Strategic Sales Enablement Playbook

Dallas Digital Services – Industry-Focused Guide for Sales Conversations

This guide is designed to help our team approach five of the most common verticals with confidence.

- Core Business and IT Challenges in Healthcare
- Strategic Technology Roadmap (What DDS Can Do)
- Sales Conversation Starters (with intent behind each question)
- Objection Handling (What to say when they push back)

VERTICAL: HEALTHCARE

Core Business and IT Challenges in Healthcare

- **Data Security & Compliance:** Healthcare is the **most breached industry**, with average breach costs soaring to **$10.93 million** – highest among all sectors ibm.com. Protecting sensitive patient data against cyberattacks (ransomware, PHI breaches) while complying with regulations like HIPAA is a top concern. In fact, **41% of healthcare IT executives rank cybersecurity as their #1 initiative** resources.cerecore.net, as increasingly large breaches carry high costs and jeopardize patient safety ciodive.com.

- **Legacy Systems & Interoperability:** Many providers rely on aging EHR systems and fragmented clinical applications that do not easily share data. Nearly *60% of hospital CIOs* report that **legacy infrastructure impedes innovation** www2.deloitte.com. This lack of interoperability hampers care coordination and efficient data exchange, creating pain points in workflow

and analytics.

- **Evolving Care Delivery Models:** The rise of **telehealth and remote patient monitoring** since the pandemic means networks must support video consults and IoMT devices. Yet, most IoMT environments are rife with vulnerabilities – a 2025 study found **99% of healthcare organizations had IoMT devices with known exploited vulnerabilities** industrialcyber.co. Healthcare IT must enable "care anywhere" while securing a rapidly expanding attack surface of connected medical devices.

- **Operational Efficiency & Cost Pressures:** Healthcare organizations face tight margins and workforce burnout. They are challenged to **do more with less**, e.g. maximize existing IT investments (over half of CIOs prioritized optimizing current infrastructure in 2023) ciodive.com – while improving patient outcomes. Supporting new tech like AI-driven diagnostics and big data analytics is on the radar (32% of health CIOs cited AI/ML as top priorities ciodive.com), but cost and scalability concerns remainaudioeye.comaudioeye.com.

- **Regulatory Compliance & Risk Management:** In addition to HIPAA, healthcare IT must adapt to frameworks like SOC 2 and new interoperability mandates without disrupting care. Managing **continuous compliance** is difficult with limited staff audioeye.com. Meanwhile, downtime of clinical systems is unacceptable – every minute of EHR or PACS outage impacts patient care. Keeping infrastructure resilient and available 24/7 is a persistent challenge.

Strategic Technology Roadmap:

- High-availability segmented Wi-Fi and local area networks (LANs) for clinical systems

- Layered cybersecurity (zero trust, endpoint protection, Internet of Medical Things [IoMT] monitoring, immutable backups)

- Hybrid cloud storage for EHR backups and patient portals

- Flash storage for PACS (Picture Archiving and Communication System) imaging and fast data access

- Managed Security Operations Center (SOC), remote helpdesk, and after-hours support

Sales Conversation Starters:

What's your current approach to protecting patient data across all devices and locations?
Why you're asking: To uncover gaps in data protection across endpoints, especially mobile and remote access points where protected health information (PHI) can leak.

Do you have a plan in place for securing legacy medical equipment or IoMT devices?
Why you're asking: These are often unmanaged, unpatched, and introduce serious vulnerabilities — a huge entry point for ransomware.

When was the last time your EHR environment had a full disaster recovery test?
Why you're asking: To introduce recovery-as-a-service or backup testing — critical for uptime and compliance.

Are you still supporting everything in-house, or are you looking for help managing uptime and security?
Why you're asking: To tee up managed services as a scalable way to extend limited IT teams and reduce incident response times.

What's your policy when a remote physician logs in from home or a satellite facility?
Why you're asking: To prompt discussion about zero-trust access, multifactor authentication (MFA), and session controls.

