ALWAYS
LEADING

Advisory Services

SCADA Vulnerability Assessment

SENTINEL®

TABLE OF CONTENTS

General Contact Information

CITY OF AURORA CONTACT INFORMATION

Ted Beck
Chief Information Security Officer
City of Aurora
Aurora, IL 60505
Office: 630.256.5863
tbeck@aurora-il.org

SENTINEL CONTACT INFORMATION

Steve Tyriver
Sr. Sales Executive
2550 Warrenville Rd.
Downers Grove, IL 60515
Office: 630.769.8583
styriver@sentinel.com

Rick Spatafore
Manager, Advisory Services
2550 Warrenville Rd.
Downers Grove, IL 60515
Office: 630.786.8062
rspatafore@sentinel.com

Darrell Vydra
Strategic Business Advisor
2550 Warrenville Rd.
Downers Grove, IL 60515
Office: 630.769.4193
dvydra@sentinel.com

NEVER FOLLOW

At Sentinel we've always taken the lead. Since 1982, Sentinel Technologies has been recognized as a premier business technology services provider dedicated to delivering the highest quality IT solutions, consulting, customer service and support. Even as our services have spanned generations of technology, Sentinel has stayed at the forefront of IT developments and maintained a singular focus on providing practical and innovative solutions. With single-source accountability, Sentinel processes and teams can efficiently address a range of IT needs – from communications, to data center, to cloud and managed services. Our proven success has allowed us to expand from our original charter of providing technology maintenance services to our current standing as one of the leading IT services and solutions provider in the U.S.

By aligning with many of today's global technology leaders including Cisco, Microsoft, EMC, NetApp and VMware, Sentinel solutions achieve tangible results.

When it comes to achieving a tangible ROI and sustainable performance from your IT environment, Sentinel takes the lead!

Headquartered in Downers Grove IL, Sentinel Technologies has independently managed offices in eleven locations: Chicago IL, Springfield IL, Milwaukee WI, Phoenix AZ, Ann Arbor MI, Lansing MI, Grand Rapids MI, Crystal Falls MI, Atlanta GA, and Denver CO, allowing us to service our customers both nationally and internationally.

SENTINEL TECHNOLOGIES
HEADQUARTERS FACILITY
DOWNERS GROVE, IL

PHOENIX
AZ

GRAND RAPIDS
MI

ANN ARBOR
MI

LANSING
MI

CHICAGO
IL

SPRINGFIELD
IL

MILWAUKEE
WI

ATLANTA
GA

DENVER
CO

SERVING CUSTOMERS
NATIONALLY AND INTERNATIONALLY

ALWAYS INVOLVED

At Sentinel, we understand technology is a "living, breathing" organism that is continually changing and evolving to better meet the demands of business. We call it "Living Technology". However, the term not only applies to how technology adapts to better serve business, it also describes our culture at Sentinel. Because here, we are "living technology" everyday — it's part of our DNA. Customizing technology to enhance the companies we serve is our life. Therefore, we remain dedicated to always be looking forward in discovering how the latest technological advancements can translate into tangible benefits for our customers. For us, "always involved" means providing the complete solution; from inception – to production turn-up of the solution – to post-install support model.

VISION | DESIGN | PRODUCT | IMPLEMENTATION | DOCUMENTATION | TRAINING | SUPPORT

THE COMPLETE PACKAGE

Sentinel provides our customers with a comprehensive solution: vision, design, product, implementation, documentation, training and support.

VISION
DESIGN
PRODUCT
IMPLEMENTATION
DOCUMENTATION
TRAINING
SUPPORT

COMPREHENSIVE SOLUTIONS

ANY INDUSTRY

Sentinel's services span the range of business verticals in mid-market, upper mid-market and enterprise level organizations. Companies in the Healthcare, Financial / Banking, Government, Education, Legal, Utilities, and Manufacturing verticals have taken advantage of Sentinel's ability to take either full responsibility or act as a supplemental contributor to our customer's business technology initiatives.
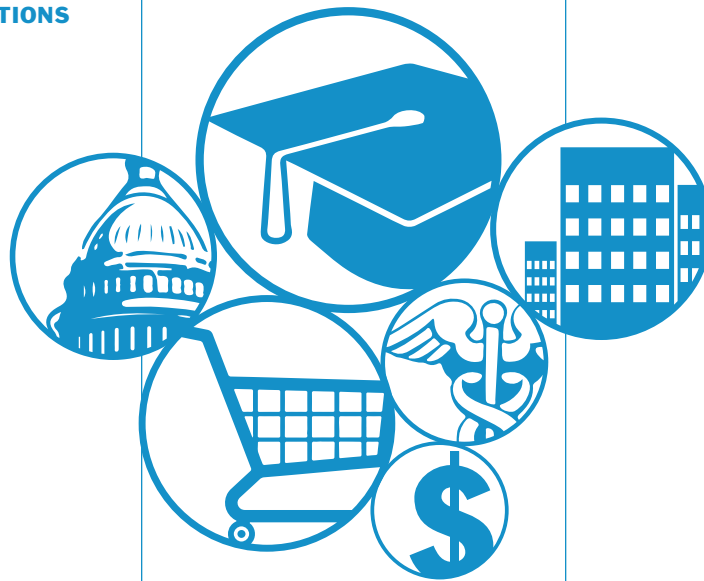
DIVERSE INDUSTRIES

THE SENTINEL DIFFERENCE

Sentinel applies an extraordinary breadth of technical solution expertise to design, sell, deploy and support our customer's business technology needs. Our unwavering commitment to thought leadership and customer satisfaction maximize both the value of technology investments and its impact to the business.

500
EMPLOYEES

HIGHLY-TRAINED

SENTINEL CORE SOLUTIONS

Sentinel understands your business is in constant motion. We take the initiative to make solutions happen that drive your business forward.

