Key Considerations When Evaluating Visitor Management Solutions

multicard

ENTRUST

Table of Contents

Visitor management best practices

Selecting a visitor management system (VMS) is a key step for organizations that are working to secure their buildings and facilities. As with any system procurement cycle, there are many factors that should be evaluated and considered when selecting the right visitor management system.

The goal of this document is to help you identify the key questions that you should be asking when evaluating any visitor management solution. As always, the questions and expected vendor responses should be tailored to your organization's needs.

In addition to the questions highlighted in this document, you should also review your current visitor management policy and overall security procedures to ensure that any new visitor management system will meet your requirements.

> **"WHEN I THOUGHT ABOUT NEEDING TO KNOW WHO WAS ON-SITE, THIS WAS THE MOST INNOVATIVE SOLUTION I KNEW OF FOR SUCH A TASK."**
>
> Leading Global Pharmaceutical Company

Availability

Is the visitor management system always available?

Any web-based system you choose should have a proven track record of availability. We have a track record of 99.97% uptime, which means you can depend on Entrust to meet all of your visitor management needs, whenever you need us.

Does the vendor have a service-level agreement (SLA) for their service and support?

All vendors should be able to provide an SLA that includes not only uptime guarantees, but also support levels and response times should you have an issue or question regarding the solution.

Does the vendor have a disaster recovery plan?

Any software or service provider should be able to provide a disaster recovery plan and/or a business continuity plan. These plans ensure that, should a disaster occur, they are prepared to deal with the disaster and make sure that your organization's visitor management system will not be adversely impacted.

We have a track record of 99.97% uptime.

Hardware requirements

What are your hardware goals for your VMS solution?

Our cloud solutions help you avoid increasing your IT hard- and soft-cost spend. There are no physical servers for you to purchase, maintain, update, and train on. No one in your IT department will need to be responsible for maintaining and operating your VMS. They are free to do what they were hired for – to be the technology experts for your business.

We handle all of the updates, servicing, and security for your VMS. No hidden costs or burden to your IT department or its budget.

On Prem/Networking

We use end-to-end encryption for all of your data and traffic:
- TLS 1.2 encryption for all data in motion
- AES-256 bit encryption for all data at rest

All of our kiosks and printers use the most secure methodology for moving your visitor information.

NO HIDDEN COSTS OR BURDEN TO YOUR IT DEPARTMENT OR ITS BUDGET.

Scalability

Scalable for users

Built in the Azure Cloud, our system has the ability to instantly scale up to meet the specific needs of your business. With our user import options, we'll help you build intuitive easy-to-use training documents that will help your employees quickly and easily adopt and use your VMS solution.

Scalable for locations/businesses

Whether we're helping you at a single location or 100, our solutions are feature-rich. We don't limit your capability or productivity; we give you everything we have no matter the size of your business.

Your start-up has the same access to the same data protection, privacy, and security as the Fortune 500 company you want to grow into. With an easy-to-calculate subscription cost, you can easily forecast your costs as you grow, and we scale with you.

YOUR START-UP HAS THE SAME ACCESS TO THE SAME DATA PROTECTION, PRIVACY, AND SECURITY AS THE FORTUNE 500 COMPANY YOU WANT TO GROW INTO.

Data protection

Entrust has partnered with Veristream for the VMS solution. Veristream is an industry leader in protecting and securing your data. Through this partnership, we offer you end-to-end encryption on all data in motion and data at rest. We use TLS 1.2 encryption for all traffic between your Multicard VMS solution and your locations. Once your data is safely inside your VMS solution, we use AES-256 bit encryption to protect your data.

The VMS solution is securely positioned in the Microsoft Azure Cloud. The Azure data centers are all U.S.-based, but are accessible worldwide.

The minimum information we need is a first name and last name of your guest. Nothing more is required. We can quickly and securely scan government-issued identification cards, reading and retrieving only the first and last names from those IDs.

To further help meet General Data Protection Regulation (GDPR) guidelines, there is a "Right To Be Forgotten"/"Delete Identifiable Information" button in the VMS solution to let you quickly and efficiently comply with EU citizens' requests to be removed from any database.

Third-party audits

Veristream goes through security audits from third-party companies every year. All of Veristream's solutions are subjected to extensive penetration and security tests. Any issues found are reported back to Veristream and resolved.

Integration

Does the visitor management system provide single sign-on (SSO) integration?

Most businesses already have a single source for their employee computing credentials, such as login ID and password. SSO integration means that employees do not have to remember yet another username and password in order to log in and use the visitor management system. While this may seem trivial, pre-registration of visitors and overall system use can be directly correlated with the system's ease of use. If users are unable to remember or locate their login ID or password, they'll be less likely to actually log in and pre-register visitors.

SSO integration with your existing computing credentials means that, in many cases, users never even have to see a VMS login screen.

Does this visitor management system require any other implementation partners?

Depending on the type of system selected, some visitor management providers require security or building management to identify other teams required to support the VMS. For example, older-generation visitor management systems that require you to host software on-site will require an IT team dedicated to installing and maintaining the visitor management servers.

A major advantage of software-as-a-service systems like ours is that building management can work directly with our VMS to roll out the system, with minimal support from outside resources.

Configurable to business needs

Is the visitor management system configurable to changing security policies and processes?

Visitor management systems that don't evolve with changing security policies put companies at risk. A VMS must be able to adapt in real-time. It should be able to provide updated visitor lists, "Do Not Admit" lists, individual hours of entry, and also adapt with your policies as they change.

Evacuation list

Does the visitor management system provide an evacuation list that is accessible online in the event of an emergency?

This is an essential feature of any VMS. With a web-based software-as-a-service system, updated evacuation lists are instantly available to security personnel in the event of an emergency. Information including visitor names and correlated hosts being visited are retained until checkout.

Watch list – do not admit

Does the visitor management system have a global watch list or "Do Not Admit" list for all locations within an enterprise corporation?

Corporations with multiple locations and facilities – whether it be around the corner or across the globe – need to be able to update and share a barred visitors list in real time. Some visitor management solutions integrate with corporate HR networks to ensure that ex-employees, disgruntled ex-customers, and those who should otherwise be barred from your building are denied access.

Technical support

Does the visitor management system include free technical support with your subscription, or does it require an annual maintenance agreement?

Web-based visitor management systems typically do not require large upfront capital expenditures for hardware and software, but many do require an annual service agreement that covers ongoing service and support. Not ours. Technical support is included with our software subscription. You are not required to pay for additional support if you have questions or concerns. We're here for you whenever you need us.

For more information

888.383.6083
info@multicard.com

multicard.com

Contact Multicard for More Information
888-383-6083 x105
info@multicard.com

Learn more at
multicard.com

ENTRUST