Rebuttals & Objection Handling:

"We already have cybersecurity tools."
That's great. A lot of our clients do — we typically find the exposure comes from unmanaged IoMT or legacy endpoints, not desktops or servers. We can help close those last-mile gaps.

"We're not doing cloud right now."
Understood — hybrid works best for most hospitals anyway. We help you offload backups and non-PHI workloads to save cost without touching your core EHR.

"Our systems are too old to modernize."
We actually specialize in securing and extending the life of legacy systems through segmentation, support, and phased upgrades — no rip-and-replace needed.

VERTICAL: FINANCIAL SERVICES

Core Business and IT Challenges in Financial Services

- **Cybersecurity & Fraud Prevention:** Banks and financial institutions are prime targets for cybercrime. The **financial sector has the second-highest data breach costs** (~$5.9 million per incident on average, second only to healthcare) ibm.com. Cyber threats like ransomware, account takeover, and payment fraud continually evolve, pressuring IT to implement robust security across online banking, ATMs, and trading systems. Regulatory bodies (FDIC, OCC, NYDFS, etc.) enforce strict cybersecurity standards – failure to comply or a major breach can trigger heavy fines and reputational damage.

- **Regulatory Compliance & Risk Management:** Financial services must comply with a web of regulations: PCI-DSS for card payments, GLBA for data privacy, SOX, GDPR for global clients, and more. Ensuring audit-readiness and real-time compliance monitoring is a major challenge, especially when dealing with legacy systems not built for modern compliance needs. **Managing risks and compliance** is consistently ranked among top CIO concerns beckershospitalreview.com. Institutions also need to implement robust business continuity (e.g. disaster recovery, geo-redundancy) mandated by regulators to protect customer data and funds.

- **Legacy Core Systems & Modernization:** Many banks still run core banking on decades-old mainframes or COBOL-based systems. Nearly **6 in 10 banking technology leaders say legacy infrastructure is the top barrier to growth** www2.deloitte.com. These systems impede agility, making it hard to launch new digital products or integrate with fintech APIs. Modernizing or replacing core systems is complex and risky (given the volume of transactions and data), often resulting in a backlog of technical debt. Meanwhile, nimble fintech startups pressure banks to modernize faster or lose market share.

- **Digital Transformation & Customer Experience:** Today's customers demand seamless digital banking experiences – mobile apps, instant payments, personalized services – on par with tech giants. Banks need to leverage **cloud, AI, and big data** to deliver personalized insights and 24/7 services. However, integrating new digital platforms with existing IT is challenging. Also, data silos between departments (retail banking, credit cards, investment) hamper a unified view of the customer. Balancing innovation with security is a constant tension: e.g. deploying open banking APIs to partners while preventing data leaks.

- **Operational Efficiency & Cost Pressure:** Financial organizations face pressure to reduce IT costs and improve efficiency, especially as margins can be thin in a low interest environment. Many banks have sprawling branch networks or global operations, incurring high networking and infrastructure costs. **95% of banking executives say they are moving fully to the cloud by 2025** to gain efficiency pwc.com. Yet, migrating to the cloud and decommissioning data centers is a multi-year journey. Additionally, the sector faces talent challenges – specialized IT skills (mainframe experts, cybersecurity analysts, data scientists) are in short supply or expensive, prompting interest in managed services and automation to fill the gaps.

Strategic Technology Roadmap:

- Secure software-defined wide area networking (SD-WAN) to lower WAN costs
- Next-gen firewalls, multifactor authentication, user behavior analytics
- Cloud migration for front-end apps; refactor core over time
- All-flash storage for transaction systems with backup to encrypted cloud
- SOC-as-a-Service, governance-as-a-service, patching support

Sales Conversation Starters:

Are you currently using SD-WAN to reduce branch connectivity costs?
Why you're asking: To explore if they're still paying for expensive MPLS circuits, which can be replaced with smarter, more affordable connectivity.

