AT&T Business

AT&T Cybersecurity

2023 Edge Ecosystem

Focus on US SLED

Focus on US State and Local Government, and Higher Education (SLED)

About this Report
This report is a special industry report with a focus on US SLED and derived from the quantitative and qualitative research and analysis conducted for the full 2023 AT&T Cybersecurity Insights Report: Edge Ecosystem. For additional information and details about securing the edge, we encourage you to download a free copy of the full report at: cybersecurity.att.com/insights-report.

About the Research
The research was conducted during July and August 2022. We surveyed 1,418 security practitioners from the United States, Canada, the United Kingdom, France, Germany, Ireland, Mexico, Brazil, Argentina, Australia, India, Singapore, and South Korea. Respondents come from organizations with 1,000+ employees except for US SLED and energy and utilities verticals. Respondents were limited to those whose organizations have implemented edge use cases that use newer technologies such as 5G, robotics, virtual reality, and/or IoT devices. Respondents are involved in decision-making for edge use cases, including cybersecurity, that involves new technologies such as 5G and IoT devices. For certain questions, participants could choose more than one response. In these cases, the responses do not round to exactly 100%. Where indicated, this report focuses on the data collected from US SLED respondents. The total number of US SLED survey respondents is 178.

The Edge Ecosystem in US State and Local Government, and Higher Education (SLED)

In the past, IT typically made technology decisions based on business and computing requirements they understood. Thanks to ongoing advances in computing, things are changing.

Welcome to edge computing in 2023.

Edge computing is a transformative technology that brings together various stakeholders and aligns their interests to drive integrated business outcomes. The emergence of edge computing has been fueled by a generation of visionaries who grew up in the era of smartphones and limitless possibilities. In this paradigm, the role of IT has shifted from being the sole leader to a collaborative partner in delivering innovative edge computing solutions. In addition, we found that leaders in the state and local government, and higher education (SLED) vertical, are budgeting differently for edge use cases. These two things, along with an expanded approach to securing edge computing, were prioritized by the respondents in the *2023 AT&T Cybersecurity Insights Report: Edge Ecosystem*.

Topline research findings

In 2023, SLED respondents' primary edge use case is building management, which involves hosted HVAC applications, electricity and utility monitoring applications, and various sensors for large buildings. This represents a shift from the primary use case in the *2022 AT&T Cybersecurity Insights Report: Securing the Edge,* which was focused on public safety.

There are several compelling reasons behind this top ranking. Monitoring occupied versus unoccupied building spaces has been imperative as office workers are often in a hybrid work mode, with varying levels of physical presence in office spaces. Edge use cases allow energy consumption to be monitored and optimized in near real-time to manage consumption and costs.

AT A GLANCE

Edge computing in SLED is still emerging. The ability to provide new services for the public and quality outcomes for educators and students is a new reality. But it does not happen by accident or in isolation. Cross-functional collaboration among groups that don't normally work together and building-in security from the start is a smart way to tap the potential of these exciting use cases that will meet the stakeholders' expectations.

Devices are changing in SLED

Mobile devices are the top endpoint choice for SLED, accounting for 46% of the device category. In addition, 89% of respondents utilize 4G/LTE cellular networks for edge connectivity. Notably, 51% of the respondents use a combined cybersecurity and networking function located on premises. The top perceived threat in this context is the exfiltration of personal information for the purpose of financial gain or extortion, among other purposes. The vast amounts of personally identifiable information (PII) that is revealed through interactions with many SLED edge computing use cases reinforces the need to protect this information.

And it's just the beginning

One of the most promising aspects of edge computing is its potential to cost-effectively benefit environmental, social, and governance (ESG) goals at both an institutional and a personal level. The 2023 AT&T Cybersecurity Insights Report highlighted two notable use cases: the convenience of having real-time information around public parking and the use of augmented reality (AR) for more immersive learning opportunities:

- The convenience of having cameras feeding into an application server that determines whether a particular public parking garage has available parking spots at each level fulfills a couple of benefits. The reduced emissions chasing after a nonexistent free parking spot, less frustration, and faster ability to get on with the task at hand, and finally, competitively, it makes the garage more desirable for many guests.
- The use of near real-time data for AR hands-on training is growing because it provides better access to realistic situations. The benefit of using it to train or practice job skills that are inherently dangerous can reduce the risk of injury. For other types of training, the immersive nature of AR, with its ability to impact sensory touch points, improves knowledge retention because people remember more when additional learning modalities are added, like touch.

