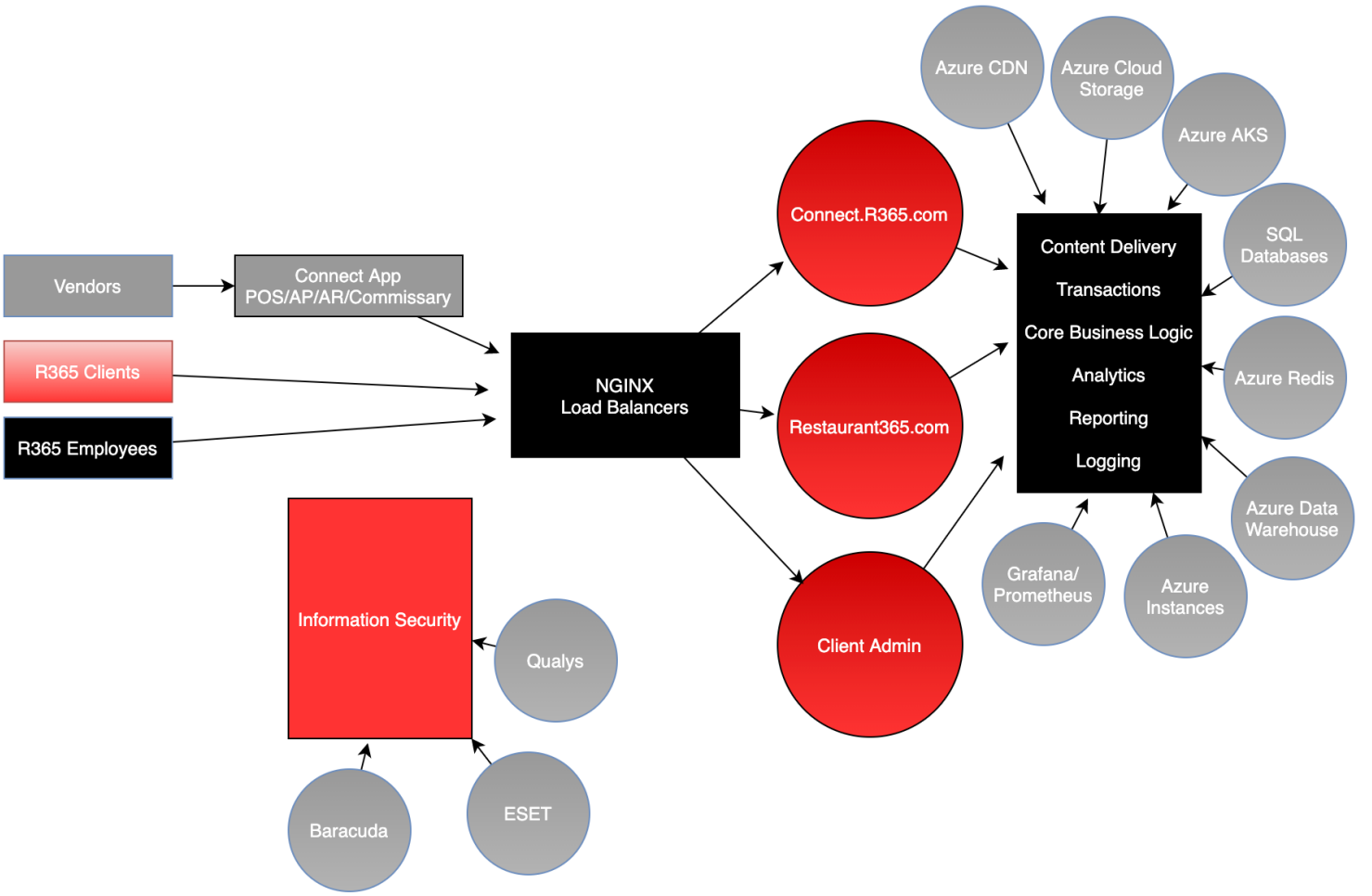