What's your fraud detection system built on — is it behavioral or static?
Why you're asking: To identify an opportunity to layer AI-driven fraud analytics on top of their legacy security stack.

What would happen if your transaction system went down for 30 minutes?
Why you're asking: To create urgency around uptime, availability, and introduce redundant networking or failover storage solutions.

Have regulators ever asked for proof of breach detection or response?
Why you're asking: To set the stage for managed detection and response (MDR), continuous logging, and audit support.

Where are you on the journey to full cloud adoption?
Why you're asking: To place DDS as a guide through hybrid migration, cost optimization, and vendor management.

Rebuttals & Objection Handling:

"We already have a cloud strategy."
That's excellent. We're not trying to replace it — we typically save clients 15 to 25 percent by auditing what's over-provisioned or underutilized.

"We do security internally."
Perfect — we'd just supplement with 24/7 detection and response and offload compliance reporting. Most internal teams are focused on operations, not forensics.

VERTICAL: GOVERNMENT (STATE & LOCAL)

Core Business and IT Challenges in Government

- **Budget Constraints & Legacy Infrastructure:** Public sector IT departments operate under tight budgets and lengthy procurement cycles. Many agencies rely on **outdated, legacy systems** (some decades old mainframes or siloed databases) due to historical underinvestment. Upgrading or replacing these systems is difficult without significant funding, leading to accumulating technical debt. In a recent survey, **"modernizing outdated systems" was the #2 priority for city and county IT leaders, second only to cybersecurity** govtech.com. Legacy systems impede the adoption of new digital services and are expensive to maintain, consuming

funds that could otherwise go to innovation.

- **Cybersecurity Threats (Ransomware & Beyond):** State and local governments have been prime targets for ransomware and cyberattacks, given often limited defenses. *Nearly 69% of state and local governments reported being hit by ransomware in 2023* statetechmagazine.com – an astonishing rate, though it dropped to 34% in 2024 as some improvements took hold statetechmagazine.com. These attacks can cripple city services (e.g. 911 systems, utility billing) and expose citizen data. Yet, many municipalities still lack dedicated cybersecurity staff or adequate tools, relying on basic antivirus and aging firewalls. The need to **strengthen cyber resilience** (network security, incident response, citizen data protection) while facing resource constraints is one of the government's biggest IT challenges.

- **Citizen Digital Services & Experience:** There is growing public expectation for **"digital government"** – citizens want easy online access to services (permits, tax payments, license renewals) similar to private sector experiences. For governments, launching modern web portals or mobile apps means integrating various departmental systems (which often weren't designed to work together). According to NASCIO, *digital services now tie with cybersecurity as the top priority for state CIOs* nascio.org. Delivering these services requires overcoming siloed data, ensuring accessibility, and handling peak usage (e.g. election information sites during elections) – all on a limited budget and often with older tech.

- **Compliance and Data Privacy:** Governments must adhere to a host of regulations and standards – from CJIS for law enforcement data, HIPAA for public health records, to new privacy laws governing citizen data. Additionally, many states align with **NIST cybersecurity frameworks** or have their own mandates for data encryption, continuity of operations, etc. Ensuring compliance across all departments is challenging, especially when IT is federated. Public records laws also require data retention and public accessibility, meaning IT must retain massive amounts of data securely and make certain datasets open to the public. Achieving this balance of transparency and security is a fine line to walk.

- **IT Workforce & Resource Limitations:** Public sector salaries often lag behind the private sector, leading to **talent shortages** in critical IT roles. Experienced cybersecurity professionals or cloud architects are hard to attract or retain in government. Over 50% of local CIOs report difficulty in staffing IT positions with required expertise statescoop.com. This leads to

reliance on external contractors or leaving positions unfilled. At the same time, IT support needs are increasing (more devices, more apps), putting strain on small teams. The result is that many governments cannot fully utilize new technologies or proactively plan strategy; they remain stuck in a reactive mode, simply trying to keep aging systems running with minimal downtime.