To jumpstart solution development, we perform analyses ranging from a rapidly-delivered "technical review" focused in a specific technology to an in-depth audit and analysis of IT processes, continuity plans, and compliance.
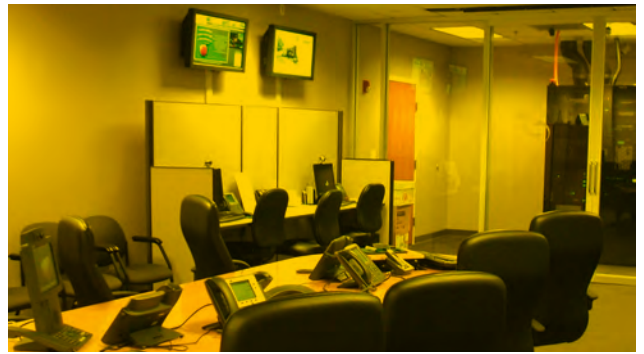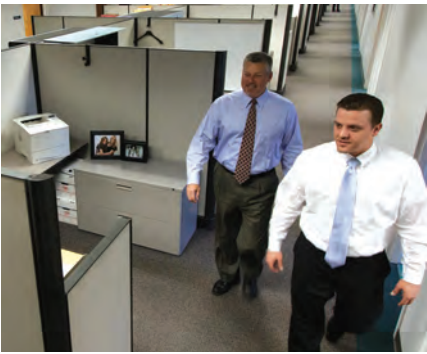
During solution development, our LMC methodology – Location/Management/Consumption – uncovers the preferred solution Location (customer site or colocation), Management (customer or Sentinel) and the financial Consumption model (CAPEX/OPEX).

If you need assistance evaluating your LMC, Sentinel Advisory Services determine how to best balance your computing workloads – whether cloud, private cloud or hybrid cloud – based on business needs.

Once the direction is set, highly skilled Sentinel teams provide technology solutions and products that keep you always engaged and always connected:

**COMMUNICATION | DATA CENTER | CLOUD & MANAGED SERVICES**

ALWAYS ENGAGED When your needs require the design, sale and implementation of a technology solution, Sentinel project teams are always up to the task! We combine the strength of a seasoned technical design team with highly-trained field engineers and a world-class Project Management Organization. The Sentinel team remains "always engaged" throughout the life of the project to ensure the highest quality solution is delivered on time and on budget.

- Unified Communications
- Collaboration Tools
- Mobility/Wireless
- Conferencing
- Unified Contact Center
- Software Defined Networking
- Video Signage and Security
- Unified Computing

- Private and Hybrid Cloud
- Big Data
- Virtualization – Network/Desktop
- High Performance Storage
- Backup and Recovery
- Cyber Security – Network/Email/Web
- Data Center Design
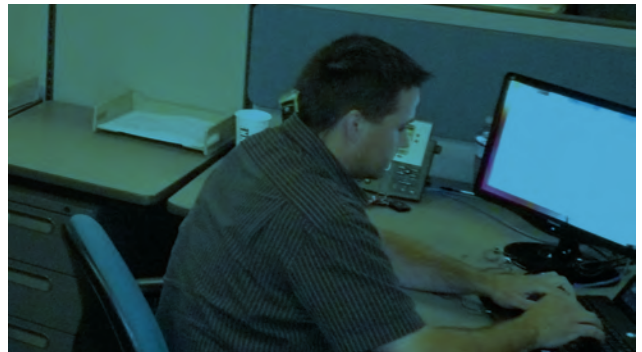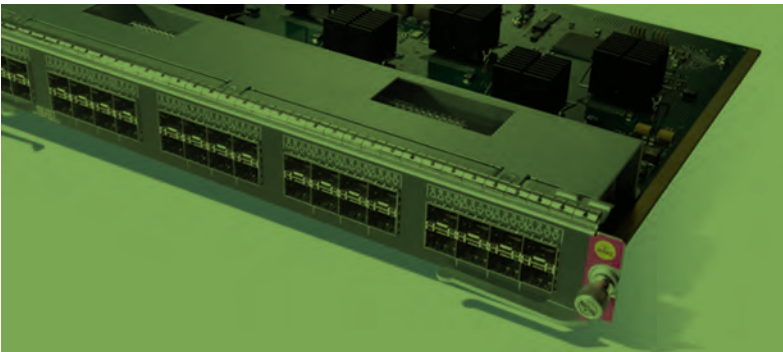
ALWAYS CONNECTED When customers seek to maximize the lifespan of their current systems or desire a more efficient model to deliver IT, Sentinel's support teams and cloud services make certain you are "always connected". • Maximizing the availability of current systems through consulting, managed services, maintenance, monitoring and staffing has always been a cornerstone of our business. • Sentinel's CloudSelect® offerings are built on a high-availability platform that delivers cloud or hybrid cloud computing solutions through a customized, cost effective model.

- Sentinel CloudSelect® – Compute, Storage, Backup/DR, Voice, Wireless, Colocation
- Fully Managed Solutions
- Complete System Monitoring and Support
- IT Processes, Continuity Plans, and Compliance
- Supplemental Staffing
- Technology Assessment and Advisory Services
- Maintenance and Support Contracts
- Sentinel High Availability Network Support (HANS™)
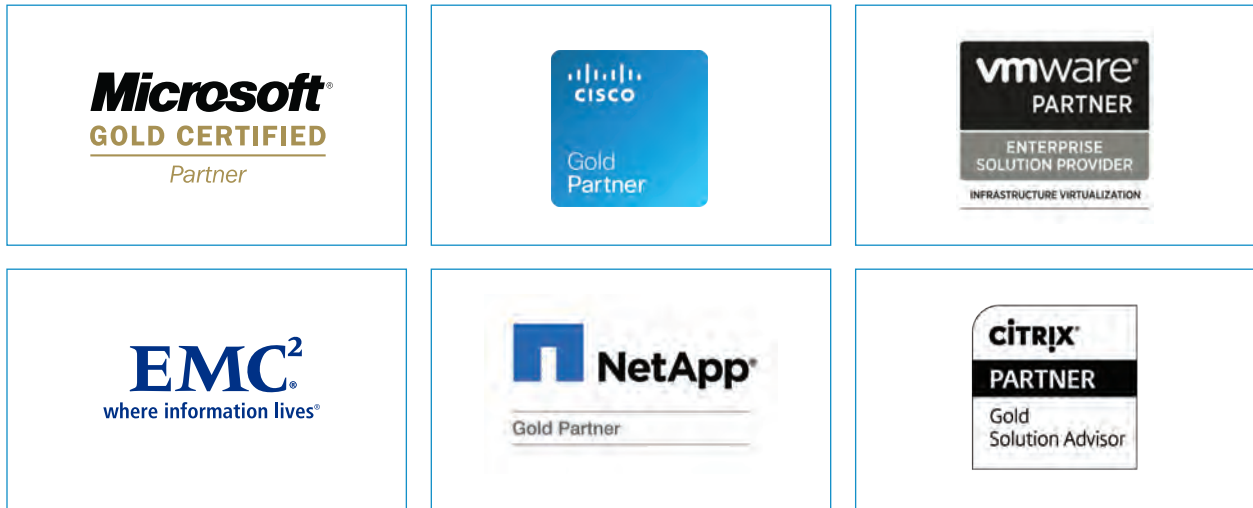- Outsourced Support Models

