ENGINEERED TO ENDURE

The Building Blocks for a New Class of Voter Registration System

Votem

ENGINEERED TO ENDURE: *THE BUILDING BLOCKS FOR A NEW CLASS OF VOTER REGISTRATION SYSTEM*

The year is 1988. From hockey rivalries to movies like *Rocky IV*, *WarGames*, and *Red Dawn*, popular culture depicts the Soviet Union as an imposing threat.

Fast forward to 2016. The attack is real. But instead of a nuclear war, a digital cold war begins. Russian hackers jeopardize the integrity of US elections, causing widespread fear and a scramble to assess any interference, revealing significant weaknesses in election infrastructure.

Besides the threat of cyber attackers, election officials face a multitude of battles. From meeting increasingly contracting budgets to serving both a retirement-age citizen and a digital native, all with the exact same technology, the challenges are enormous.

So how does an election official combat these pressures? The best solution is to mobilize the most secure, high-performing, and simultaneously easy-to-use election technology available. At the core of the election technology ecosystem is the Voter Registration System (VRS). And *how* the VRS is engineered is of paramount importance, as the building blocks of the architecture will translate to a system that is resistant to failure, secure, budget-friendly, and is equally pleasing to use among a diverse demographic.

This white paper will provide a comprehensive discussion of those building blocks, and demonstrate how intelligently piecing them together results in the ideal VRS. These building blocks are Software Architecture, Interoperability, Database, and Hosting Infrastructure.

GOOD DESIGN SOLVES PROBLEMS FOR TODAY, AND THE FUTURE

MODERN SOFTWARE DESIGN: *FAILURE RESISTANT ARCHITECTURE*

One of the greatest fears keeping election officials awake at night is the potential failure of a VRS the day before an election. Even if election day is months away, a disruption at any time is a hassle that costs time and money, and wreaks havoc on the administrative process.

The VRS building block that mitigates this fear is a failure-resistant software architecture. The resistance to failure comes from a software design known as microservices, a containerized approach to building an application where no single component of the system can impact the performance of the other components of the system. This is in contrast to the monolithic architecture used by older Voter Registration Systems, which have dependent connections between system components.

Microservices and Containers

The best example of microservices and containers is a scenario where the VRS vendor takes down the system to apply a security patch to the Candidate Registration module. They say the update is complete, but suddenly, the Petitions Management functionality fails. Then the Voter Facing Site crashes. What happened? How could an update to Candidate Registration be causing this mayhem?

Essentially, that problem arises because most VR systems previously deployed in the market were built on monolithic architecture. Those systems were implemented 10–15 years ago, when high-quality tooling for developing microservices architecture did not yet exist. However, with the advent of tools such as Docker, Kubernetes, and mature cloud platforms such as AWS GovCloud, a VRS can be built with a containerized- or microservices- architecture, allowing for independent modules that are able to be updated without potential to disrupt service to other modules. Modern container tooling also allows for robust monitoring, alerting, scaling, and auto-healing capabilities at the individual component level.

With a failure-resistant, microservices architecture, an election official can rest easy at night.

Platform Independence

A forward-looking VRS should be designed to be platform independent. A web-based application with nothing to install locally, using technologies like HTML5 and Angular, that does not rely on browser plugins like Java or Flash, avoids the problems of changes in operating systems and technology. There are county election offices still using Windows XP because their VR application is not compatible with current browsers, but the browser they need is incompatible with modern operating systems. Not only is Windows XP no longer supported by Microsoft, but it does not support TLS 1.2, the minimum level of encryption for safe web browsing, putting those county voter records at risk. Requiring an unsupported operating system and browser to access a security-sensitive application is a "worst practice" that is completely antithetical to the idea of securing voter records.