While mobile devices and personal computers are still extremely popular in SLED, their ubiquitous availability and connectivity make them vulnerable to cyberattacks. Successful cyberattacks can disrupt public services, highlighting the need for robust cybersecurity measures.

Collaboration is critical for development

The edge ecosystem in higher education requires collaboration among various stakeholders, including education leaders, research and development, innovators, legal, compliance, teachers, students, and experts in networking, cybersecurity, and IT. Successful edge computing in education is more likely to succeed when stakeholders, with all their unique perspectives, frameworks, and priorities, are engaged early and often – throughout development.

SLED edge computing use cases could have significant public visibility. Design teams will need to be aware of the various regulations surrounding the privacy and protection of PII. Most respondents indicated they are using experts who can navigate these complexities. Furthermore, considering an endpoint strategy that prioritizes user experience and secure data transfer may require intentional devices, as off-the-shelf consumer devices often fall short in terms of security requirements.

The research found that engaging trusted advisors from internal and external sources is a priority for those embarking on an edge computing path. The report reveals that SLED respondents incorporate external expertise for project planning (84%) and 85% for production. Seeking external advice can streamline processes, save time, and reduce costs, whether designing an access management approach, ensuring data integrity, or selecting the appropriate tools for data movement and protection.

The common characteristics of edge computing

Based on the research, respondents agreed that these edge-computing characteristics are common elements of most use cases.

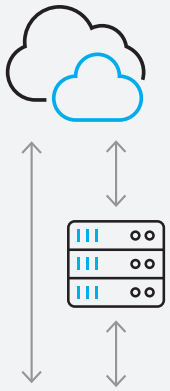
Use cases are data-driven

Edge computing is different from traditional computing. In edge computing, data is created and consumed at or very near the consumer or business of the specific use case. That means it's often happening outside traditional environments. In the public sector, as the name implies, it often happens in publicly available spaces, such as the park, the courthouse, the interstate highway, the voting booth, or the airport. In addition to data creation and consumption, decisions are often made closer to where the process is occurring, ideally resulting in better outcomes because it is personalized and near real-time and allows for rapid analysis.

The challenge is that edge data creates different security requirements. It is potentially more vulnerable and could even include physical theft if a device is stolen or lost. The quantity and length of time that data resides on an edge device impacts the potential risk if the device ends up in the wrong hands. Imagine what could occur if the data from a voting device were to be viewed. Hard decisions need to be made about whether that data should be kept on the device and for how long. It may be safer to keep it on the device until it is brought to a centralized elections site, or it may be better to transmit it immediately upon a ballot being cast. There are security considerations in both scenarios.

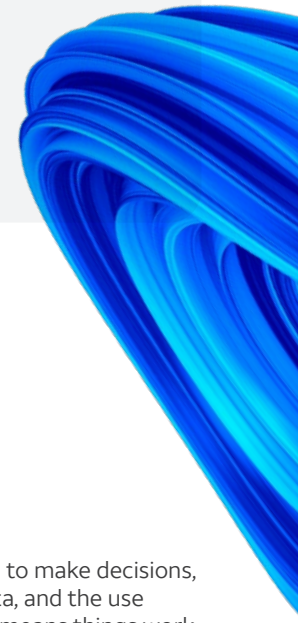
What are the common characteristics of edge computing?

Software defined
Cloud - public or private, or on-premises



Distributed configuration
Intelligence, networks, and management

Data driven
Closer to user creation and consumption



Edge computing is software-defined

Edge computing changes the network and applications, driving a digital-first experience. Workloads, hosting, and applications are closer to where data is generated and consumed. This means the cybersecurity framework needs to adapt.