Sentinel recognizes that the quality of our solution partners directly affects the quality and value of the solutions we deliver to our customers. Our strategy is to partner with the best in the industry and obtain the highest level of certification available from all our key partners which, in turn, enables us to buy at the best price available. This ensures that we not only have the technical and business expertise to deliver on our promise, but we can do so in the most cost-effective manner possible.

Sentinel is proud to maintain the following organizations as our strategic business partners:

Key Partner Certification Levels

Microsoft GOLD CERTIFIED *Partner*

CISCO Gold Partner

vmware PARTNER ENTERPRISE SOLUTION PROVIDER INFRASTRUCTURE VIRTUALIZATION

EMC² where information lives®

NetApp® Gold Partner

CITRIX PARTNER Gold Solution Advisor

Valued Partners

nimble

APC by Schneider Electric

IBM

Elite Partner hp

VCE THE VIRTUAL COMPUTING ENVIRONMENT COMPANY

BridgeWave COMMUNICATIONS

DragonWave

CERAGON

Cambium Networks

Symantec

commvault

solarwinds

GOVERNMENT

Chicago Housing Authority
City of Ann Arbor
City of Joliet
City of Naperville
City of Phoenix
City of Rockford
City of Tucson
Cook County
DuPage County
Genesee County
Gila River Indian Community
Maricopa County
State of Illinois
Tohono O'Odham Gaming Ent.
Village of Downers Grove
Village of Huntley
Village of Palatine
Village of Wheeling
US RRB

EDUCATION

Ann Arbor Public Schools
Arizona State University
Champaign CUSD 4
Chicago City Colleges
Chicago Public Schools
Chippewa Valley Schools
Eastern Illinois University
Glendale School District
ITT Technical Institute
Joliet Junior College
Kalamazoo College
Loyola University Chicago
New Trier High School
Perspectives Charter Schools
Roosevelt University
Schaumburg SD 54
University of Chicago
University of Michigan
Washtenaw Intermediate School

HEALTHCARE

Access Community Health
Advocate Healthcare
Altarum Institute
Cancer Treatment Centers of America
CFNI
Children's Memorial
Cook County Hospital
DuPage Medical Group
Fort Defiance Indian Hospital
Gila River Healthcare Corporation
Hospice of Northeastern Illinois
Midwest Palliative & Hospice CareCenter
Northwestern Memorial Hospital
Passavant Area Hospitals
Resurrection Healthcare
Rush Presbyterian St. Luke's Hospital
Sarah Bush Lincoln Health Center
Silver Cross Hospital
Sparrow Health Systems
University of Wisconsin Hospitals

MANUFACTURING

Agro-Culture Liquid Fertilizers
AM Castle
Amcol
Chicago Bridge and Iron–CB&I
Danfoss Inc
Gardner Denver Inc.
GATX
Kohler Co.
Komatsu Corporation
Kone
Nalco Company
Panduit
Rustoleum Corporation
Steelcase, Inc.
Tate & Lyle
Tenneco Automotive

BANKING & FINANCIAL SERVICES

ABN Amro
Acquity Group
American Express
Banco Popular
BMO Harris Bank
Chicago Trading Company Holdings
Citibank
Euclid Insurance
First Analysis
First Midwest Bank
Fortune Brands
Michigan State Univ. Federal Credit Union
OptionsXpress
Optiver
PPM America LLP
Wheels, Inc.

RETAIL

Art Van Furniture
Apothecary Shop Inc.
Brookfield Zoo
Capital Fitness
Casino Arizona
Coinstar
Crescent Crown
Dot Foods
East Bank Club
Field Museum
Koch Foods
National Van Lines
Personalization Mall.Com
Redbox Automated Retail
SC Johnson & Sons Inc.
Sears

PROFESSIONAL SERVICES

Acxiom Corporation
A.J. Gallagher
AT Kearney
Duff and Phelps, LLP
HPR Partners
Locke Lord Bissell and Liddell
Mayer Brown Rowe & Maw
Reyes Holdings
Schiff Hardin LLP
Unitrin Data Systems
Videojet
Zenith Administrators

UTILITIES

Arizona Electric Power Cooperative
Central IL. Water, Light and Power
City Water Light & Power–Springfield, IL
Exelon
We Energies–Wisconsin

REAL ESTATE

Ambitech Engineering Corp.
AMLI Residential Properties
Bentley Forbes
CB Richard Ellis
Equity Residential
GITC–Greater Illinois Title Company
LeaseCorp
Marmon Group
NAI Hiffman
NPL Construction
US Equities

ALWAYS KNOWLEDGEABLE

At Sentinel Technologies, we are committed to being at the forefront of thought leadership. Our strategy is to partner with the best in the industry. We then obtain the highest level of solution specialization available from these key partners.

