SecurePlan™

SECURITY MITIGATION FRAMEWORK

0623_046_EB_MCA_SP_SMF

SecurePlan™ | Security Risk Mitigation Framework

Table of Contents

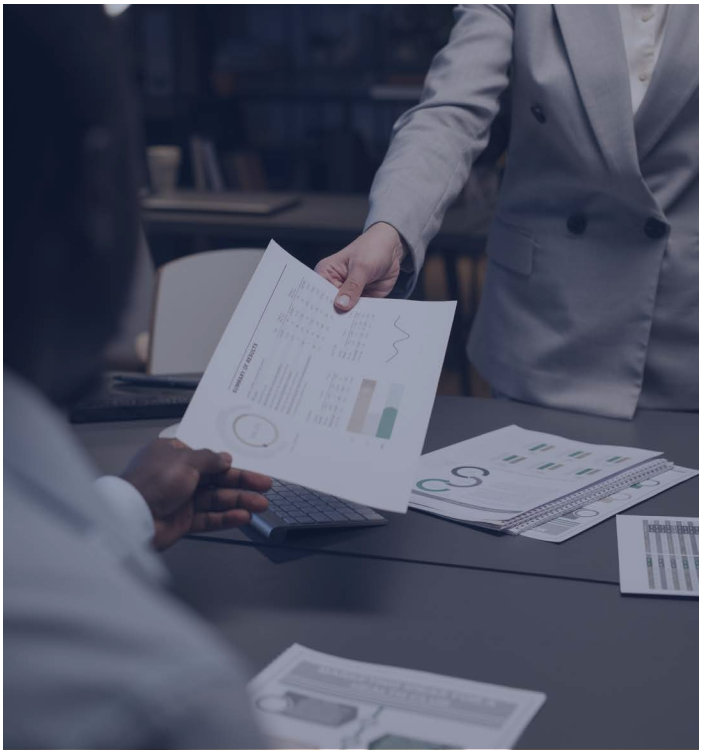
Executive Summary	1	On-Site Support	7
The Cost of Being Reactive	2	MCA Overview	8
Tools for Efficiency and Economy	5	SecurePlan Summary	9
Remote Support Benefits	6	SecurePlan Options	10

Executive Summary

In our industry, safety and security is the top priority. However, modern technology is creating ways to help you with another key part of your business: *improving your bottom line.*

Implementing a service level agreement (SLA) with your security service provider can ensure that cost-saving benefits such as remote and on-site support are available to you quickly, efficiently, and without question, rather than worrying about cost every time an issue arises. A good service level agreement can resolve more than 50% of issues remotely, which saves greatly on travel and labor costs.

At MCA, we create these programs are being created with customer service top of mind, to match your growing security needs and ensure maximum uptime - *up to 99.99%* - in an economically mindful manner.



An SLA, creates an understanding with a customer that defines expectations at the very beginning of a relationship, and set penalties and compensation for when these expectations might not be met.

On a very basic level, an SLA is beneficial for both the client and the business because everyone is on the same page, and the customer is much less likely to be disappointed if an unexpected complication or malfunction occurs.