Consider the use case of edge computing in the airport. Everyone has felt the pain of trying to get through security checkpoints. Passengers are seen trying to juggle suitcases, backpacks, phones, passports, or driver's licenses to prove who they are. Enter edge computing to speed up the process by allowing the layering of different edge devices to enable security professionals to identify who should and, more importantly, who should not be there. The importance of having optimized network routing capabilities is imperative for the time-sensitive decision-making that needs to occur.

The elastic capabilities of software-defined networking (SDN), which enables dynamic scaling of networking throughput to match varying demand levels, recalibrate during peak demand situations, like the day before Thanksgiving, to function. SDN can allocate more resources during peak usage: scale up for busy periods and scale down during low activity. In addition, SDN allows for centralized network configuration, reducing costs by minimizing the time needed to configure individual devices. This improvement in operational efficiency can lead to significant cost savings, particularly in the context of a shortage of network experts.

Decision-making is closer to the data

With edge computing, the intelligence required to make decisions, the networks used to capture and transmit data, and the use case management are distributed. Distributed means things work faster because nothing is backhauled to a central processing area such as a data center and thus delivers a near-real-time experience. Rapid decision-making is also supported by machine learning powered by multi-access edge computing (MEC) devices. Some use cases rely on a mix of MEC for immediate decisions and then transmit detailed or summary findings back to a cloud environment for further processing.

The introduction of these capabilities raises concerns regarding regulatory compliance. It is important to consider whether PII is stored away from its final destinations, such as cloud computing platforms or data center servers. If the data is being transferred from the edge site to a different location, it is crucial to make sure that it remains private and encrypted throughout the process.

The Challenge

Securing it is non-linear, dynamic, and unconventional

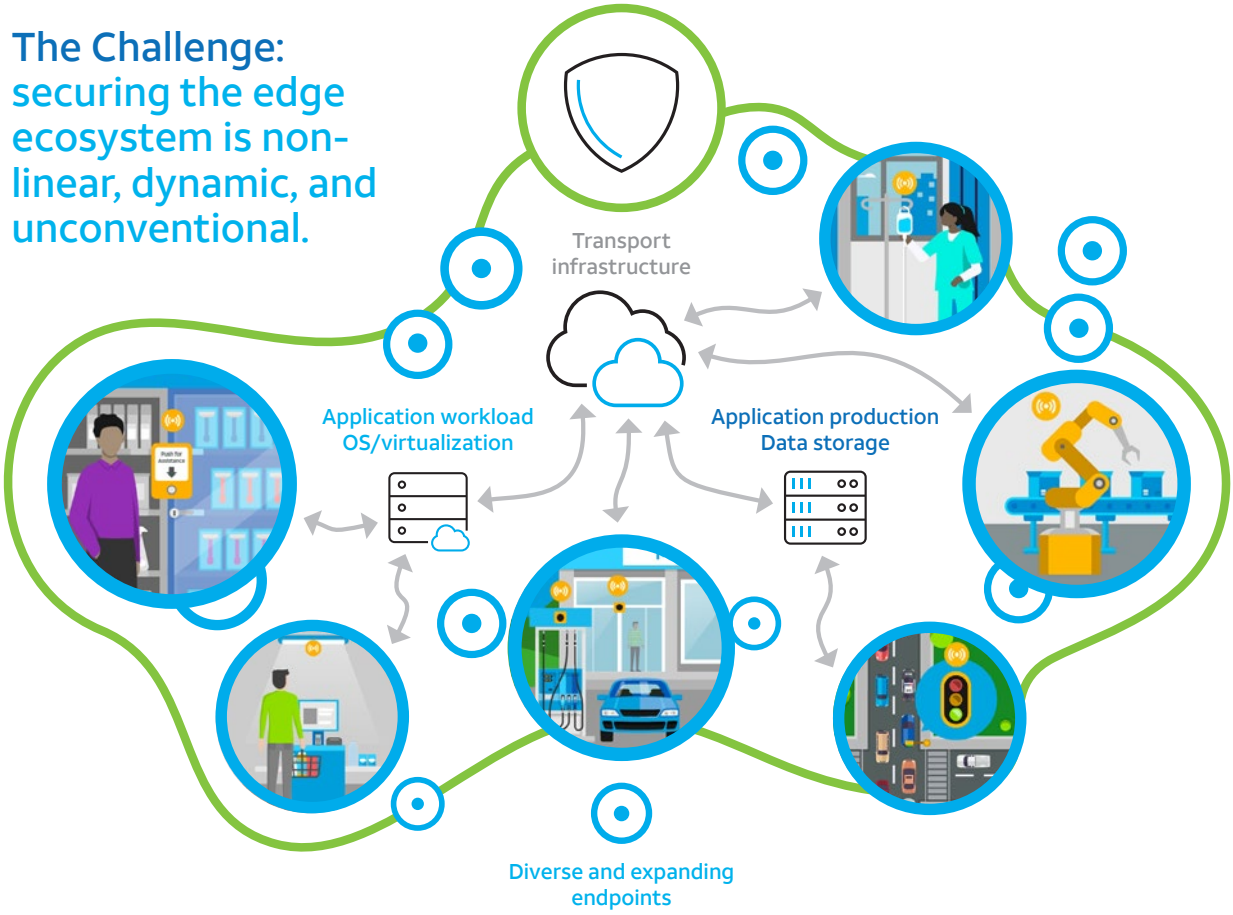
To help ensure the success of SLED edge use cases, organizations should break down the silos that have traditionally separated network, application development, cybersecurity, and education or public sector departments. Quality education for higher education students is hampered when administrators, faculty, and staff are not aligned. This teamwork is also necessary for planning, deploying, and operating edge computing environments that aid educators in the new and unique ways that learning is being consumed.