SPECIALIZATIONS | CERTIFICATIONS

Company Specialization / Certifications

The following Manufacturer Technology Certifications recognize Sentinel's expertise within each of our manufacturer partner's technologies:

SPECIALIST DESIGNATION FROM CISCO IN:

- Master Collaboration
- Master Security
- Master Cloud & Managed Services
- Master Cloud Builder
- Cisco Powered Cloud Services
- Cisco Powered Managed Services
- Advanced Routing & Switching
- Advanced Data Center Architecture
- Advanced Borderless Network
- Advanced Content Security
- Advanced Unified Fabric
- Advanced Wireless LAN
- TelePresence Video Advanced Plus
- Cisco Partner Support Services
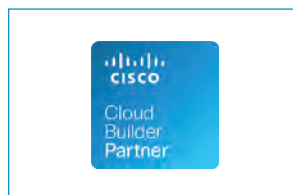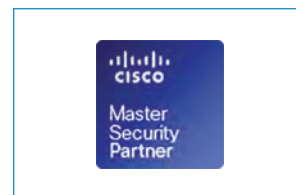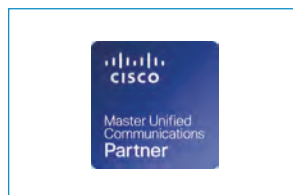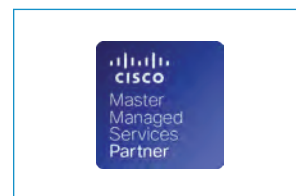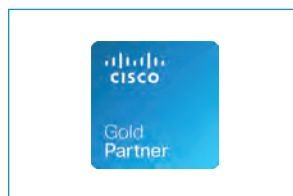
ADVANCED TECHNOLOGY PARTNER (ATP) FROM CISCO IN THE FOLLOWING AREAS:

- Application Centric Infrastructure (ACI)
- Identity Services Engine (ISE)
- Cloud Partner – EMC, NetApp, Microsoft and VMware
- Unified Contact Center Enterprise
- Customer Voice Portal
- Advanced Internet of Things – Safety & Security Specialized Partner
- VBlock

MICROSOFT AUTHORIZATIONS:

- Gold Management and Virtualization
- Gold Communications
- Silver Midmarket Solution Provider
- Silver Server Platform
- Silver Messaging
- Silver Data Center

EMC AUTHORIZATIONS:

- Premier Partner Level
- Velocity Advantage Partner
- Authorized Service Partner
- Consolidate Specialty
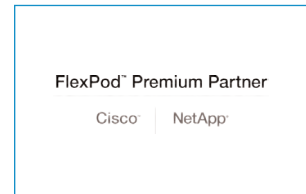- BRS Specialty
- VCE Design & Installation

VMWARE AUTHORIZATIONS:

- Solution Provider Enterprise Partner
- Infrastructure Virtualization
- Business Continuity
- Desktop Virtualization

NETAPP AUTHORIZATIONS:

- Gold Level Partner
- Virtualization Specialized
- FlexPod Specialized
- NetApp Support Services Certified
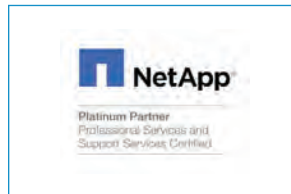
SSAE16 AUDITOR CERTIFIED

50+
COMPANY
CERTIFICATIONS

Individual Technical Certifications

Sentinel makes substantial investments in keeping the training of our technical, sales, and design team members up to date to ensure we have the technical and business expertise to deliver on our promise.

Sentinel possesses over 2,400 technical certifications from our manufacturer partners. A sampling is below.

NETWORK AND DATA CENTER

584 CISCO CERTIFICATIONS

- CCIE – 28, CCDP – 12, CCDA – 22, CCNA – 146, CCNP – 72, CCSP – 2, Cisco Data Center – 62
- 50+ Unified Communications Specialist Certifications
- 100+ Sales and Design certified

44 EMC CERTIFICATIONS

- ASN Partner – certified for complete installation and implementation of the entire EMC portfolio
- Storage / Cloud / Big Data / Data Protection / Security / Content Management / Converged Infrastructure

OTHER PROFESSIONAL CERTIFICATIONS

| 87 Certifications | 18 Certifications | 16 Certifications | Certified Professional |

2,400+ INDIVIDUAL CERTIFICATIONS

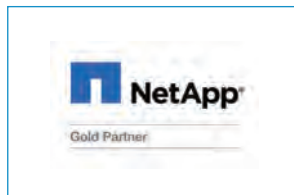## MAINTENANCE AND REPAIR

- **HP –** 698 certifications (workstations, notebooks, server, printer etc)
- **DELL –** 229 certifications (server, storage, notebook etc)

- **LENOVO –** 86 certifications (desktop/laptop)
- **LEXMARK –** 34+ certifications (printers)
- **PC SUPPORT –** 163 Certifications (workstations, notebooks, server, printer etc)

CUSTOMER SATISFACTION QUALIFICATIONS

- Recipient of Advocate Healthcare Corporate Partner Award
- Recipient of AM Castle Supplier of the Year Award

- Recipient of Illinois Auto Auctions Inc. Outstanding Performance Award
- Recipient of hundreds of letters from customers recognizing outstanding contribution and performance

TECHNOLOGY PARTNER AWARDS

- Recipient of Cisco Customer Satisfaction Excellence Award for seven straight years
- Best year over year performance in Central Operations District
- Cisco Southwest Territory Partner of Year for three consecutive years
- Best year over year performance U.S. Regional VAR
- Southwest Territory Enterprise Networks Cisco Partner of the Year
- Best of AVVID Show Award in Customer Satisfaction for Sentinel's IQ for Education application suite for Cisco IP phones
- Awarded Cisco "Global IP Communications Partner of the Year"
- Southwest Territory Security Cisco Partner of the Year

- Awarded Cisco "Great-Lakes-Region – Partner of the Year"
- Southwest Territory Data Center Cisco Partner of the Year
- Awarded Cisco "Central Region IP Communications – Top Partner"
- Awarded Cisco "Central Region Partner Summit - Partner of the Year"
- Awarded Cisco Wireless "Excellence in Partnership"
- Six time HP Service Excellence Award Winner
- Excellence in Cisco Collaboration Architecture Award - Cisco U.S/Canada Partner Summit
- 2014 EMC Quality Service Award
- Outstanding Customer Satisfaction Award – Cisco U.S/Canada Partner Summit
- Cisco 2015 SLED Partner of the Year

ALWAYS MOTIVATED
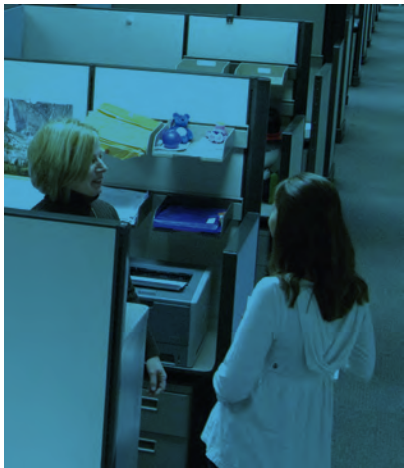
Since the inception of Sentinel in 1982, the Company has abided by a simple philosophy – "happy and motivated employees equal happy customers". To that end, Sentinel has been vigilant in creating a work environment that encourages creativity, fosters growth, and rewards success.

