vStructure™ Security

A VAZATA White Paper

Companies often underestimate the time, resources and efforts required to continuously and rigorously maintain compliance and secure computing in-house. Security systems require significant capital investments in hardware and software and are costly to implement, maintain and monitor. Outsourcing to the right provider enables businesses to achieve and maintain compliance while controlling costs.

Other companies turn to outsourcing because their current business volume has outgrown existing compliance resources. Customers are subject to increasingly complex compliance requirements as the amount of data and online computing grows. Meeting those requirements becomes extremely resource-intensive which makes outsourcing an attractive option.

Many cloud vendors provide public cloud solutions where you share resources - such as applications and storage – with the rest of their customer base over the internet. They present cost savings and easy access, but if you're interested in securing a mission critical application, then a public cloud solution poses risk. Capacity shortages and outages are unfortunate drawbacks to public cloud solutions and if you have security or compliance requirements, this is often not an option for you. While a private cloud offering may give a greater sense of comfort and control over virtualized resources, the economies of scale are no longer present. A compromise must be reached, and a provider must be chosen which can provide the benefits of a shared multi-tenant environment with a security-focused implementation usually reserved for private cloud environments.

Security in a Multi-tenant Environment

In order to achieve this balance, VAZATA has implemented a layered protection of its multi-tenant virtual environment comprised of Network (physical and virtual), VMware and administrative security for the vCenter™ management layer:

- All of VAZATA's vStructure™ IaaS solutions utilize dedicated ports and each customer is configured using dedicated VLAN(s) with continuity from the compute and storage infrastructure up through the security and routing infrastructures.

- The VMware bare-metal virtualization is built around the "VMkernel", a special-purpose microkernel that has a much smaller attack surface than a general-purpose operating system. VMware's ESX is designed for use in virtual production environments to prevent malicious activity and compromised network traffic from posing a threat to guest virtual machines. Since ESX is designed specifically for virtualization, there is no mechanism or need to share user information between virtual machines and their host. VMware bare-metal virtualization allocates resources intelligently while isolating virtual machines from underlying hardware components. No single virtual machine can use all the resources or crash the system.

- Strong isolation and strict separation of management greatly reduce any risk of harmful activity going beyond the boundaries of the virtual machine. Access to the vCenter™ management layer is restricted to certified personnel with permissions granted only as needed to perform individual, authorized functions. All access and permissions are removed as personnel leave the company or transition to other roles.

Additionally, VAZATA performs the following activities on a continuous basis:

- Host Hardening - Each host in the cluster is managed by Host profiles and VMware "update manager" to control configurations. All hosts are "locked down" per VMware best practices.

- Security Testing (e.g. vulnerability scanning and penetration testing) - VAZATA's infrastructure is regularly scanned via 3rd-party auditors.

- Customer Segmentation (e.g. network segmentation) – VAZATA segments customer configurations and traffic by locking down Layer 2's physical and virtual network, including dedicated VLAN configurations. VAZATA layers this configuration with isolation of the management layer and separation of administrative duties.

- Log aggregation and monitoring – The infrastructure is monitored by 3rd-party commercial applications utilizing both syslog approaches and domain audit approaches.

Data Security

VAZATA's virtual environment is built strictly around NIST definitions and standards for cloud computing (v26). The VAZATA virtual environment was designed for use by the Federal Government to address the Government's special computing infrastructure needs; specifically, its three major security concerns: Confidentiality, Integrity, and Availability.

By default, VAZATA segregates all data and network instances for different subscribers. Ensuring separation in a multi-tenant environment is a standard operating procedure within all Vazata virtual environments. All data at rest or in transit in a VAZATA environment will be handled IAW standard security procedures such as ISO 27001. All data remains both physically and logically secure while under control of VAZATA.

VAZATA is compliant with the FIPS 140-2 standards – the data are in the form of a LUN, which holds the image of the computer (the VMDK file).

VAZATA adheres to NIST Special Publication 800-88: *Guidelines for Media Sanitation*. The main objective of VAZATA security policy is to ensure that data are protected - - in all forms, on all media, during all phases of its life cycle - - from unauthorized or inappropriate access, use, modification, disclosure, or destruction. This policy applies to all VAZATA and customer data assets that exist throughout any of VAZATA's processing environments. The processing environment is collectively defined as all applications, systems, and networks that VAZATA or its agents own and operate.

VAZATA's security policy defines the overall security and risk control objectives that VAZATA endorses. The premise for the policy can be stated as: "Other than data defined as Public, which are accessible to all identified and authenticated users, all VAZATA and processing resources are only accessible on a need-to-know basis to specifically identified, authenticated, and authorized entities."