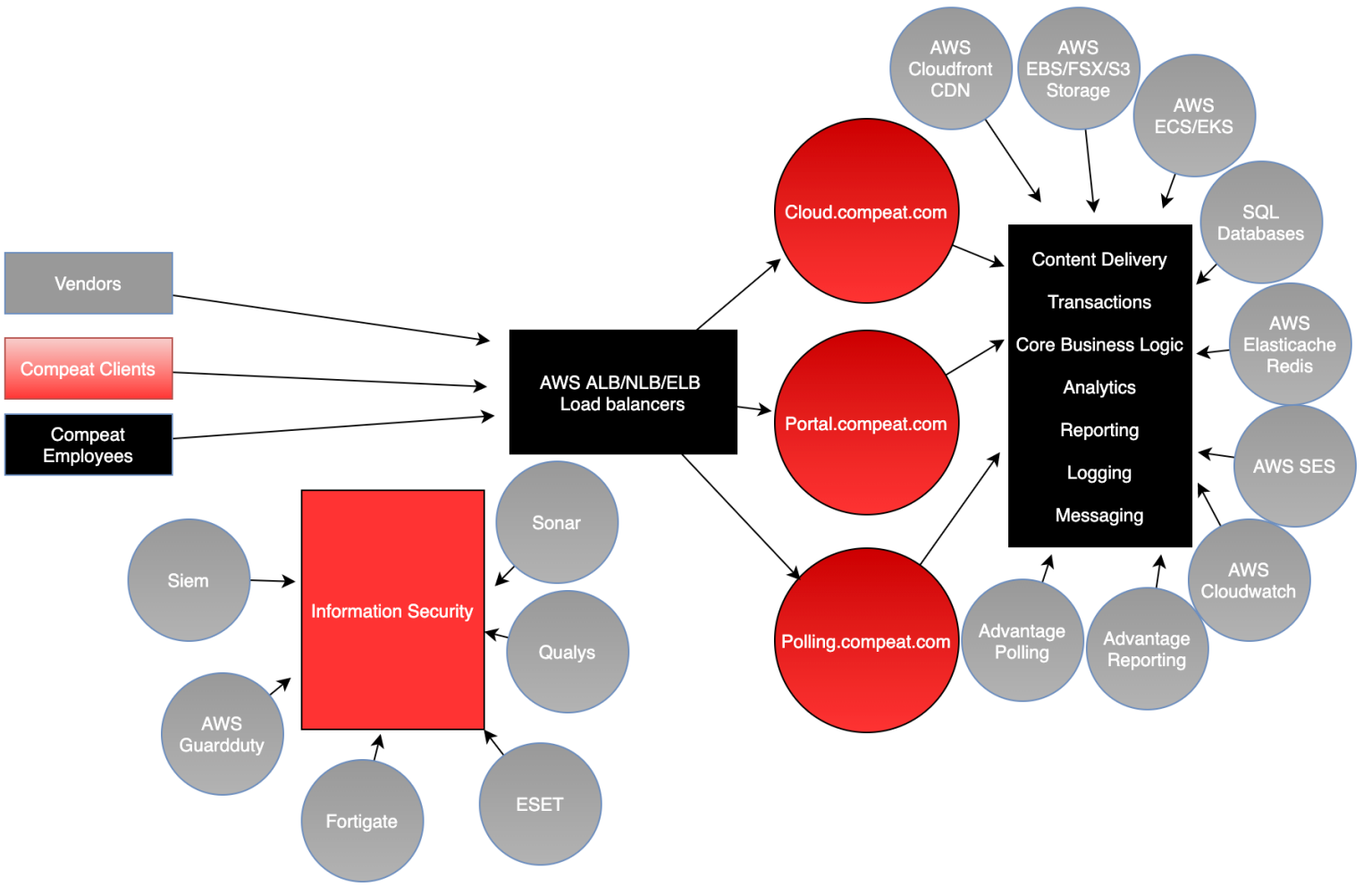
Restaurant365