Sentinel has received independent recognition for their ability to create an outstanding work environment and has been recognized as a "Best Place to Work" by the Chicago Tribune, Crain's Chicago Business, and AZCentral.com. The Company has also received hundreds of letters of recommendation from national and international customers for the outstanding support delivered by the Sentinel team.

Sentinel is proud to have been recognized as a "Best Place to Work" in the U.S. Midwest and Southwest regions. In the Midwest, Sentinel has been named a Top 100 Workplace by the Chicago Tribune for four consecutive years and also recently received recognition as a "Top 100 Workplace" for Arizona. In both cases, Sentinel was selected based on employee feedback compared to other companies in the region. Sentinel has also been recognized as a "Best Place to Work" by Crain's Chicago Business.

ALWAYS EFFICIENT

Sentinel is committed to producing high quality results as efficiently as possible for our customers. This is why we have embraced professional project management as the cornerstone of every project we undertake.

Sentinel's approach to Project Management incorporates a unique blending of both Strategic and Tactical monitoring and control techniques thus realizing the "how" of the work we perform. We have achieved this via formal planning techniques and sophisticated virtualized work-flows – "Guides to Assembly" which are real mechanisms that help guide project participants through communication channels and work assignments in order to realize task sequence, manage risk, and avoid re-work.

Sentinel's Enterprise Project Management Organization (EPMO) has a large core of PMP certified Project Managers who work with our customer and the assigned Sentinel technical project team to ensure we deliver on our promise. Our PM's have the professional certification and a strong technical background necessary to provide the management and guidance required to keep projects on time and on budget. Sentinel's EPMO utilizes tools such as Microsoft SharePoint Portal and Organizational Project Management Maturity Model (OPM3) along with basic blocking and tackling around issues like defects, root cause analysis, and risk mitigation to deliver optimum results.

For projects requiring project management (typically 80+ hours of technical services), Sentinel will adhere to the following guidelines:*

1 INTRODUCTION CALL

Within two business days of PMO notification, a Sentinel Project Manager will contact you for an introduction and to answer any questions you might have.

2 SCHEDULE EXTERNAL KICK-OFF

Within three business days of the Introduction Call, the Project Manager will call again to arrange a time and date to set up an initial "Customer Kick-Off" meeting with you and your Team.

(Between the Introduction Call and the subsequent Kick-Off Meeting, Sentinel assembles the project team for a Internal Kick-Off or formal review of the project's characteristics, inherent risks, and to perform formal planning and scheduling.)

3 KICK-OFF MEETING (CUSTOMER SITE)

Ten business days from the Introduction Call, the Customer Kick-Off will be held at the customer location.

The purpose of this meeting:

- Acceptance of Initiation Documentation, Risk Review and Top Down Structured Planning (TDSP)
- Walk though *(if needed depending on Solution purchased)*
- Scheduling of Blueprint Meeting(s)

As a result of this session, a detailed *final* work schedule *(MS Project)* will be created and used to track and control the project. Once completed and resources are scheduled, the Design phase can commence.

DETAILED WORK SCHEDULE

SENTINEL PM SLA TO KICK-OFF

INITIATION

PMO PROJECT NOTIFICATION

PM ASSIGNMENT

INTRODUCTION CALL

PLANNING (INTERNAL)

PLANNING / SCHEDULING

KICK-OFF MEETING

KICK-OFF SCHEDULE CALL

KICK-OFF MEETING (SCHEDULING / RISK REVIEW)
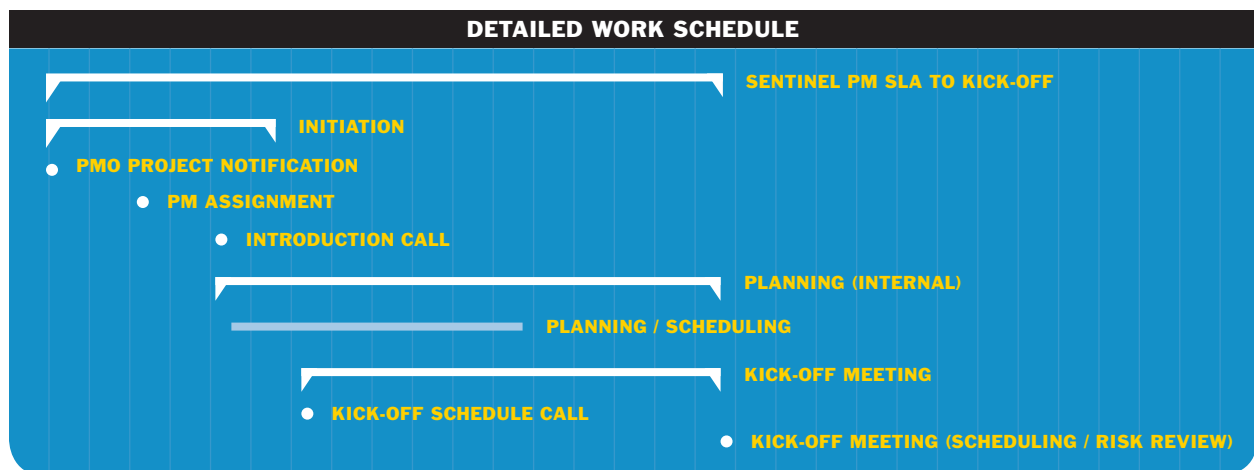
★ Depending on the size and complexity of the project, planning sessions and the subsequent creation of schedules and other administrative project management artifacts such as risk plans, communications plans, and resource scheduling, can extend out from the intervals shown above.