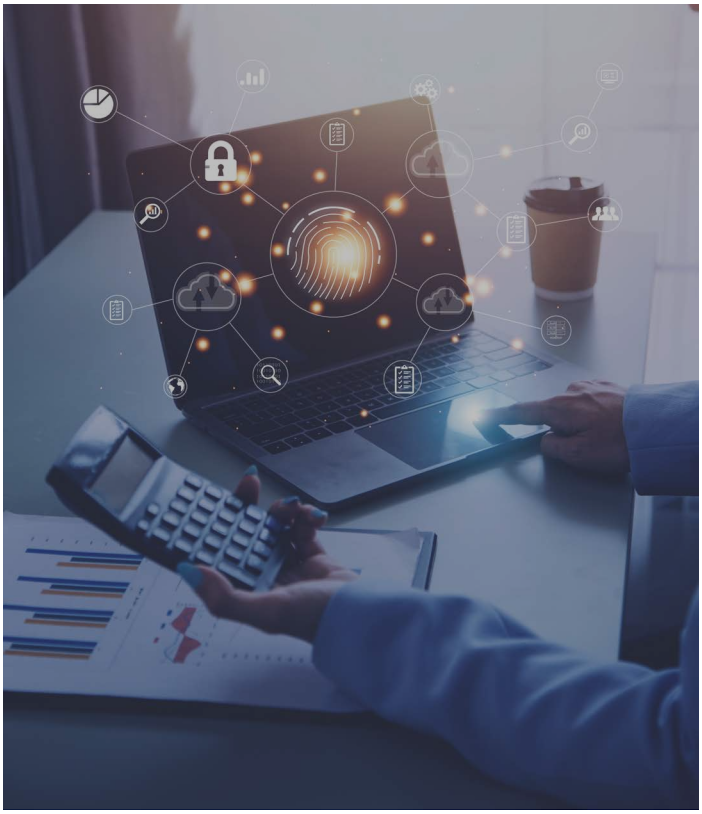
With technological advancements drawing physical security systems such as access controls, video surveillance, detection systems, and more, under the umbrella of IT, the needs of customer service have changed.

In the past, and even now, many organizations are covered under the Time and Material Model (T&M), meaning clients contacted their providers only after discovering an issue and then are obligated to pay for all labor and parts required for the repair.

At first, the T&M model looks less expensive, based on only paying for critical issues, but think of an SLA the same way you would think of a home warranty. You pay upfront to ensure that your problems are covered at no extra *(and undetermined)* costs to you.

Additionally, SLA's can include preventative services — just like annual physicals are covered at no cost with health insurance. An SLA also strengthens the customer relationship by ensuring that their issues can be resolved quickly and with the best solution rather than the easiest or cheapest one. When you outline service expectations, improved customer satisfaction stays a clear objective.

In today's world, information is moving quicker than it can be absorbed, and technology is advancing at exponential rates. If businesses react to issues and trends after the fact, they are already far too behind the curve. In the security industry, extra seconds of reaction time can make the difference in preventing a cyberattack or a security breach from damaging a company in ways they may never fully recover.



The cost of being reactive is not always necessarily the monetary cost of the bottom line or damaged profits — it could also be the cost of a damaged reputation, stolen information, or not having the vital video evidence when it is needed. Utilizing IT-Level Technology Infrastructure Management, these tools and automation practices can optimize your infrastructure documentation, problem detection and assessment processes, diagnostic information storage, corrective action plans and collaboration technology.

The Cost of Being Reactive

Manual processes are not timely enough or cost-feasible for maintaining security system cyber hygiene and full performance. Security automation can help combat the rising cost of attack discovery, with savings of approximately $3.05 million, according to the IBM Security Cost of Data Breach Report 2022.

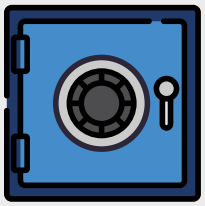
But companies are still hesitant to make the switch, with just 41 percent of the IBM respondent sample saying they leverage automation. When a malfunction is found, the actions required to fix it sometimes leave opportunities open for attackers to find different weaknesses. This is why near-instant detection of security system problems, coupled with proactive, preemptive and predictive maintenance and service, is a great idea.

One of the most reactive practices in the physical security industry right now are self-test health checks. There is real ROI in the IT practices that security industry self-test health checks can't deliver. Best practice updates are becoming more important in the physical security industry as our technologies become more and more intertwined with the IT industry.

Previously, companies tried to limit security system access to a select, privileged few within the department. Now, with a growing number of points of access, security systems must also put more real-time monitoring into place. According to a 2022 report by IBM Security, a single breach costs over $4.35 million on average. This figure represents a 2.6% increase from last year, when the average cost of a breach was USD 4.24 million. The average cost has climbed 12.7% from USD 3.86 million in the 2020 report. Rather than waiting for a breach, companies can know everyone on their networks at all times.