For example, the increased use of sensors and video cameras to better manage car traffic benefits from the capabilities of 5G networks, such as improved speed and cybersecurity features, including network slicing and enhanced encryption. However, when 5G is unavailable, and legacy 4G is utilized, organizations can build resilience into their solutions by adopting compensating controls. These may include further use of multifactor authentication, data-at-rest encryption, and SDN technologies that offer dynamic routing capabilities.

With this level of complexity, it's common to reevaluate decisions regarding security, data storage, or networking. Decisions are often revisited based on insights gained during the initial pilot stage and when consulting outside expertise. As the capabilities of the connected car become more widespread, the issue of who owns and can see the data that is kept on the car will likely see increased regulations.

IT and cybersecurity teams should establish a collaborative relationship to ensure all devices, including servers, computers, sensors, and robots, are regularly patched.

The Challenge: securing the edge ecosystem is non-linear, dynamic, and unconventional.



The Opportunity Securing the Ecosystem

Respondents identified three key initiatives they're embracing as they evolve their edge ecosystem. These initiatives are described in the sections that follow.

Proactive investing

When examining investments in SLED edge computing, the saying "follow the money" holds true. The research reveals that the allocation of investments across overall strategy and planning, network, application, and security for the anticipated use cases that organizations plan to implement within three years is almost equally distributed. Each use case will have its unique investment breakdown based on the scenario's specific nature.

Figure 2 illustrates the variation in investment allocation among the top five primary SLED use cases analyzed. Overall, spending is approaching a balance not typically seen in conventional computing. Where there are differences, it is likely tied to the requirements associated with the use case.

For example, the mass transit management and optimization use case shows a relatively higher percentage of spending on the network portion. The highly dispersed nature of the devices that are needed to capture all this information and safely transmit it to other field devices is paramount, hence the higher network cost. The relative maturity of this use case, with other use cases available from other municipalities, allows some of the spending on up-front strategy and planning to be allocated to other functions.

Overall, these investment allocations exemplify the dynamic nature of SLED edge computing, where there is no one-size-fits-all approach.

Cross-functional collaboration

Some of the newer use cases, such as the use of AR/virtual reality (VR) systems for training, require a broad set of skills. Prior technology revolutions have often been led by technology-focused disciplines like IT or networking. The mishaps that occurred because the consumers of the technologies were not adequately part of the planning process have caused issues.