Project Management process may be customized based on factors such as project size, urgency or complexity.

At Sentinel, environmental protection is a management responsibility as well as the responsibility of every employee. Our environmental protection policy addresses all aspects of the corporation's operations which can potentially impact the environment. In creating this policy, we have taken into account the following factors:

- Compliance with applicable laws, regulations, and standards concerning environmental protection

- Establish corporate environmental objectives and targets

- Minimize the environmental risks to our employees and the communities in which we operate

- Promote employee awareness of environmental concerns, actions, and responsibilities

- The efficient use of energy and materials in our operations

- Reduce/ eliminate waste through recycling and responsible disposal

- Continuous improvement and monitoring of the current environmental policy

Further, Sentinel suppliers are encouraged to develop an Environmental Policy and Environmental Management System by following the Environmental Protection Agency guidelines.

Standing at the apex of Sentinel's awards and certifications is its SSAE 16 Service Organization Control (SOC) 2, Type II Attestation which has been undertaken annually by the nationally-renowned auditing firm Plante Moran, PLLC for the past three years. The SOC 2, Type II attestation is the highest and most rigorous in the SSAE 16 portfolio of audits, evaluating Controls and Processes that encompass the Five Trust Service Principles of Security, Availability, Processing Integrity, Confidentiality and Privacy.

Why should this matter to you? The SSAE 16 attestation provides independent validation and assurance that Sentinel is in compliance with best practices regarding items of critical importance to you -- security, confidentiality, data protection, project management and IT strategic solutions, to name a few. If you are seeking consulting or services support for your IT environment, the SOC 2, Type II attestation should be one of the most important factors in your evaluation.

The SSAE 16 Attestation is a standard that was created by the American Institute of Certified Public Accountants (AICPA) in 2010 to replace the SAS 70 certification process, and expand reporting to the effectiveness of a service organization's controls relating to operations and compliance.

Executive Summary

The City of Aurora has engaged Sentinel to provide an SCADA Vulnerability Assessment of the current Water Department infrastructure and provide recommendations that are based on a strategic approach.

The strategic assessment approach aligns overall organizational goals and objectives with technology recommendations. Sentinel will meet with key organization stakeholders to gain insight into current challenges as well as future initiatives. This process will pave the way for the rest of the assessment and provide guidance for the analysis phase of the engagement.

Sentinel will gather information about the current Water Department SCADA infrastructure, topology, devices, and configuration to review it for technical best practice adherence and alignment with National Institute of Standards and Technology (NIST) Special Publication 800-82 Rev.2 – Guide to Industrial Control Systems (ICS) Security. A prioritized list of recommendations will be presented to the organization and linked to the key initiatives that are defined in prior phases.

The goal of the assessment is to provide a comprehensive analysis and objective review of the current implementation and provide insight into any future changes that should be made. Although assessments will cover all areas outlined in this proposal, the following areas will be specifically focused on as part of the engagement:

- How City of Aurora's Water Department infrastructure aligns with NIST Special Publication 800-82.

As a follow-up to the assessment engagement, Sentinel can provide remediation services for those objectives the City wishes to pursue and remediate further. Sentinel appreciates the opportunity to provide these services to the City and looks forward to reviewing the results with the team.

Assessment Services Overview

The assessment will provide actual (as-built) documentation, analysis, and recommendations. Sentinel follows a multi-phased approach with assessments as outlined below:

GATHER

- Gather Organizational Goals & Objectives via Interviews
- Baseline Information Gathering via Sentinel Tools
- Detailed Documentation of the Scoped Infrastructure
- Summary of Equipment, Configs, Diagrams, Lifecycle & Maintenance Information

ANALYZE

- Organizational Goal and Objective Focused
- Longer-Term, Best Practice Alignment
- Informal Technical Gap Analysis
- Immediate Fix Changes with Device-by-Device Review
- Validation of Configurations, Versions, Security Fixes

RECOMMEND

- Align to Stakeholder Organizational Goals/Objectives
- IT Roadmap and Budgetary Planning Assistance
- Sentinel and Industry Best Practices Recommendations
- Prioritized Analysis Criteria (Impact, Likelihood, Risk, etc.)
- Technical Background and Contextual Information Provided

Phase One - Information Gathering

The first phase of the assessment is an information gathering engagement that will provide detailed information about the current infrastructure. Sentinel will meet with the City's stakeholders through an interview session to gather key objectives and goals for the organization. This information will be used to provide perspective and influence on the analysis and recommendations in later phases of the assessment.

A solid security plan goes beyond technology and addresses the entire cybersecurity lifecycle of an organization. During the stakeholder interview session(s) a Sentinel Strategic Advisor will review the National Institute of Standards and Technology (NIST) Special Publication 800-82 (Revision 2) Guide to Industrial Control Systems (ICS) Security. The NIST SP 800-82 framework provides a comprehensive approach to protecting critical infrastructure.

Technical information will be gathered using the existing access credentials to perform a discovery with custom Sentinel tools and manual efforts. The documentation produced by Sentinel will include connectivity information about the infrastructure as well as any additional information discovered for ancillary devices. This documentation provides the baseline information needed by the Sentinel team to analyze the respective technology areas in future phases of the engagement.

Phase Two - Analysis

The second phase of the assessment includes a thorough analysis of the collected information from phase one and performs a technical gap analysis between the current implementation and a best practice implementation in several areas. A strategic is performed during this phase and are outlined as follows:

STRATEGIC ANALYSIS

The strategic analysis identifies actionable items that factor in to the City's organizational requirements, objectives, and goals. This option allows the recommendations to be tailored for the City, thereby providing influence and perspective in other areas such as growth, performance, and resiliency, using a holistic approach to ensure the most reliable and functional environment possible. Stakeholder interviews will be performed during the information discovery phase to identify the goals and objectives that will influence the analysis and subsequent recommendations in the final phase of the assessment.

TACTICAL ANALYSIS

The tactical analysis provides immediate benefit, such as improving reliability, stability, and performance. This approach identifies common misconfigurations and software versions which are known to have security vulnerabilities. For this level of analysis, the City will be responsible for selecting areas of each respective technology area (including devices) for Sentinel to review during the presales phase. For security assessments a security vulnerability scan will be performed against selected devices and a prioritized risk report will be provided. The tactical approach analysis does not take into account organizational goals and objectives. For this project, there will no Tactical Analysis.