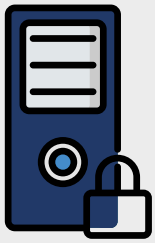
At MCA, our clients who use , our service level agreement, save around 33% for their yearly security needs. This happens because of the technology utilized, and tools used to be more proactive. Around 50% of the tickets generated within a year, through our health monitoring software, are self-generated, which means that no employee had to spend hours finding this issue and subsequently costing labor hours.

These are just a few basic examples of where proactive maintenance, monitoring and real-time system checks are beneficial. The cost of reacting is far too great these days to ignore the data.



USD 4.35 million
Average total cost of a data breach

83%
Percentage of organizations that have had more than one breach

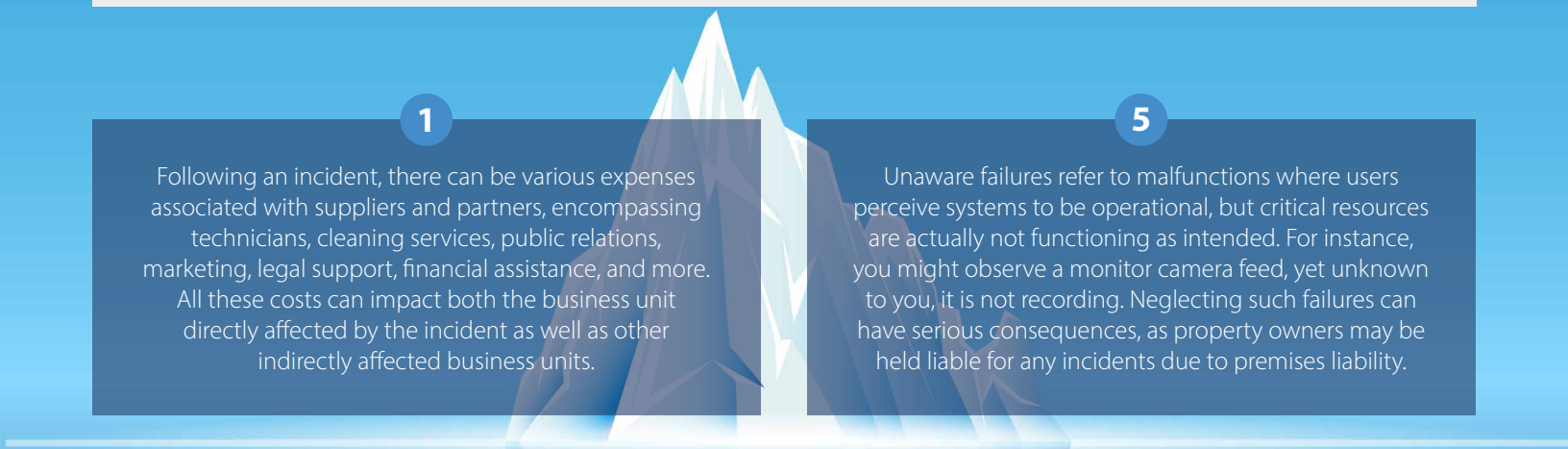


USD 4.82 million
Average cost of a critical infrastructure data breach

USD 3.05 million
Average cost savings associated with fully deployed security AI and automation

The Cost of Being Reactive

The cost of a reactive approach goes beyond surface level financial implications and can encompass damage to reputation, loss of valuable information, or the absence of crucial video evidence when it is most needed.



1

Following an incident, there can be various expenses associated with suppliers and partners, encompassing technicians, cleaning services, public relations, marketing, legal support, financial assistance, and more. All these costs can impact both the business unit directly affected by the incident as well as other indirectly affected business units.

2

As a consequence of the incident, there may be expenses associated with replacing damaged equipment, goods, or materials. These costs arise from the need to procure new items to replace the ones affected by the incident.

3

Incidents can incur legal or contractual costs when an organization fails to meet predefined requirements for product or service delivery. Inability to comply with these obligations due to an incident can result in additional expenses and potential legal consequences.