Strategic Technology Roadmap:

- SD-WAN and campus fiber upgrades for high availability
- Firewalls, endpoint protection, access control per National Institute of Standards and Technology (NIST) guidelines
- Azure Government or AWS GovCloud for hosting and resilience
- Consolidated data storage and archival for compliance
- Shared IT services and co-op models to stretch budgets

Sales Conversation Starters:

What’s your plan if ransomware hits your 911 dispatch or water systems?
Why you're asking: To address business continuity and expose gaps in disaster planning.

Are you leveraging shared service models to reduce infrastructure cost?
Why you're asking: To suggest multi-agency support models (like shared backup or helpdesk) that reduce overhead and streamline support.

Have you mapped which departments are still running unsupported software?
Why you're asking: To uncover shadow IT or risk from old systems, and to offer lifecycle management.

Do you have grant-friendly partners for cybersecurity modernization?
Why you're asking: To frame DDS as procurement-aware and able to align to funding windows like E-Rate, CARES, or ARPA.

Are all of your public services available online, or are some still manual/paper-based?
Why you're asking: To pitch low-cost digitization of citizen portals and licensing/payments.

Rebuttals & Objection Handling:

"We don't have the budget."
Totally understandable. That's why we stagger deployments, align to grant cycles, and help bundle services across agencies to bring down unit cost.

"We just modernized our systems."
That's great — our role is to make sure those systems are secure, integrated, and monitored 24/7 so you get full value from them.

VERTICAL: EDUCATION (K–12 AND HIGHER ED)

Core Business and IT Challenges in Education

- **Cybersecurity and Student Data Privacy:** Schools and universities have become prime cyber targets. Alarmingly, the K-12 sector saw a surge in attacks – the number of school districts hit by ransomware **more than doubled from 2022 to 2023** varonis.com, and in 2023 lower education had the highest attack rate of any industry at 80%. On average, U.S. school districts face **five cyber incidents per week** ed.gov, ranging from phishing and ransomware to DDoS attacks during online exams. These incidents can lead to stolen student records, disrupted classes, or even weeks-long closures. Yet, K-12 IT teams are often small, with limited cybersecurity training, and budgets prioritizing classroom needs over IT security infrastructure. Ensuring student data privacy (as required by laws like FERPA) and keeping critical systems (learning management, SIS, testing platforms) secure is an urgent challenge with life-long implications for students' data.

- **Insufficient Infrastructure for Digital Learning:** The rapid shift to **1:1 computing and digital learning** (accelerated by the pandemic) has strained school IT infrastructure. By 2021, *90% of districts provided a device for every middle and high school student* edweek.org, a massive increase in connected devices. Many schools struggle with Wi-Fi dead spots, aging network switches, and internet bandwidth that wasn't designed for an entire campus streaming video or using online curriculum simultaneously. In higher

ed, universities must support not only student and faculty devices, but also research labs, dorm networks, and campus IoT (smart lighting, ID card readers) – all requiring robust networking. Outdated networks lead to slow or unreliable access, directly impacting learning (e.g. online testing interruptions, choppy virtual classes). Upgrading infrastructure and expanding broadband access (especially to underserved or rural schools) remains a core challenge.

- **Legacy Systems and Data Silos:** Educational institutions often have a patchwork of legacy administrative systems – separate databases for student information (SIS), learning management (LMS), library, HR, etc. These systems often do not interoperate, causing duplicated data entry and inconsistent information. For example, a change in a student's address might need to be updated in three or four systems. This inefficiency consumes staff time and can impact data accuracy for funding reports or student services. Moreover, some legacy software used by schools (for finance or grading) may be outdated and insecure. Tight budgets and fear of disrupting school operations make it hard to replace these systems.