Sentinel will work with the City to help identify any gaps between the current organizational security approach and those defined by NIST SP 800-82 Cybersecurity Guidelines. Cybersecurity policies and procedures will be reviewed and compared to NIST SP 800-82 best practices to identify any potential compliance or audit exposure for the organization. Many users are unaware of proper security policies and procedures when it comes to utilizing company infrastructure. As an optional component to the strategic assessment approach Sentinel can provide planned phishing attacks against the organization to determine whether additional policy development is necessary as well as user education.

Phase Three – Recommendations

The third phase of the assessment is where Sentinel will provide a prioritized list of recommendations based on the analysis performed during phase two of the assessment. The strategic assessment recommendations will be influenced and evaluated based on City organizational goals and objectives gathered during phase one and will be prioritized based on business impact, likelihood, and risk, in order to determine overall priority.

Sentinel services during this phase may include, but are not limited to the following:

- Validated design and deployment architecture alignment.
- Identifying ideal software versions with bug and security vulnerability awareness.
- Configuration standardization with best-practice consistencies.
- Recommended configuration changes.
- Software/hardware upgrade recommendations.
- Security deficiency identification with recommendations.
- Organizational alignment to goals and future state objectives.
- Overall constraints, budgets, non-technical influences.

Assessment Methodology (Strategic Assessments)

An assessment is the result of a deterministic process, which consists of information gathering and then analysis of that information. An assessment is most relevant when non-technical and technical data elements are married together to ensure the organizational goals are kept top-of-mind when providing recommendations. Sentinel breaks these non-technical and technical data elements into various topic areas as shown below:

Non-Technical Data

One of the most important factors in determining how a particular infrastructure area should operate is first determining what the organization expects from it. This opinion or viewpoint is often quite subjective as you move across differing business units, departments, and stakeholders. Sentinel's goal during this interview period is to formulate a relative consensus and agreement among key personnel on what the overall organizational objectives should be and work to marry technology solutions to them. These objectives will take into account items such as goals, growth, facilities, functionality, requirements, and constraints, as well as any overall concerns that need to be addressed.

Non-Technical Data
- Organizational Goals
- Stakeholder Goals
- Constraints, Budgets, Etc.

Technical Data
- Topologies
- Configurations
- Performance

Recommendation Process
- Gap Analysis
- Holistic Vision
- Strategic/Long-Term
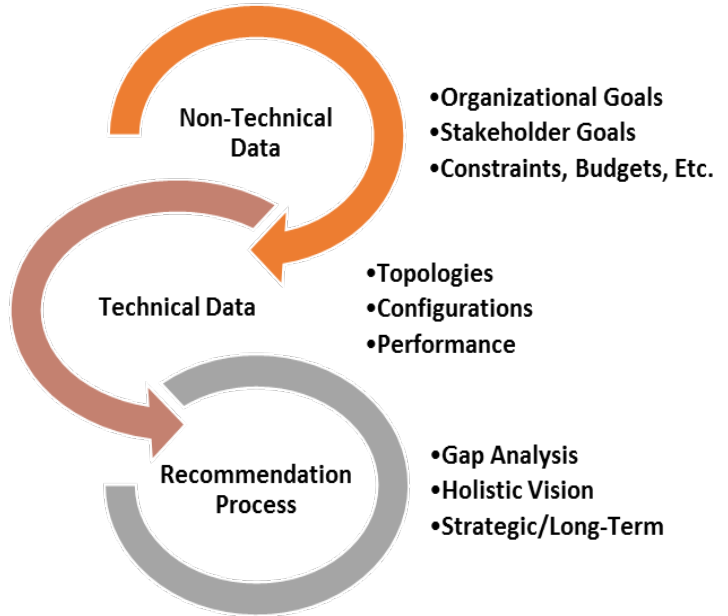
Technical Data

Once we have an understanding of the organizational goals for the various infrastructure areas, we know which technical data is required to assess whether the current environment meets those goals or not. Additional information may be required to further analyze the distinct technical areas as it relates to utilization, performance, traffic, and overall stability. Each respective technical area (I.e. Network, Datacenter, Security, Wireless, Collaboration, etc.) will have differing technical requirements that need to be analyzed as part of the assessment services.

There are several tools that Sentinel may utilize to gather this information such as commercial applications, custom in-house applications, and manual gathering techniques. This information will allow for a better overall understanding of the topology, health, and operation of each environment in order to provide meaningful recommendations. In multi-technology assessments, Sentinel will take into account all infrastructures under assessment when performing the best practice analysis.

If a specific technology area is not considered part of the assessment services, Sentinel will provide a cursory review of any adjacent infrastructures (i.e. A network assessment touches security, datacenter, collaboration, and wireless infrastructures. Therefore a network assessment will cover the network ports leading to these systems at a high-level (cursory) review rather than a comprehensive review provided by a specific assessment. The technical data gathering will also help identify any current and/or potential future equipment capability shortcomings that may affect future upgrades.

Recommendation Process

Sentinel uses both the non-technical and technical data gathered in the first phase of the assessment to perform an informal technical gap analysis and create customized recommendations for the City's environment. Information gathered about the current infrastructure(s) is reviewed and compared to the ideal infrastructure(s) to ensure it meets all organizational goals and requirements. By identifying any technical gaps between the ideal design and the current design, Sentinel is able to develop a holistic vision and set strategic long-term goals for the organization in each respective technology area under assessment.

Scope of Work

Phase One – Information Gathering

Process

- Strategic Assessments
    - o Sentinel will work with the City to determine the appropriate stakeholders that will be interviewed.
    - o Sentinel will provide the City with a pre-interview overview of the question topic areas so that stakeholders can be properly prepared.
    - o Sentinel will perform an on-site or remote interview session with key City stakeholders to gather information regarding organizational goals and objectives. This activity will be performed in person or via Cisco Webex conference.
    - o Security assessment
        - ▪ Sentinel will perform on-site interviews following the NIST SP 800-82 Cybersecurity Framework with identified stakeholders.
        - ▪ Sentinel will review all SCADA-related policies and procedures.
        - ▪ Vulnerability scanning of identified SCADA infrastructure.

