Whitepaper

Data centre security; fighting on two fronts

Genetec™

techUK

Contents

Executive summary

The UK's data centres are an undisputed success story. Collectively they underpin an internet economy that contributes to over 16% of domestic output, 10% of employment, and 24% of total UK exports. They are a physical manifestation of our digital economy and just as central to our economic prosperity as concrete or steel. Yet, several factors are heightening complexity for operators when it comes to staying on the cutting edge of security while remaining compliant.

Consistent demand from customers for increased bandwidth means operators must anticipate future mergers, acquisitions, and expansion to new sites, leading to the convergence of existing security departments. Often, this also means inheriting various security technologies and processes that must be integrated to maintain a consistent picture of security operations. Added to this is the need to keep on top of a growing volume of regulatory frameworks related to data privacy and information security.

Meeting and demonstrating compliance with the stringent criteria for the likes of the General Data Protection Regulation (GDPR), SOC 2, and ISO 27001 information security standard requires specific consideration of how physical security systems are configured and managed. For example, Article 15 of the GDPR states any member of the public can

file a data subject request to obtain CCTV footage and that "the right to obtain a copy… shall not adversely affect the rights and freedoms of others". This short clause presents a logistical challenge for any data centre operator not relying on software for the automated redaction of faces in video footage as every frame of requested video could contain many other third parties. Equally, SOC2 contains non-negotiable requirements related to adhering to appropriate retention periods for data generated by video surveillance and access control systems.

Finally, there is the evolving threat of cyberattacks. Data centres are of course well equipped to provide high levels of security far beyond what customers could ever hope to maintain in-house. They are rightly seen as part of the solution for security-conscious companies and individuals. That's why a cyberattack on a data centre can be catastrophic.

So, how can operators centralise security, be compliant in operations to protect data, and satisfy regulatory requirements while also functioning effectively across multiple sites? This white paper outlines the rationale and guidance for addressing the cyber and physical security of data centre facilities in a single plan.

1

Security as a shared responsibility

Data breaches are a global reality, impacting everybody, everywhere. Some are caused by weaknesses in an organisation's virtual perimeter. For instance, when hackers can exploit software vulnerabilities to gain access to a connected system from the outside. Others rely on a breach of a physical perimeter, such as when a visitor can get inside the facility to connect a rogue device. In the case of the most sophisticated and targeted attacks, it's common for criminals to probe for weaknesses in both realms until they discover the weak link that allows them to gain access, remain undetected, and exfiltrate sensitive data over a significant period.

It's why maintaining good cyber hygiene relies on a combination of people, processes, and technology. And why securing an organisation against cyberattacks cannot simply be delegated to IT or appropriately addressed within departmental siloes that do not collaborate. Data centre employees, contractors, and visitors all periodically require access to restricted areas. Yet, a failure to appropriately restrict, monitor, and audit access to physical servers instantly compromises any cybersecurity precautions that have been put in place. For example, IT professionals can rely upon monitoring tools to detect an incidence of a USB device being connected to a server. However, it is only by integrating such an alert with the operator's video management system that security teams can be put in a position to quickly respond. Having instant access to the associated video footage in that part of the facility makes it far easier to quickly ascertain who was responsible before it is too late.

HR, physical security and information security professionals within a data centre environment all share a common goal of supporting the business and mitigating risk. They exist in a symbiotic relationship as none can succeed without effective teamwork with colleagues in other departments.

Having instant access to the associated video footage in that part of the facility makes it far easier to quickly ascertain who was responsible before it is too late.

2

Strategic takeaways

Number one – centralise compliance, security, and operations

The ability to easily keep track of who had access to what and when, who granted it and why, has benefits far beyond the security function. It sits at the core of satisfying regulatory requirements and ensuring the smooth flow of people throughout the facility. Commonly, there are a significant number of people and steps involved in granting access to a room or rack and, if authorisation relies upon manual intervention in the access control system, there is a lot of room for mistakes. Social engineering is therefore often used by criminals as a means of getting inside a data centre facility. Making use of a physical identity and access management solution that bridges physical and IT security to automate the workflow removes the potential for human error while also delivering associated cost efficiencies.