The same principle of collaboration applies when designing SLED edge computing use cases. There are significant consequences when things go wrong for many of these use cases, such as the ones involving public safety or transportation-related areas. Fortunately, despite edge computing being a relatively new technological approach, a growing ecosystem of experienced edge partners can provide valuable insights and expertise.

In fact, the research reveals that 84% of SLED use cases involved external firms in crucial project planning processes, and 85% relied on external expertise during production. Organizations can minimize the risk of costly mistakes or missteps using outside expertise.

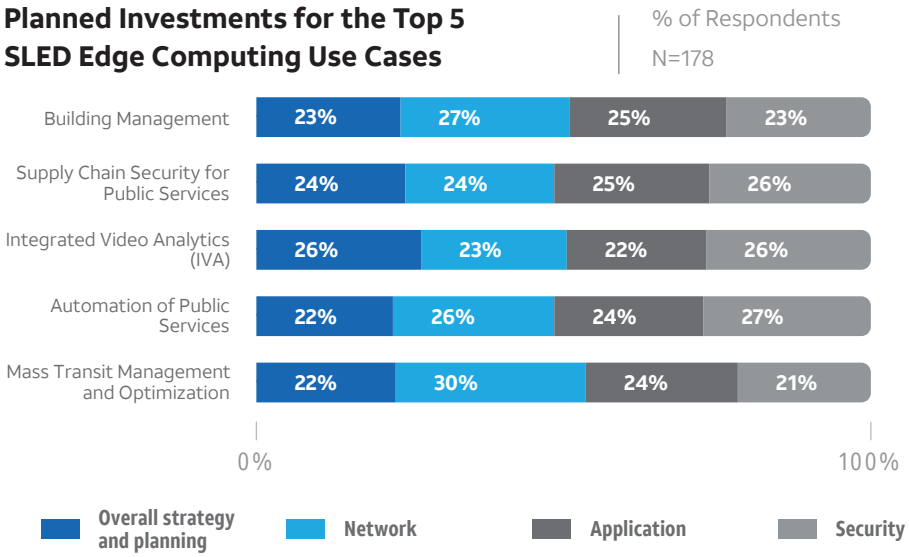
Dynamic cyber resilience

Cyber-resilience is crucial, encompassing various disciplines beyond cybersecurity. While cybersecurity is a top concern, other factors should also be considered:

- Network resilience plays a vital role in supporting edge devices, whether it's an AR/VR headset used to train a new skill set to a construction apprentice or a temperature sensor in a smart building. Edge architects must incorporate forward-thinking strategies to accommodate advancements in network technologies.
- The ability to account for various failures within an edge computing use case needs to be considered. Having a plan to patch things like an open-source library used in an edge application. Backup devices and sensors can take over the immediate functions in a traffic management system is another example of an extremely focused edge use case that could manifest big problems if a hacker were to take over the system.

Figure 2

Planned Investments for the Top 5 SLED Edge Computing Use Cases



US SLED Edge Ecosystem

Primary use case:

Building Management

Provide visibility into a building's energy and operational status through advanced technologies that help automate energy and operational functions to optimize performance and cost.

Business need:

Optimize building management performance and energy efficiency through increased automation.

Security approach:

Combine network and security functions on-premises to thwart perceived ransomware threats.

Primary use case snapshot:

Implementation Stage

71%

Partial

Top Endpoint

46%

Mobile Devices

Data Rate

28%

Enhanced Mobile Broadband (embb)

Edge Network Connectivity

89%

4G/LTE Cellular

Top Percieved Threat

2.91/5

Personal Information Exfiltration

Cybersecurity Approach

51%

Combined Cybersecurity and Networking Functions On-premises

% of respondents, or % respondents rating 4 or 5 on a scale of 1-5 N= 201

Prepare to Secure the Ecosystem

The 2023 AT&T Cybersecurity Insights Report reveals best practices and recommendations that SLED edge computing practitioners can follow to help secure current and future use cases.