Security Controls

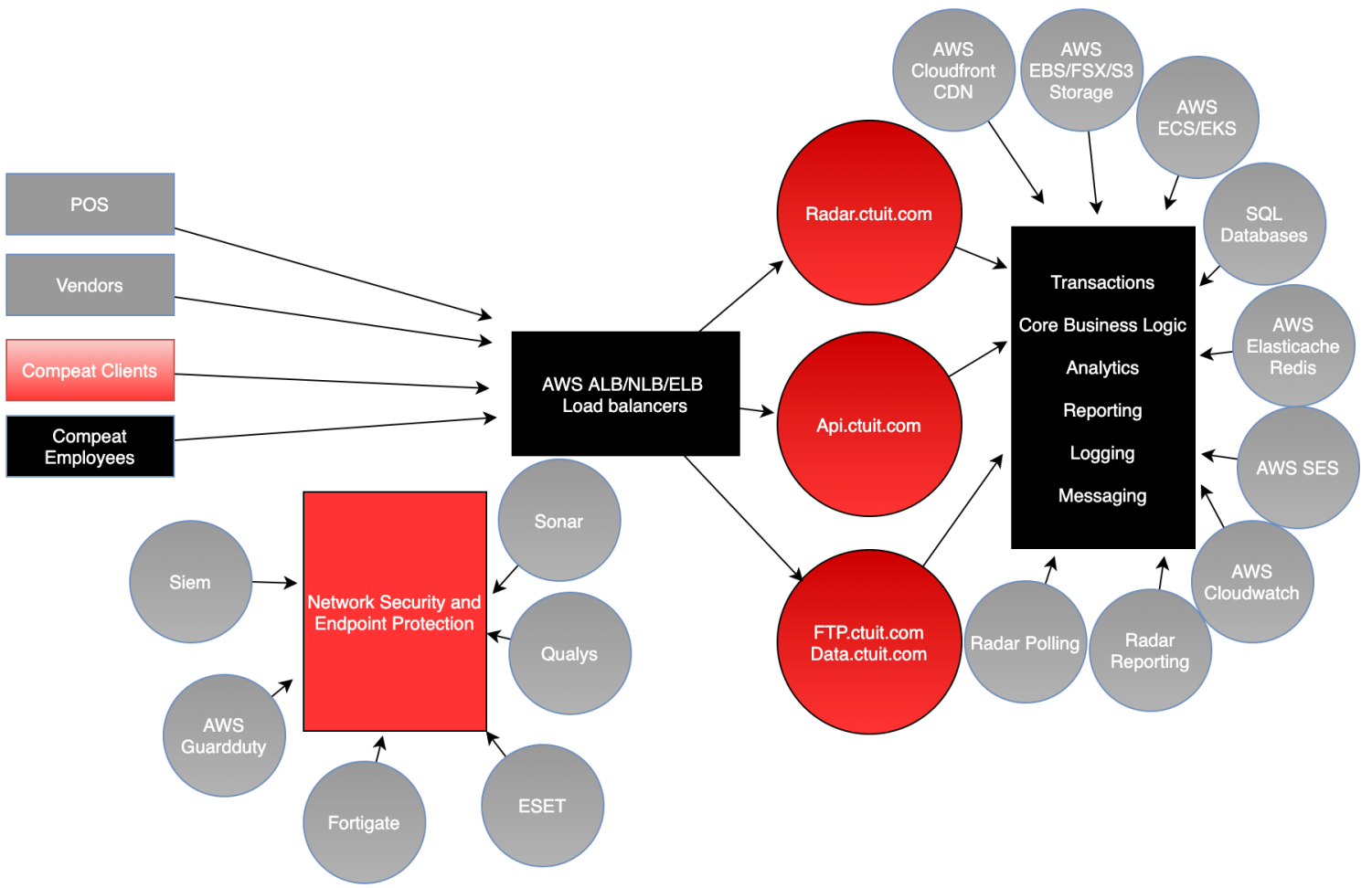
Restaurant365 System Architecture



Advantage System Architecture



Radar System Architecture



Infrastructure and Data

The Technology department is responsible for the development, integration, operation, and support of the: Restaurant365, Radar, and Advantage products. The Restaurant365, Radar, and Advantage products are based mainly on Microsoft .NET framework, and include services that are built on Angular and Node.js. The hosting infrastructure includes AWS Load Balancers (ALB, ELB, and NLB depending on the service), Nginx load balancers are also utilized to load balance Restaurant365 customer traffic across redundant services. The infrastructure for all products is composed of Windows and Linux servers, containerized applications running on Azure Kubernetes Services/AWS Elastic Container Services/AWS Elastic Kubernetes Services depending on the product. Content Delivery Networks are utilized such as AWS CloudFront for Radar and Advantage products, and Azure CDN for Restaurant365. The AWS S3/AWS FSX/AWS EBS/Azure blob services are used for storage. The applications are connected to SQL server databases for all products. Azure services are mainly utilized for the Restaurant365 product and AWS is utilized for the Radar and Advantage products. The Azure and AWS cloud providers are not included in the scope of this report.

The Restaurant365, Radar, and Advantage products utilize AWS services to host FTP/FTPS/SFTP servers for customer and vendor integrations. Integration services are utilized to collect Polling data from Point of Sale (POS) systems. Customers have polling clients in their environment, which send data for the various products. The polling data is automatically ingested, transformed, and written to the SQL databases. The polling files that are sent to the Restaurant365 and Radar products are proprietary to the company and are encrypted.

The Customer Success team utilizes Bomgar and LogMeIn tools to access the remote desktop of the customer's system. Radar polling clients are installed for the Radar customers, and A third-party tool Comida, is installed for Restaurant365 customers. These clients are utilized for gathering polling data from customers.

