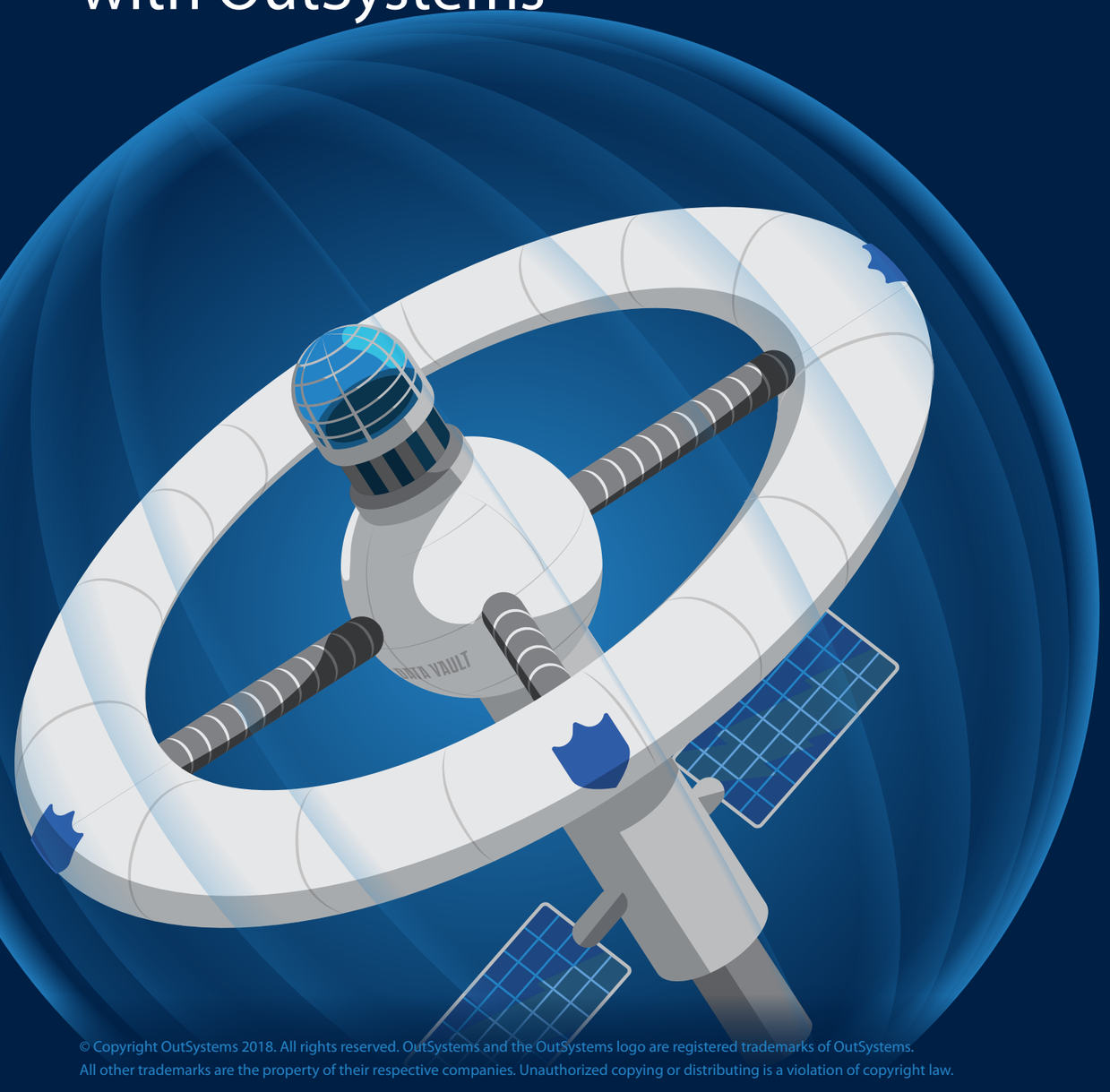
outsystems

Safeguard Your Applications with OutSystems



Organizations—especially those enabled with low-code—are creating applications at record speeds. All of those applications have something in common; they are creating more data, interfaces, supported devices, and environments to care for. At your new rapid delivery pace, who is looking after all of that new stuff? OutSystems is!