INTEROPERABILITY: *INTEGRATES FOR EFFICIENCY AND DATA INTEGRITY*

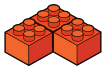
The election ecosystem of today uses a variety of types of technology, including equipment provided by multiple vendors, and data provided by external databases. It can be a struggle to coordinate the many sources of data, often arriving in file formats incompatible with each other or the VRS. This not only costs time, but also puts the accuracy of data at risk.

Enter the concept of interoperability. A VRS that integrates seamlessly with other election components such as electronic poll books (even if purchased from different vendors) results in less manual work and fewer potential human errors by staff, and an easier experience for voters on election day. A well-designed VRS will also integrate with external databases such as the state's motor vehicle agency, the National Change of Address (NCOA) database, Electronic Registration Information Center (ERIC) and many more. This allows new entries or changes to existing voter data to be quickly processed, and eliminates the kind of manual entry that can result in duplicate voter files, or misspellings and transposed street addresses.

National Institute of Standards and Technology (NIST) is exploring this concept via a working group to inform requirements for the Election Assistance Commission Voluntary Voting System Guidelines 2.0 (*https://www.nist.gov/itl/voting/voting-system-interoperability-working-group*). The goal is to standardize data formats that vendors will then unite to support. A VRS built without interoperability will not be able to benefit from these new industry standards and vendor cooperation.

Building a VRS with the core principle of interoperability requires design that ensures security and resistance to intrusions, while still being able to integrate with external components and

databases. This leads to a system that will continue to promote productivity and accuracy even as it ages.



DATABASES: *BUILT FOR FLEXIBILITY AND PERFORMANCE*

We live in an era where the expectations around a digital experience have permanently shifted. If a jurisdiction's system is slow and difficult to navigate, or doesn't offer the basic search functionality as our daily internet browsing, the user perception—by both employees and voters—is that the system is unreliable and antiquated.

A VRS must deliver performance and security, while being affordable and sustainable for the next decade. Building a VRS with a NoSQL database, such as MongoDB (used in big data and real-time web applications, and by companies such as Facebook, Google, and LinkedIn) provides benefits like availability and disaster recovery, flexibility for change, and high performance.

Availability and Disaster Recovery

Ever been hindered by a computer software update and not been able to do anything else until it's complete? What if that happened to the VRS on election day? NoSQL supports automatic database replication to maintain availability in the event of outages or planned maintenance, with automated failover and recovery. The database can be distributed across multiple geographic regions to withstand regional failures in the event of a disaster, whether natural or man-made.

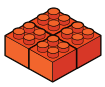
Flexibility for Evolving Data Requirements

If new legislation were to require the addition of a reporting function to the VRS, in an older system there would be costly and extensive redevelopment that could result in downtime for other parts of the database. However, NoSQL databases allow data to be organized and manipulated freely without the fixed restrictions of a SQL database, enabling developers to implement changes quickly without disrupting the application.

High Performance

Resource constraints demand that election professionals be able to do more, but with less time. Query times for voter records are 10 times faster compared with systems on older databases (a 5–10 second process is shaved down to ½ second), providing efficiency and time savings for staff. NoSQL databases are optimized for rapid querying of unstructured data. This translates not just into near-instantaneous, full-text searches with fuzzy matching, but also into look-ahead address entry, complex analytics, and the ability to store and manage documents directly in the database without impacting performance.

A NoSQL database allows the use of Elasticsearch, a distributed full-text search engine, which then provides fuzzy matching capabilities. This means that as data is pulled in from external databases, from scanned documents, or entered manually, the database will find similar or matching voter data. Staff then can approve, fix, or dismiss, radically reducing the number of duplicate and incorrect voter files.



HOSTING INFRASTRUCTURE: *MEETING DOD AND NIST REQUIREMENTS*

One important building block to consider in the design of a VRS is where it will be hosted. Increasingly, the best option for hosting infrastructure is becoming cloud hosting.

Unfortunately, there is still a pervasive mindset that cloud-hosting is in some way unsafe; that if you can't touch it, it must not be real. An election administrator may believe that self-hosting is the best strategy for maintaining control, but this false sense of security can result in escalated costs, critical down-time, or security breaches.