4

Maintaining up-to-date firmware for IoT devices is paramount to ensure operational efficiency, mitigate cybersecurity risks, and avoid compliance hurdles. Neglecting firmware updates can have detrimental consequences for the entire organization, impacting its overall performance and exposing it to potential vulnerabilities.

5

Unaware failures refer to malfunctions where users perceive systems to be operational, but critical resources are actually not functioning as intended. For instance, you might observe a monitor camera feed, yet unknown to you, it is not recording. Neglecting such failures can have serious consequences, as property owners may be held liable for any incidents due to premises liability.

6

By regularly applying Software Update Packets (SUPs), you can effectively safeguard your software against security issues and reduce vulnerabilities. Keeping your software up-to-date through SUPs is crucial for maintaining a secure and protected system.

7

Inadequate service levels can result in a loss of revenue, potentially leading to client dissatisfaction and potential customer attrition. Ensuring consistent delivery of products and services is vital to maintain customer loyalty and revenue streams.

8

Failure to properly maintain and manage IoT infrastructure can result in increased insurance premiums. Insurance costs are influenced by factors such as the frequency, severity, and expenses associated with incidents. Neglecting the care and maintenance of IoT devices raises the risk profile significantly, leading to exponential increases in insurance premiums.

An Evolving Landscape

Staying up-to-date with the latest security technology is crucial in today's rapidly evolving landscape. Whether it's IP cameras, AI-powered video surveillance, or leveraging the capabilities of cloud services, embracing these advancements is essential. The Internet of Things (IoT) has permeated our daily lives, connecting various smart devices that transmit and receive data through the internet. From thermostats to cars and security systems, IoT devices offer convenient access to real-time data, facilitating efficient communication between machines and yielding improved outcomes at a faster pace. The automation of tasks within businesses enhances service quality while reducing labor costs by minimizing human intervention.

However, it is important to recognize that intelligent industrial IoT (IIoT) devices have become prime targets for hackers. Many of these devices lack built-in cybersecurity measures, leaving them vulnerable to various cyberattacks. The utilization of IoT technologies has witnessed explosive growth, with current estimates indicating over 23 billion connected IoT devices, outnumbering the global population threefold. Unfortunately, the past couple of years have seen a significant surge in the frequency, magnitude, and sophistication of cyberattacks targeting these devices. It is essential to address these security concerns to safeguard the integrity of IoT deployments.

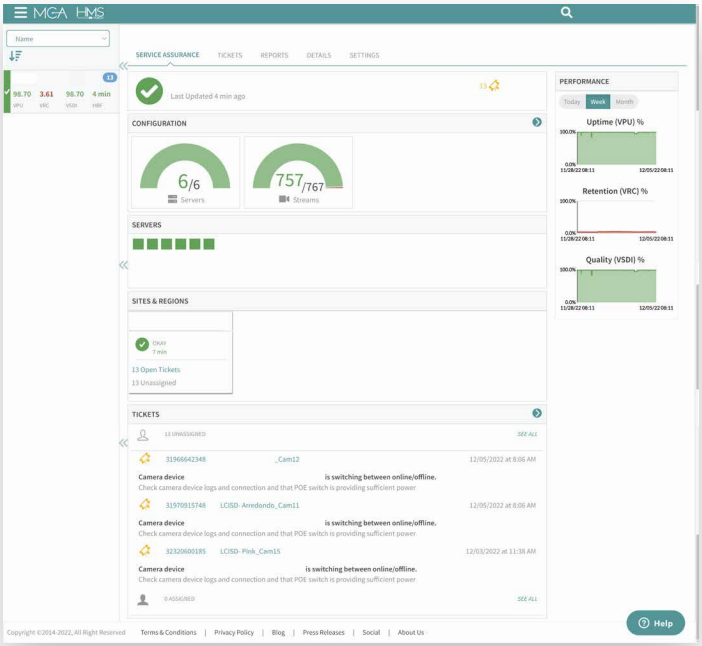
Comprehensive Assurance

To maintain robust cybersecurity and optimal performance for security systems, it is imperative to possess strong and comprehensive service assurance capabilities.