Locations and Infrastructure in Scope:

- **Note:** Service provider managed equipment may be excluded if Sentinel access is unavailable. A cursory review of excluded infrastructure devices will be provided where they interface with the infrastructure components within scope.

Sites/Locations within Scope				
Aurora, IL				
4 locations				
Infrastructure/Devices/Applications within Scope				
Network Infrastructure	**Security Infrastructure**	**Collaboration Infrastructure**	**Datacenter Infrastructure**	**Application Infrastructure**
Entire Water Plant Network	Internal and External Firewalls	N/A	N/A	N/A
Remote devices, e.g. PLCs				
HMI workstations				

- Please note: All other locations and infrastructure are considered out of scope unless listed in the above table.

Sentinel Deliverables

- Strategic Assessments
    - o Identified Vulnerabilities of Plant Network.
    - o Identified Vulnerabilities of the Remote Station devices.
    - o Engineering review of network configurations.
    - o Stakeholder goals and objectives gathered during interview sessions.
    - o Security policies and procedures information for NIST 800-82 r2 alignment.

Customer Responsibilities
- Strategic Assessments
  - Determine appropriate organization stakeholders who should participate in the stakeholder interview sessions. This will include both technical and non-technical participants.
    - Provide employee list and contact information.
  - Provide access to security policies and procedures.
  - Participate in stakeholder meetings to gather appropriate organizational information.
  - Access to Water Plant Network and remote devices.

Phase Two - Analysis Process

- Strategic Assessment
  - This includes a broader scope conversation around the infrastructure as a whole and includes a deeper analysis of the City's requirements based on organizational goals.
  - Sentinel will perform a technical gap analysis between the current environment and the desired goals and objectives. A priority weighting will be performed based on organization impact, likelihood of occurrence, and risk for each recommendation.
  - Sentinel will document recommendations and tailor them to meet the City's identified goals and objectives where applicable.
  - Security assessment
    - A broader in scope conversation around the NIST SP 800-82 Cybersecurity Guidelines will be performed as well as a deeper analysis of the City's security posture.
    - Deeper analysis of the City's adherence to the NIST SP 800-82 Cybersecurity systems.
    - Sentinel will review collected policies and procedures and identify areas of improvement and/or compliance concerns.

Sentinel Deliverables
- Sentinel will provide a summary of the analysis findings in a prioritized listing. This document will identify issues that were observed during the information gathering and analysis phases of the assessment. This information will be used to develop the prioritized list of recommendations for the infrastructure under assessment. Priority will be weighted based on organizational goals and objectives for strategic assessments.

  Strategic Assessment:
    - Stakeholder interview session goals and objectives summary.
    - Technology alignment with the organizational direction and focus.
    - Best practice design, configurations, and deployment methodologies.
    - Planned and organic growth, scalability, etc.
    - Redundancy, failover, high-availability, etc.
    - Future project impact, timelines, milestones, and goals.
    - Strategic assessment approach will also incorporate tactical assessment items.

Customer Responsibilities
- Participate in any meetings to review documented findings.

Phase Three – Recommendations

Process
- Sentinel will utilize the findings from the analysis phase to provide a prioritized list of recommendations.
- Each recommendation will include background information on the topic being discussed in order to provide context for the technical recommendation to follow. Recommendations may reference industry or manufacturer best practice documentation as well as suggested high-level remediation steps.
- Recommendations will be aligned with organizational goals and objectives as part of a strategic assessment and for tactical assessments, provided based on Sentinel opinion and industry practices.
- Supplemental documentation may be provided for customer reference and additional supporting documentation for topic areas.

Sentinel Deliverables
- Sentinel will provide a prioritized list of recommendations to the City based on the analysis findings.

Customer Responsibilities
- Participate in meetings to review documented recommendations.

Project Management

Sentinel will provide a Project Manager committed to the success of the project. The Project Manager will be responsible for each of the following:

- Complete success of the Project.
- Optimal coordination of all resources.
- Guiding City resources on aspects of the project they are required to perform.
- Tracking and reporting of progress.
- Management of expected timelines for the assessment.
- Changes to the project and communications of changes in writing using a Project Change Request (PCR) form.
- Post-assessment document gathering, assembly and presentation.
- Post-assessment project completion agreement and signature.

Project management will ensure complete project success. Communication is the cornerstone of sound project management and the Project Manager will be the central communication mechanism for all parties. This will ensure all resources are informed about decisions that may affect the success of their component of the solution.

General Assumptions

The following is a list of general project assumptions:

- Sentinel guarantees it will perform all tests in a responsible and professional manner in accordance with best practices and that it will use its best efforts not to change or amend any applications, data, programs, or components of the City's network or computer system (including hardware and software) but does not guarantee against any disruption or effect on the City's production. The City understands that Sentinel shall not be liable for any damages to arise from any such disruption.

- Current infrastructure under assessment is in an operational state, excluding any specific issues that may be under evaluation as part of the assessment services. Sentinel has not included any troubleshooting or remediation services as part of this proposal.

- City has access to all infrastructure areas under assessment and can provide this information to Sentinel. **Note: Service provider managed equipment may not be accessible and therefore excluded from assessment unless configuration(s) can be provided by the City.**

- Sentinel assessment services are performed **<u>remotely</u>** utilizing City provided remote access. If on-site services are desired or required, they can be quoted separately.

- For strategic assessments, the stakeholder interview sessions may be performed on-site in person depending on City audience and resource availability. Otherwise, sessions will be performed via Cisco WebEx conference.

- Business process analysis is not included as part of this proposal. These services can be quoted separately by the Sentinel Business Process Consulting group.

- Any information discussed and/or provided by Sentinel to the City is considered confidential and should not be distributed to outside the City's organization without Sentinel's written approval.

- Remediation of any assessment recommendations are not included within this proposal and can be quoted separately.

Pricing Summary

Pricing Breakdown			
Phase & Description	**Type**	**Technology**	**Price**
Phase 1-3 SCADA Assessment	Strategic	Security	$54,890.00
Grand Total			**$54,890.00**

Pricing is valid for 30 days