer grade SIMs. The question is, how can such CCTV networks continue to operate at high performance and also prioritise security? There are some critical considerations for those purchasing, installing, and managing CCTV systems to think about, explains Shaun Nicholls, Technical Director, Comms365.

The Requirements of CCTV Network Users Today

A reliable, secure optimised Internet connection is crucial to fulfil the purpose of CCTV surveillance: to prevent, detect and record crime. High-quality images require high bandwidth connectivity from a network with high resilience and reliability, both of which can be achieved from a solution using bonding technology. A bonded Internet connection is created by combining two or more separate Internet feeds into one single, higher bandwidth and faster connection.

Furthermore, the degree to which images can be viewed, recorded, and shared is also dictated by bandwidth. If CCTV cameras pick up on and capture movement, a high bandwidth – and subsequently a large data connection – may be required. Larger data connections mean there will be minimal camera delays and latency, which in turn will capture images as and when the movement takes place.

Another requirement of CCTV network users is remote monitoring and access. Different sites with surveillance around the country, and even the world, can be centralised. These centralised sources feature managed connectivity platforms through networks and for various facilities.

These requirements, both individual and combined, have led to CCTV networks becoming increasingly connected. This offers a range of benefits in accessing and streaming high-quality images, but there can be pitfalls. The more connected a CCTV network is, the more it falls under threat – especially if the organisation doesn't take security as seriously as it should.

With more cyber-attacks than ever, network security is of paramount importance. It is vital to transport traffic securely, and for the sites and network to remain uncompromised, so security arrangements have equal or greater importance to the speed and performance of the Internet connection.

So, how can maximum security and optimal performance complement one another?

CCTV providers should take a multi-layered security approach to their systems to protect infrastructure and data. This approach would incorporate seamless failover between different providers to improve resilience and maintain robust connections. This should be the plan at all site locations, even those that offer the most challenges.

Ensuring CCTV Security

In light of incidents such as the 2016 Mirai malware attack, legislation around IoT devices is becoming stricter. The Cyber Resilience Act proposal aims to bolster security and combat the €5.5-trillion global cost of cyberattacks. Once passed as legislation, it will require device manufacturers to review the risk profiles of their products and fix any discovered vulnerabilities. Not only that, but these vulnerabilities must be reported to the European Union Agency for Cybersecurity (ENISA) within 24 hours.

Security at the device level means that manufacturers need to apply techniques such as securing the chip and protecting the hardware, software, and firmware. As legislation around CCTV surveillance security becomes widespread, these manufacturers may have to start proving the security measures taken.

On a network level, there is also a growing emphasis placed on security. Network providers must deliver secure solutions that don't compromise high-speed, reliable Internet feeds. Best practice would include switching from public Internet-facing to private VPN SIM networks for installation, which can then enforce 24/7 security access and surveillance via firewalls.

The simple process of installing a CCTV camera and connecting it to the Internet is no longer sufficient. Multiple layers of security technology and policies are essential to maintain the integrity of surveillance systems, with minimal risk of economically-damaging cyberattacks, which secure Always on Internet Connectivity can now deliver.

Conclusion

IT security remains the top priority for CTOs and CIOs – and, in turn, for those setting up and managing the organisation's CCTV network. The volume of data and resilience required for high-quality images may need a bonded Internet solution to optimise performance and reliability. Coupled with VPN-based secure access control, this solution mitigates against security threats without compromising quality. Moreover, network providers are recommended to act now to ensure customers' devices are protected and meet legislative guidelines, such as those outlined in the Cyber Resilience Act proposal – again, these are guidelines that SIM-enabled devices can be inherently configured to adhere to.

www.comms365.com
sales@comms365.com
01234 865880