Achieving this goal requires a highly scalable, multi-vendor solution specifically designed for security infrastructure. In the market, there are tools available, including MCA's own health monitoring software, that offer cloud-based service assurance solutions tailored for video and physical security system infrastructure.

These tools continuously monitor and analyze your physical security infrastructure to identify abnormalities or suspicious conditions. With the rise of botnets that hijack resources for malicious purposes, these tools can provide you prompt alerts when unusual traffic is detected from camera devices.

Furthermore, they can be utilized to inspect other resources within the physical security network, effectively identifying potential issues and ensure overall system integrity.



Password Vulnerabilities

Password security is a critical aspect that should never be underestimated, as it serves as a potential gateway for hackers to infiltrate a system. While managing passwords may seem manageable in small-scale intelligent IoT device networks, it becomes increasingly complex when dealing with deployments comprising hundreds or thousands of devices. In such cases, automated password management tools become essential.

These tools not only facilitate password changes within the devices themselves but also ensure that stored passwords in devices and associated software are updated. By employing our tools, IoT device owners can maintain control over password management while keeping auditable records to adhere to password management policies.

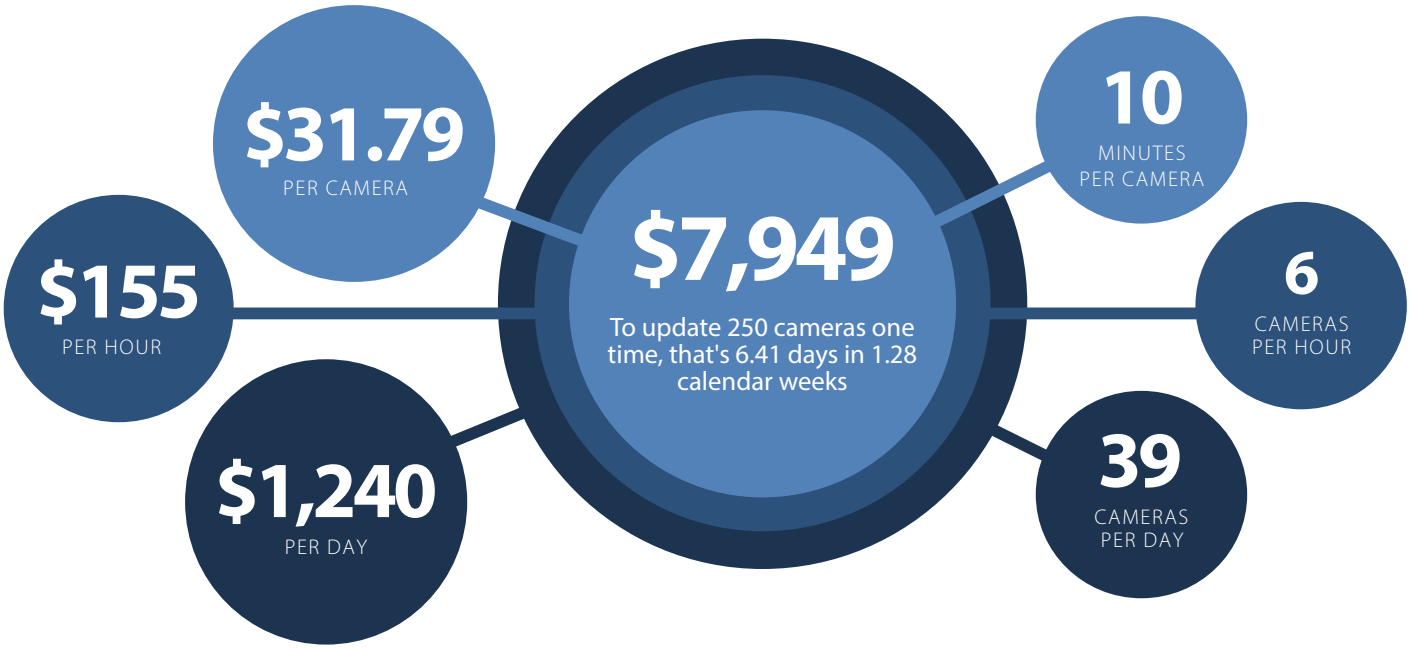
By implementing the appropriate tools through a Service Level Agreement (SLA), it becomes possible to automatically scan all camera devices on the network and generate reports identifying cameras still using default or easily guessable passwords. If compromises are suspected, prompt password changes are essential. The effectiveness and cost-efficiency of automated password management cannot be denied, especially when dealing with large-scale deployments.