Develop your edge computing profile

It is essential to break down the barriers that typically separate the internal lines of business, application development, network, and security teams. Technology decisions should not be made in isolation but instead through collaboration with line-of-business partners. Understanding the capabilities and limitations of existing business and technology partners makes it easier to identify gaps in evolving project plans.

The edge ecosystem is expanding, and expertise is available to offer solutions that address cost, implementation, mitigating risks, and more. Including this expertise from the broader SLED edge ecosystem increases the chances of outstanding performance and alignment with organizational goals.

Develop an investment strategy

During SLED edge use case development, organizations should carefully determine where and how much to invest. Think of it as part of monetizing the use case. Building security into the use case from the start allows the organization to consider security as part of the overall budget. It's important to note that no one-size-fits-all solution can provide complete protection for all aspects of edge computing. Instead, organizations should consider a comprehensive and multilayered approach to address the unique security challenges of each use case.

Increase your compliance capabilities

Education or public sector regulations can vary significantly across different jurisdictions, including countries, states, and municipalities. This underscores the importance of doing more than a simple checkbox approach. Conducting regular reviews helps ensure compliance with the growing number of regulations. Keeping up with technology-related mandates and helping to ensure compliance requires ongoing effort and expertise. If navigating compliance requirements is not within your organization's expertise, respondents report using outside help from experts.

Align resources with emerging priorities

External collaboration allows organizations to utilize expertise and reduce resource costs. It goes beyond relying solely on internal teams within the organization. It involves tapping into the expanding ecosystem of edge computing experts who offer strategic and practical guidance. Public sector and educational institutions are used to working with outside consultants as their respective disciplines seek to raise the capabilities of their respective disciplines. Involving outside SMEs in edge computing can help prevent expensive mistakes and accelerate the deployment process. These external experts can help optimize use case implementation, ultimately saving time and resources.

Build-in resilience

Consider approaching edge computing with a layered mindset. Take the time to ideate on various "what-if" scenarios and anticipate potential challenges. During the planning stages of development, it's crucial to analyze and address these potential disruptions thoroughly. It's not uncommon for certain situations to be overlooked. That's why the pilot phase is essential for uncovering any unforeseen issues before full-scale implementation. Seek input from industry peers and engage external expertise to identify vulnerabilities. Investing time and resources can yield significant benefits in preparedness and cost savings.

Prepare for dynamic response

Edge computing is characterized by its data-driven nature, software-defined infrastructure, and distributed configuration. These key attributes highlight the dynamic nature of edge use cases, where constant data insights drive continuous improvements. By transitioning from a device-centric approach to a software-defined model, edge computing enables greater flexibility in network and security components, enhancing overall resilience. The distributed configuration allows organizations to choose where data is processed and stored, providing additional options for optimizing performance and efficiency.

Conclusion

Successful SLED edge computing implementations require a holistic approach encompassing collaboration, compliance, resilience, and adaptability. By considering these factors and proactively engaging with the expertise available, public sector and education organizations can unlock the full potential of edge computing to deliver better outcomes, operational efficiency, and cost-effective solutions.

The edge ecosystem is expanding, and expertise is available to offer solutions that address cost, implementation, mitigating risks, and more. Including this expertise from the broader US SLED edge ecosystem increases the chances of outstanding performance and alignment with organizational goals.

About AT&T Cybersecurity

We simplify securing valuable business assets by providing broad cybersecurity experience and award-winning services for network security, extended detection and response, and endpoints. From traditional computing to edge computing, we're focused on business innovation. We help make complexity easy to understand and navigate.

By providing affordable, strategic services, our clients rely on us as trusted advisors. Our cybersecurity consulting is product neutral, so you get unbiased answers for your business. Our managed security services, threat awareness, and ground-breaking research are dedicated to help keep you protected today and prepared for tomorrow.

AT&T Cybersecurity manages the risk. You reap the reward.