The corporate IT environment consists of Active Directory as the central authentication database, which authenticates users to provide access to the: Company's corporate services and applications, company network, file shares, and for any other tools needed to support the Restaurant365, Radar, and Advantage products.

This document serves as an overview of the security controls and practices of Restaurant365.

We strive to protect our client's data as well as our own.

Risk Management

Risk Management assessments are conducted annually to proactively identify risks, fraud prevention, as well as management and acceptance pertaining to information technology activities. As part of the Risk assessment: Vendors, technology, hosting and corporate assets and services are reviewed for any risks. Risks are reviewed by the Risk Management team, senior management, and the Board of Directors.

Software Development Lifecycle

Restaurant365 has a refined software development lifecycle (SDLC) to ensure all code is tested and approved prior to releasing it to customers. Customers receive only the highest-quality product. This process ensures any code defects are detected at development, quality assurance testing, or pre-release. This policy is to be adhered to by all staff, including employees, contractors, consultants, temporaries, volunteers, and vendors. Restaurant365 strives to achieve and provide the highest quality and reliable software.

Information Security Policies

Restaurant365 maintains formal and documented information security policies. The information security policies ensure that company assets and data are appropriately protected from unauthorized access and disclosure. The policies also ensure that the confidentiality and integrity of data is maintained throughout the

organization. Policy deliverables are formally reviewed and approved by information security management and senior management on a periodic basis, as are policy updates and revisions.

Incident Response Team

Restaurant365 aggregates performance metrics from infrastructure and the software application. Alerts are triggered based on abnormal behavior and delivered to the appropriate response team. Our response teams are available 24/7 and work immediately to resolve any triggered alerts before any degradation of services is experienced by customers.

SOC Compliance

Restaurant365 uses a reputable independent auditing firm to perform an assessment of its procedures and controls for SOC (SOC 1 and SOC 2 Type 2) compliance. Restaurant365 conducts SOC audits annually. Each control is tested, and the results are reviewed by the compliance team and senior management. The SOC audit is intended to provide customers assurance about the controls in place, integrity of systems, confidentiality, and privacy of the information processed by these systems at Restaurant365 are intact. These Standard Operating Procedures (SOP) are associated with trust criteria defined for Service Organization Controls ("SOC") reports. Trust services are a set of services based on a core set of criteria that address the risks and opportunities of IT and Hosting enabled systems and/or privacy programs.

Security Awareness & Training

Restaurant365 provides annual training for employees on data security and privacy.
This mandatory training course is designed to educate employees on safe handling of sensitive information, appropriate response to a suspected data security breach, and awareness around responsibilities for security.

Data Security Safeguards & Encryption

We protect our customer data with industry-accepted solutions and practices, including:

- Intrusion prevention system (IPS)/intrusion detection system (IDS)
- Web application firewalls (WAF)
- Network firewalls
- Virus/malware detection
- Penetration testing
- Vulnerability scanning
- Real-time monitoring and alerting.

Clients access our cloud SaaS environment via encrypted TLS sessions. Sensitive client information is encrypted both during transmission and at rest using industry standard protocols. All data or files transferred or uploaded to the Restaurant365 is encrypted during transmission.

High Availability & Disaster Recovery

Restaurant365 follows best practices for the continuity, availability, and reliability of customer and company operations critical to Restaurant365 and its customers. The infrastructure for Restaurant365, Radar, and Advantage are hosted AWS and Azure cloud. These cloud providers have enterprise-class data centers to ensure both the physical security of customer data and consistent uptime for our workloads. Customer data is safely copied to another region for Disaster Recovery purposes. Restaurant365 relies on a multi-tiered, redundant backup strategy to help ensure recovery of archived data. Backup procedures include snapshots of all critical customer data to geo-redundant locations, review of daily backup logs, full monthly backups, and daily differential backups. Backups are tested regularly to ensure recovery reliability. Offsite data backups are encrypted and securely transported to our secondary data center location.

Web Application Security

Restaurant365 promotes secure coding practices to eliminate OWASP vulnerabilities in its web application. In addition, the application is protected by multiple firewalls, including a web application firewall (WAF) to enhance the level of protection. The WAF decrypts the packets and does a deep analysis of the incoming payload to determine if the traffic is legitimate. The web application undergoes external penetration testing at least annually. Discovered web application vulnerabilities are remediated immediately. We strive to provide the most secure and highly available web application.

Restaurant365

949.652.7800
support@Restaurant365.com
www.Restaurant365.com