- **Scaling and Supporting Remote/Hybrid Learning:** The pandemic forced a crash course in remote learning. Many districts and universities adopted platforms like Zoom, Google Classroom, or Canvas, but supporting hybrid models (mix of in-person and remote) remains a challenge. Teachers and students now expect digital access to resources 24/7. IT must maintain high uptime for e-learning platforms and often support a wide range of devices (school-issued Chromebooks, personal laptops, tablets, etc.). Providing effective IT support to students/faculty who may not be on campus (remote help desks, device troubleshooting) is a newer demand on school IT departments. Even post-pandemic, the flexibility of hybrid learning means schools need IT infrastructure that can accommodate sudden shifts to online instruction (e.g. during weather closures) without downtime.

- **Budget Constraints and IT Staffing:** Much like government, education faces chronic budget constraints. Funding for technology often comes from bonds, grants (like E-rate), or special budgets, which can be infrequent or restricted. This leads to cycles of feast-and-famine – e.g. a burst of device purchases without sustainable refresh funding. Additionally, **IT staffing in schools is limited** – a district may have just a handful of IT personnel supporting thousands of students and staff. In higher ed, certain IT roles (network engineers, security analysts) are hard to fill due to salary competition with industry. As a result, proactive planning and maintenance suffer; IT is stuck reacting to the most urgent fires (like systems down or

devices broken) rather than strategic improvements. Outsourcing and managed services are not yet as common in education as in other sectors, but the need is growing as tech complexity outpaces what small teams can handle.

Strategic Technology Roadmap:

- Wi-Fi 6/6E access points in every classroom, VLANs to separate traffic
- Web filtering, endpoint security, backups with disaster recovery
- Google Workspace, Microsoft 365, or cloud LMS integration
- Shared storage and automated backups across devices
- Managed support and training services for teachers and admin

Sales Conversation Starters:

Do your students have reliable Wi-Fi in every room?
Why you're asking: To justify network infrastructure upgrades (which are E-rate eligible) for device-heavy learning environments.

How do you handle support requests after school hours?
Why you're asking: To pitch a managed help desk or ticketing platform that gives teachers and students 24/7 coverage.

How long would it take you to recover from a ransomware hit?
Why you're asking: To highlight backup, business continuity, and testing gaps.

Are your LMS, SIS, and email systems integrated in any way?
Why you're asking: To position integration services and eliminate time-wasting redundancies.

Are your teachers receiving professional development on these tools?
Why you're asking: To offer training services or EdTech partner content that ensures full ROI from past tech investments.

Rebuttals & Objection Handling:

"We don't have money for this right now."
Completely fair. We work within E-rate and grant cycles — we also help bundle things to eliminate overlap across departments.

"We just bought new Chromebooks."
Perfect. We'll help make sure your Wi-Fi, filtering, and backup environment can scale with them so you don't see slowdowns or gaps.

VERTICAL: MANUFACTURING

Core Business and IT Challenges in Manufacturing

- **Legacy OT Systems and IT/OT Convergence:** Manufacturers often run legacy operational technology (OT) – PLCs, SCADA systems, old Windows machines on factory floors – that were not designed with modern networking or security in mind. These systems control production lines and are extremely sensitive to downtime, so they are seldom patched or changed. Integrating these with modern IT (for data collection or control) is a major challenge. Many plants have **"air-gapped" networks** historically, but digital transformation requires bridging that gap (Industry 4.0 initiatives, IoT sensors feeding data to analytics platforms, etc.). The result is a vastly expanded attack surface and complexity: engineers who understand OT may not know IT networking, and vice versa. This convergence is cited as a top concern – **cyber threats have resurfaced as a top concern for manufacturers, largely due to vulnerabilities in OT systems and proliferation of IoT devices** protiviti.com.