Remote Support Benefits

When considering a service level agreement, there are numerous benefits across various aspects of your service requirements. This includes remote customer service provisions that save time and reduce or eliminate downtime by eliminating the need for scheduling or travel. Ultimately, this leads to cost savings for both parties involved.

Modern businesses leverage advanced analytics, artificial intelligence (AI), and machine learning systems to gain comprehensive insights into their entire information infrastructure. However, security directors and managers often rely on security officers to manually monitor camera displays to ensure system integrity. This traditional approach is ineffective as the mere activation of a camera does not guarantee recording.

Fortunately, advanced IT monitoring and management technology can continuously audit all devices and systems around the clock. Instant notifications are sent to personnel in case of component failures, accompanied by detailed diagnostic information. Nevertheless, security departments may still lack end-to-end visibility across their complete security systems infrastructure, resulting in potential issues such as video recording interruptions or failure to meet retention periods without anyone being aware. ***This is precisely where tools like our health monitoring software and specialized monitoring centers play a crucial role.***



In a manual environment where IT practices were not utilized, the limited information collected was stored on the system's own server. This setup required server access for troubleshooting, resulting in data loss if the system failed or inaccessibility when the application crashed or the intelligent device was off-line or non-functional. Nowadays, diagnostic information can be centralized outside the monitored systems and securely backed up in the cloud. This ensures that troubleshooting information remains available even if the system or device experiences a failure.

Let's consider the costs associated with updating firmware for 250 cameras, which represents a significant technology infrastructure investment of over $375,000.

Taking into account the best-case scenario cost and performance figures shown in Figure 1, additional costs include supervision and manual generation of audit reports. However, the manual approach lacks verification of firmware update accuracy and does not validate the device inventory used.

Conducting three update cycles and generating at least one audit report using the manual approach would exceed $24,000 and require a month's time. As demonstrated, an effective Service Level Agreement (SLA) leverages remote efficiencies that save money and relieve you of certain responsibilities.

When a business like MCA places the highest priority on its customers, an SLA becomes a commitment to addressing their needs even in extraordinary circumstances.

Considering the safety of all technicians, staff, and clients, remote support leveraging advanced technology ensures that your issues can be resolved regardless of the prevailing conditions. This includes scenarios as diverse as inclement weather, pandemics, government shutdowns, and more.

Even when an on-site visit is not infeasible due to extreme circumstances, our technicians can guide you and your staff to resolve problems through video conferencing and phone calls. No matter the nature of the issue, a reputable company utilizes a service level agreement to form a partnership with you in maintaining utmost safety and security at all times.

On-Site Support

Typically, an SLA encompasses on-site response times and technician services tailored to your needs. Depending on the contracted service level, this can often include priority dispatch responses, giving your organization precedence over non-SLA clients, as well as guaranteed time windows.

Once a technician is dispatched, in addition to their swift response, the labor costs for repairs and replacement parts are covered during regular business hours. This reduces your overhead expenses and allows for predictable budgeting. A robust SLA should also offer special pricing or discounts for services beyond the standard scope of work or outside of regular business hours.

Superior SLA's like those at MCA, incorporate device repair or replacement policies that account for normal wear and tear. Whether your devices are within or out of warranty, these inclusions in an SLA ensure that repairs and replacements are conducted without incurring additional costs.