Contributing Organizations

AT&T Business

IDC

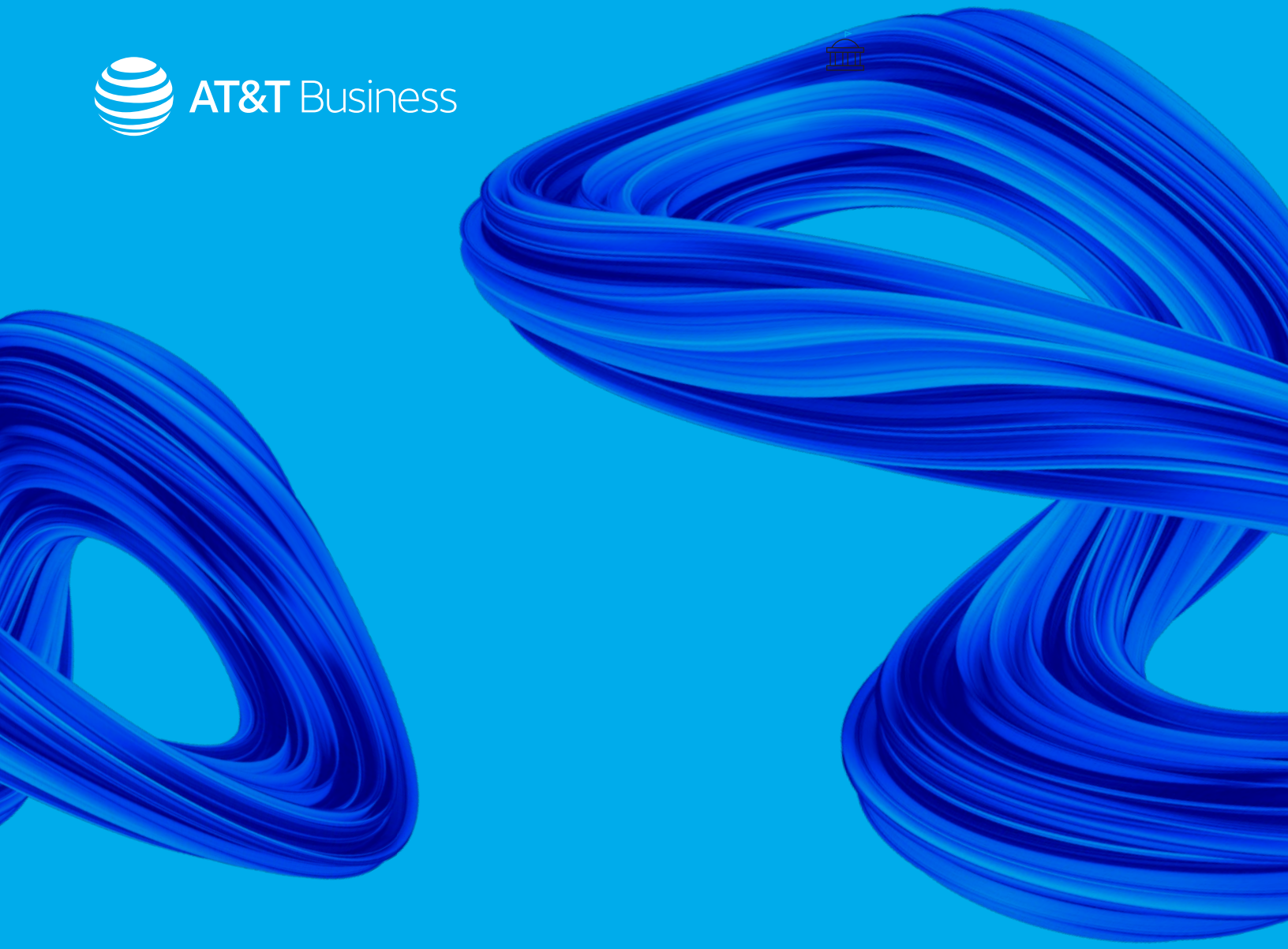
Akamai

cisco

ivanti

SentinelOne

AT&T Business



Edge computing in US SLED is here, providing new insights and services with accessibility for all aspects of state and local government, and higher education.