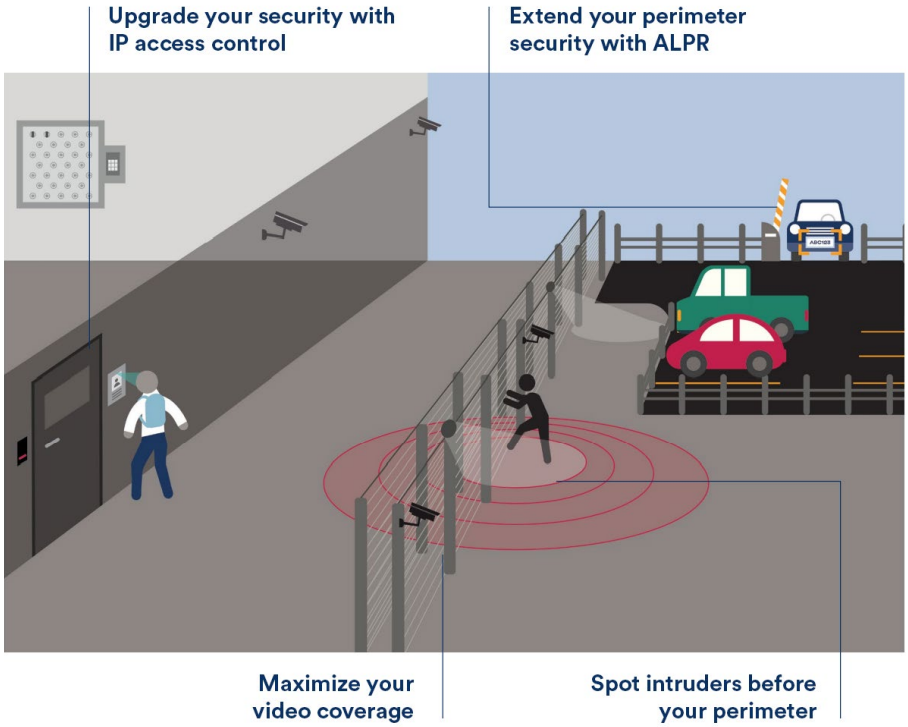
That is why operators should invest in and rely upon a scalable and unified security platform that takes into account the requirements of users within and outside of the physical security function. There are many other ways in which centralisation can enhance security and streamline compliance operations. For example, by making it easier to set expiry times for contractor passes or by automating the generation and sharing of audit reports so that any irregular activity is quickly brought to light. Automation is key as these activities are easy to specify but difficult to consistently carry out if manual intervention is required.

Pooling resources and expertise from across the business allows for the specification and deployment of a common platform with greater capabilities than any one function could hope to develop in isolation. It simplifies day-to-day operations and prevents future headaches surrounding overlapping systems that create operational blind spots through a failure to integrate.

Pooling resources and expertise from across the business allows for the specification and deployment of a common platform with greater capabilities than any one function could hope to develop in isolation.

Diagram 1

A layered approach to physical security



Number two – take a layered approach

It is easy to think in terms of a facility having a single perimeter that needs to be secured. However, it is important to recognise that facilities comprise of multiple overlapping perimeters, each with its own rights of access, risk profile, and operational requirements.

For data centres, the situation is particularly nuanced. There are all the usual considerations over public and private areas and where people may pass between them to consider. Equally, there are specific partitions that must be maintained concerning individual customers' hardware or data. It's not a case of simply controlling access to the facility but of dynamically controlling access to specific data halls, rooms, and even the individual cabinets that they hold.

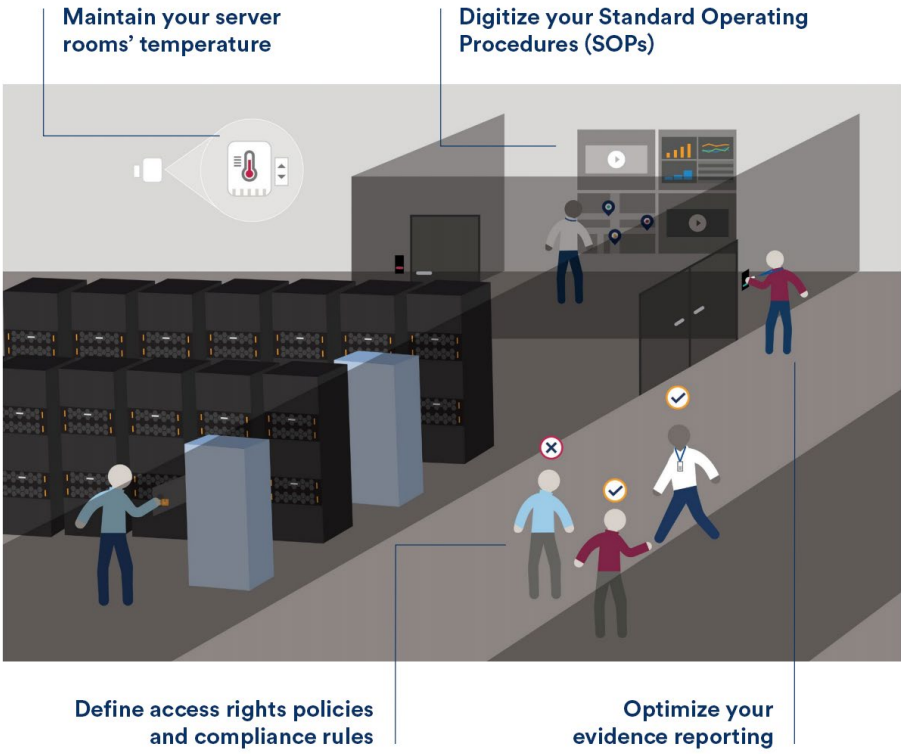
Don't put too much reliance on any one sensor or analytic to detect intrusion. Instead, build out a layered approach to perimeter security that ensures all is not lost should one method fail. As outlined in the diagram above, video surveillance, number plate recognition, biometrics, LiDAR, and fencing are just some of the technologies

that can be combined as part of a comprehensive plan to discourage unwanted incursions. Also, don't be too reliant on security operators having to actively monitor the input from these sensors to identify a specific security threat as the amount of incoming information can quickly become overwhelming. Optimising the time to resolution is the key metric here given a report conducted by the Ponemon Institute calculating a single minute of downtime within a data centre costing on average $9,000 to the business as a whole.