In the event of a system malfunction, there are instances where a device or component may require repair directly from the manufacturer. Such manufacturer repairs often take several weeks, or even a month. However, being without your security system for that amount of time is simply not feasible. This is where a well-crafted service level agreement surpasses a mere warranty, as it includes the provision of loaner equipment while yours is being repaired.

Aside from addressing unexpected issues, it is crucial to ensure your security system maintains optimal performance. A reliable SLA encompasses annual visits to assess the system and thoroughly test its overall functionality.

Who is MCA?

MCA is one of the largest and most trusted integrators in the United States offering world class voice, data, and security solutions that enhance the quality, safety, and productivity of customers, operations and lives.

Enterprise leaders faced with problems from communication gaps, security challenges, and data threats choose MCA's certified teams to design, implement, and maximize solutions, from the most trusted and reliable US-based manufacturers.

These leaders love the assurance of MCA's local sales and service teams, being there in the moments that matter throughout the life of the solution.

More than 65,000 customers trust MCA to provide carefully researched solutions for a safe, secure, and more efficient workplace. As your trusted advisor, we reduce the time and effort needed to research, install, and maintain the right solutions to make your workplace better.

What We Do

We pride ourselves on employing experts who understand the latest cutting-edge wired and wireless voice, data, and security technologies for your specific industry. We pursue only the most effective solutions to fit your budget and meet your exacting needs. Some of the industries we collaborate with are outlined below:

- Manufacturing
- Construction
- Education
- Fire & Rescue
- Emergency Services
- Healthcare
- Hospitality
- Law Enforcement
- Logistics
- Public Safety
- Security
- Utilities
- Recreation
- Retail
- Transportation

The MCA Difference | A Service-First Approach

What does it mean to take a service-first approach?

At MCA, we provide service wherever and whenever it is needed. In short, our greatest commitment is to serve our employees, our customers, and tens of thousands of individual communities across the United States.

The MCA advantage is our extensive service portfolio to support solution life-cycles from start to finish combined with our team of certified professionals. As your trusted advisors service is woven into the DNA of our company. It is more than a motto — ***it is who we are.***

Large-Scale Support and Local Management

As a family company, MCA furnishes its clients with all the management and support advantages of a local business while also offering a vast array of state-of-the-art security and communications solutions.

Despite being a large enterprise, we're embedded in the communities we serve — with teams equipped with the experience, knowledge, and expertise needed to provide the most advanced solutions possible.

THIS IS THE MCA DIFFERENCE.

SecurePlan™ | Overview

When it comes to choosing the right partner for your security needs, there are several criteria you should consider – customer service expertise, responsive tech support, remote support, a trusting relationship, the capacity to identify and mitigate threats, effective tech support and updates, and expertise and experience. MCA meets all these criteria and strives to go above and beyond your service expectations. With the ***SecurePlan™*** program, take advantage of all these benefits within a service level agreement.

Customer Service Expertise

Within our Client Service Center (CSC), we leverage over 20 years of collective experience in the security industry, along with certifications and specialized training, to diligently monitor your health system — swiftly identifying and addressing any potential issues that may arise.

Responsive Tech Support

Our extensive capabilities for onsite and remote repair/diagnostics arenotable. With over 80 strategically positioned offices across 13 states, we guarantee swift service and enhanced uptime, providing you with valuable support whenever and wherever you need it.

Remote Support Services

Alongside our onsite visits, our team possesses the ability to resolve over 50% of issues remotely. This remote troubleshooting capability ensures efficient problem-solving without the need for physical presence, saving you time and minimizing disruptions to your operations.

Trusting Relationships

MCA values transparency and openness as integral components of successful partnerships, and we prioritize fostering strong and trustworthy relationships with the thousands of clients, employees, and communities we serve.

Threat Identification & Mitigation

When selecting a partner, it is crucial to prioritize those with a robust strategy in place for actively monitoring, identifying, mitigating, and addressing threats. The effectively identify and mitigate threats is essential for ensuring the security and protection of your organization.