With budgets and security being two of the biggest concerns when considering hosting, the best option is to trust a provider with vast knowledge and experience. It's financially impractical for election departments to staff an IT team and maintain in-house servers that could match the resources of a hosting service like AWS GovCloud, particularly considering that hosting mission-critical government agencies is their single focus.

Security

A google search for "Voter Registration System" returns numerous articles detailing recent hacking attempts. Not all internal IT teams have the experience to ensure security, while for AWS GovCloud, security is always the top priority. They are compliant with high-integrity regulatory requirements such as Department of Defense (DoD) Cloud Computing Security, U.S. International Traffic in Arms Regulations (ITAR), and Federal Risk and Authorization Management Program (FedRAMP) requirements. This frees IT staff to focus on other critical tasks.

Cost Effective

Researchers estimate that many companies spend as much as 75% of their IT budget on infrastructure alone. Using AWS results in savings up to 80% compared to self-hosting on premises (*https://d1.awsstatic.com/whitepapers/compliance/AWS_Security_at_Scale_Governance_in_AWS_Whitepaper.pdf*). The cost of physical servers aside, extraneous financial factors are eliminated with AWS GovCloud, such as the electricity costs to run in-house servers, IT resources, and software licenses.

The scalability of cloud hosting (see below) also plays a part in reducing costs. If temporary workers are hired for a month before an election and the system needs more capacity, cloud hosting only charges for the extra power as it's needed. With self-hosting, extra hardware must be purchased, and service paid for even though it's not needed during the rest of the year.

Scalable and Reliable

Cloud hosting allows performance scalability—efficiently accommodating the election cycle need for focused high performance followed by lower resource needs. For any critical operation like elections, uptime is a key consideration for a hosting solution. AWS GovCloud offers a 99.95% service commitment.

Redundancy

One failed in-house server would be reason enough to consider a cloud service. If a server fails in a physical datacenter, staff must either deploy a spare, or buy a new one very quickly. With cloud services, the host simply starts a new one. A cloud host also has multiple Availability Zones to easily backup data in geographically diverse locations. This eliminates the risk of having an in-house server damaged by a burst water pipe or vengeful former employee, or even being destroyed during a natural disaster, thereby taking crucial data with it.

Monitoring and Auditability

AWS and other cloud providers have robust, mature tools for monitoring infrastructure and keeping detailed records of what has changed, and who changed it. This would be massively costly and time consuming for an election office to re-create, and would also lack the integrity of an impartial third party logging changes in a neutral system. Another advantage is the ability to define "infrastructure as code". This allows software engineering best practices to be applied to the design and development of infrastructure, where changes can be applied automatically from a source code document using automated tooling.

Cloud storage is already a regular part of most people's lives—from banking to sharing music to online file collaboration—and with Government-focused hosting agencies, it has proven itself as a reliable option for hosting modern election management systems.

CONCLUSION

As the most integral, but potentially vulnerable, element of the election system, a Voter Registration System should use the most modern, secure, and future-proof technology available to the industry. The VRS feeds the entire election ecosystem and must feature precisely engineered technological components constructed for longevity and durability. The meticulous evaluation and selection of these systems by election officials will provide a legacy that will properly serve employees and voters in the future, while ultimately bolstering the national defense.

ABOUT VOTEM

Votem Corporation was founded in 2014 to foster and restore trust, access, and transparency in elections with a core focus on developing the most secure and verifiable voting platform globally.

Votem offers five voting products: online voting utilizing blockchain, online voter registration, voter registration and election management system, and remote accessible voting for military and overseas voters.

Votem
50 Public Square, Ste. 200
Cleveland, OH 44113

www.votem.com

© Copyright 2018 Votem Inc. Reproduction of this document, in whole or part, must not be performed without written consent of Votem, Inc.