- **Downtime and Reliability Concerns:** In manufacturing, **downtime is incredibly costly** – production stoppages directly hit the bottom line. For example, the auto industry loses an average of **$22,000 per minute of downtime** on the production line ibm.com. This creates a critical need for reliable systems and quick recovery. Aging equipment or network outages can halt operations. IT/OT incidents (like a server crash that halts an automated line, or a ransomware attack that encrypts CNC machine controllers) aren't just inconveniences – they stop product output, delay shipments, and can break supply commitments. Thus, manufacturers require highly resilient infrastructure and fast incident response. Disaster recovery and business continuity plans are often weak in smaller manufacturers, so improving that is a challenge.

- **Supply Chain Integration and Data Silos:** Modern manufacturing operates in complex supply chains that demand tight integration – from suppliers of raw materials to distributors of finished goods. Many manufacturers struggle with siloed systems (ERP, MES, inventory, logistics, etc.) that don't seamlessly share data. This leads to inefficiencies like excess inventory "just in case," slow responses to supply chain disruptions, and difficulty in implementing Just-In-Time (JIT) manufacturing. Additionally, data is often trapped at individual sites – e.g. each factory might have its own database – hindering enterprise-wide visibility. Consolidating and integrating data for real-time supply chain monitoring and predictive analytics (e.g. predicting machine failures or supply delays) is a key challenge.

- **Quality Control and Traceability Requirements:** In industries like automotive, aerospace, food, or pharma, there are stringent requirements for tracking every component/batch and maintaining quality records for compliance and recalls. This puts pressure on IT systems to collect and store massive amounts of data from the production process (sensor readings, test results, origin of each part). Many manufacturers still rely on paper-based or semi-automated systems for this, which are error-prone and not scalable. Implementing digital traceability (e.g. scanning at each station, centralized databases, analytics to detect quality issues) requires investment in IoT devices, reliable networks on the shop floor, and large storage/processing capabilities – all of which can be daunting to deploy and integrate with existing processes.

- **Security Threats and IP Protection:** Beyond ransomware, manufacturers face threats like industrial espionage – theft of intellectual property (designs, formulas, CAD models) – often by nation-state or competitor-aligned actors. The manufacturing sector saw a significant increase in breach costs, with the average breach costing **$5.56 million in 2023, up 18% from the previous year** ibm.com. This reflects not just IT system compromise but the high value of stolen trade secrets. Many manufacturing firms have limited cybersecurity staff, and their focus historically was on safety and physical security, not cyber. Now they must contend with sophisticated attacks on both IT and OT (e.g. the infamous NotPetya attack that hit Maersk's shipping operations, or attacks on automotive companies stealing EV designs). Protecting proprietary data and ensuring malware doesn't disrupt production are paramount concerns that require new strategies and tools many manufacturers haven't used before.

Strategic Technology Roadmap:

- Industrial Ethernet and ruggedized switching, VLAN segmentation
- OT-aware firewalls, anomaly detection for production traffic
- Cloud for ERP and analytics, edge compute for factory sensors
- Secure storage of quality control and sensor data
- Remote monitoring, maintenance, and managed detection and response (MDR)

Sales Conversation Starters:

How do you detect and respond to cyber threats on your shop floor or OT systems?
Why you're asking: To expose risk where most manufacturers are weakest — production network security.

What would it cost if your production line went down for 30 minutes?
Why you're asking: To quantify the financial urgency around uptime, and justify disaster recovery and redundancy.

Are your IT and OT networks segmented or flat?
Why you're asking: To open a discussion around reducing risk of cross-contamination or malware spread.

Is your production data tied into your enterprise resource planning (ERP) or analytics platforms?
Why you're asking: To reveal inefficiencies and set up a conversation about integrating machine data for visibility.

Who supports your legacy PLCs and automation gear — is it still the OEM?
Why you're asking: To offer support and maintenance alternatives if the manufacturer no longer covers those assets.

Rebuttals & Objection Handling:

"Our machines are too old to integrate."
That's exactly where we come in — we deploy non-invasive overlays like sensors or secured gateways to modernize without replacing.

“We already back everything up.”
That’s great — are your backups offsite, immutable, and tested against cyber scenarios like ransomware on OT systems? Most aren’t.