Automated alerts, alongside a structured process that guides the operators step-by-step in how to respond, help to ensure possible threats are identified, investigated, and resolved in a timely and consistent manner across different shift patterns and individuals. Many events could present a security threat that can be hard for a person to spot but that technology can quickly flag for further investigation. For example, if a contractor entering an area unexpectedly coincides with a device going offline. Or if a specific numberplate is detecting in the vicinity of a data centre many times in a short timeframe.

Diagram 2

Examples of how one platform can help to centralise security, operations, and compialnce



Genetec data reveals 68% of cameras trying to connect to its systems are typically running out-of-date firmware.

Number three – ensure physical security systems aren't themselves a cybersecurity risk

A final reason to address cyber and physical security in a single plan is the possibility that attackers could use the physical security systems themselves as potential entry points to the network. Over 90% of all IoT attacks go through routers and connected cameras.

Security cameras, access control readers, and alarm panels are all IoT devices that run the software and may contain cybersecurity vulnerabilities that can be exploited by attackers. Yet, many of the risks could be eliminated simply by taking basic steps such as ensuring they are running on the latest version of the firmware and not using default passwords. They are a shared physical and cybersecurity responsibility that could easily result in avoidable unplanned downtime.

While the automated updating of core business systems and devices is a key concern of the IT function, it is not always front of mind for physical security professionals. Genetec data reveals 68% of cameras trying to connect to its systems are typically running out-of-date firmware. Of these more than half involve known vulnerabilities for which a security update is available. It's a situation that needs to change fast and that can only be resolved by removing the burden from employees and leveraging automation to manage the firmware and passwords. Only then can organisations hope to build a resilient cyber-physical security framework from which to operate.

3

Data centres: where cyber meets physical

The data centre industry remains at the forefront of technical innovation, with strong global demand for data storage and processing as industries digitise ensuring that the market will continue to expand year on year. Against this backdrop, it's important to plan for future growth, to address physical and cyber security within a single plan, and to invest in a security system now that can scale, adapt, and evolve in line with immediate and future requirements.

Data centres must keep up with evolving regulations and security threats while ensuring their customer's needs are always met. With its ability to unify and centralise all of these considerations, the physical security platform should be considered integral to reaching these goals. It should be designed to reduce security risk, improve decision-making, and enhance compliance. No matter how the organisation grows, or how the threat landscape evolves, it should be flexible enough to evolve in line with future needs.

Video surveillance: Achieve greater situational awareness and enhance security within your city with the ability to share cameras across agencies and organizations, providing a common operational picture and improving incident response time.

Access control: Heighten your organization's security, effectively respond to threats, and make clearer and timelier decisions with a unified, IP-ready platform, whether deploying a new access control system or updating an existing installation.

Automatic license plate recognition: Automate the detection of vehicles of interest, increase parking enforcement efficiency and accelerate public safety investigations through the ability to share license plate data with selected agencies and partner organizations, without forfeiting ownership and privacy.

Operational decision support: Create efficiency for incident handling and decision making with advanced workflows that guide operators from situation alerts through policy-based procedures to detailed case compilation export.

Investigative case management: Simplify case management and speed up investigations with a platform that allows you to centralize digital evidence and securely collaborate with investigators, outside agencies and the public.

Cloud services: Extend the capabilities of your on-premises security system and reduce IT costs with highly scalable, on-demand cloud services that allow your city to easily cope with rapidly changing security requirements and operate with greater efficiency.

About Genetec

Genetec Inc. is a technology company that offers on-premises and cloud-based solutions encompassing security, intelligence, and operations. The company's flagship product, Genetec™ Security Center, is a physical security platform that unifies IP-based video surveillance, access control, automatic license plate recognition (ALPR), communications, and analytics. Genetec also develops cloud-based solutions and services designed to improve security in the communities in which we live.

For more information about Genetec, visit **genetec.com**.

About techUK

techUK is a membership organisation that brings together people, companies and organisations to realise the positive outcomes of what digital technology can achieve. We collaborate across business, Government and stakeholders to fulfil the potential of technology to deliver a stronger society and more sustainable future. By providing expertise and insight, we support our members, partners and stakeholders as they prepare the UK for what comes next in a constantly changing world.

For more information, visit **www.techuk.org**

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

UPDATED:30-JUN-2021