Effective Tech Support & Updates

A reputable security systems company possesses essential infrastructure for ensuring operational continuity. Moreover, it regularly updates software and upgrades technology to address emerging threats and close any security vulnerabilities.

Expertise & Experience

With centuries of combined experience, MCA's executive team has successfully undertaken notable high-profile deisgn and install projects for government agencies, power and utility companies, and Fortune 500 corporations.

MCA's exclusive ***SecurePlan™*** program is designed to cater to all your growing security needs cost-effectively, work to protect your budget from the unexpected, and SLA options provide clients with much more than a "simple warranty." MCA offers a flexible service level agreement (SLA) option to meet any coverage need.

Fundamental
SecurePlanLimited™

Level 1
SecurePlanLimited™
24/7 system health monitoring + alerts + software updates

Comprehensive
SecurePlan™

Level 2
SecurePlanLimited™ + SecurePlan™
Proactive resolution + onsite support with guaranteed same-day response *(includes free loaner equipment, annual function tests and software updates, and as-needed replacement for all devices)*

Highest Security Environments
SecurePlan™ 24

Level 3
SecurePlanLimited™ + SecurePlan™ + SecurePlan24™
24/7 onsite service with guaranteed 4-hour response window

www.callmc.com • 800-596-8205 • info@callmc.com

In Security, There are No Second Chances

A crisis is no time to discover system errors. That's why it's critical to have SecurePlan™ by MCA.

This exclusive program was designed to cost-effectively scale alongside our customers growing security needs to ensure maximum uptime.

SecurePlan™ is superior to standard warranties because it remediates risks before they become issues.

Discover the Benefits

- Priority Dispatch *(with Guaranteed Same-Day Response)*
- Preventive Maintenance
- No Labor & Travel Costs *(During Standard Business Hours)*
- Nationwide Coverage
- No Unknown Failures or Downtime
- Saves Money Long-Term
- No Surprise Expenses

SYSTEM HEALTH MONITORING*	SecurePlan 24	SecurePlan	SecurePlan Limited	MCA Standard Warranty
System health monitoring*	✓	✓	✓	N/A
Client notification of detected system issues	✓	✓	✓	N/A
Predictive failure alerts on core components	✓	✓	✓	N/A
Proactive resolution of detected system issues	✓	✓	✓	N/A
REMOTE SUPPORT				
Remote diagnostics and issue remediation	✓	✓	✓	N/A
On-demand remote support session	✓	✓	✓	N/A
Customer help desk	✓	✓	✓	N/A
Coordination of on-site repair	✓	✓	✓	N/A
Same day remote service	✓	✓	✓	N/A
Remote delivered annual function test	✓	✓	N/A	N/A
ON-SITE SUPPORT				
Warranty device replacement	✓	✓	N/A	**1yr**
Out of warranty device repairs/replacement	✓	✓	N/A	N/A
Guaranteed same-day response	✓	✓	N/A	N/A
Free loaner equipment	✓	✓	N/A	N/A
Technician travel included	✓	✓	N/A	**1yr**
Annual system inspection, cleaning & testing	✓	✓	N/A	N/A
Annual system software upgrades (including labor)	✓	✓	✓**	N/A
Discount on labor for billable service work	**10%**	**10%**	N/A	N/A
On-site customer training session	✓	✓	N/A	N/A
24x7 Service included	✓	N/A	N/A	N/A
4 Hour service response	✓	N/A	N/A	N/A
ADMINISTRATIVE				
Maintenance of system records	✓	✓	✓	N/A
Software license management	✓	✓	✓	N/A
Annual technical planning session	✓	✓	N/A	N/A

**System Health Monitoring Requires access to Internet for outbound traffic*

***Annual System Software Upgrades for SecurePlan Limited are remote only*

CONTACT US TODAY TO MAKE YOUR WORKPLACE MORE SAFE AND SECURE

www.callmc.com • 800-596-8205 • info@callmc.com