48%

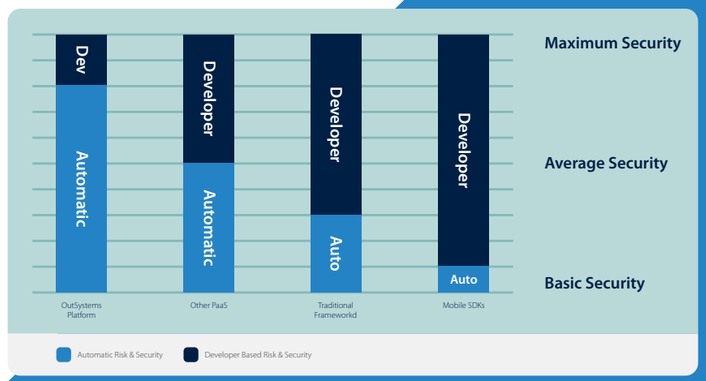
According to the 2018 DevSecOps Security Report, **48 percent** of developers know security is important but don't have enough time to spend on it[1].

Pretty scary statistic, right?

It is especially scary when you consider Forrester is predicting that one major brand will lose more than **25 percent** of its valuation in 2019 due to a cyber attack[2].

25%

With stakes that high, it is time to stop relying on error-prone human-based risk and security measures. Don't become one of 2019's security statistics. Let OutSystems remove a bulk of the risk mitigation and security burden from developers' already full plates.



OutSystems automatically applies an ever-growing list of risk and security controls to the OutSystems platform and the applications built on it. Just for starters, OutSystems application, infrastructure, and data protection controls protect your applications from the OWASP Top 10 Most Critical Web Application Security Risks, as well as the OWASP Top 10 Mobile Threats. The policies, procedures, and governance in place ensure OutSystems compliance and the security of your software supply chain.

Want to learn more?

Check out over 200 of the OutSystems Automatic Security and Risk Controls.

1) DevSecOps Community Survey 2018 (https://info.signalsciences.com/devsecops-community-survey-2018)

2) Forrester's Predictions 2019: Transformation goes pragmatic (https://mktg.forrester.com/predictions-2019)

Policies and Procedures

Prescriptive instructions for how security measures are determined and implemented.

COMPLIANCE AND GOVERNANCE
- Apps and APIs that conform to industry standards
- Internal apps and APIs conform to industry standards
- Regular audits to assess policies and procedures
- Control framework for policies and procedures
- IT governance based on industry standards
- Defined responsibilities with regular training
- Defined and tested backup and recovery plan
- Pre-authorize data center and operational changes
- Restrict software installed on devices with access
- Establish security requirement baselines
- Regular review of sensitive data handling
- Regular review of data retention handling
- Regular review of data classification and access
- Annual formal risk assessments
- Risk resolution service level agreements
- Annual reviews of network connections
- Legally defendable security forensic procedures
- Transparent supply chain agreements
- Third-party suppliers will comply with standards

PERSONNEL
- Documented administration and user guides
- Business partners adhere to policies and procedures
- Managerial accountability for security
- Authorized and published information security policies
- Security violation and employee sanction policy
- Regular review of security policy by leadership
- Asset return policy
- Employee background checks
- Documented change in employment procedures
- Non-disclosure and confidentiality agreements
- Security awareness program
- Points of contact for rapid engagement with law enforcement
- Contractual agreements to disclose security events

CHANGE CONTROL AND MONITORING
- 24/7 Monitoring of critical systems
- Risk from changes to business-critical apps and APIs
- Quality, change control, and testing processes
- All changes correspond to official change requests
- Risk management for infrastructure changes
- Access controls to all audit tools and data
- Track and quantify any security incidents

PHYSICAL SECURITY
- Monitoring and testing of data center environmental conditions
- Low-probability environmental risk locations
- Physical security perimeter and access
- Automatic equipment identification and authentication
- Preauthorization for equipment or data relocation
- Secure equipment and data disposal procedures
- Secure facilities for accessing sensitive information
- Restricted and monitored entry and exit to secure area
- Isolate secure area from service areas
- Restricted information access

IDENTITY AND ACCESS GOVERNANCE
- Controls to detect file integrity anomalies
- Controls to detect suspicious network behaviors
- Employee access authorization
- IT level permissions
- Customer access authorization
- Mobile device access management
- Management of bring-your-own-devices
- Access restriction and authorization to ports
- Roles-based access management
- Restricted access to data and/or intellectual property
- Third-party access will be restricted and monitored
- Restricted access to data replication
- Identity trust verification
- Account credential lifecycle management
- Account credential identity store minimization
- Authentication, authorization, and accounting rules
- Restricted access by utility programs
- Isolated multi-tenant environment

OPERATIONS AND PROCESSING INTEGRITY
- Malware on devices with access
- Vulnerabilities on devices with access
- Unauthorized mobile code
- Data confidentiality, integrity, and availability measures
- Cryptographic keys lifecycle management
- Encryption of sensitive data
- Unattended and unlocked workspaces policy
- Synchronization with reliable external time source
- Risk mitigation for future capacity requirements
- Triage process for security-related events

Application Protection

Encrypting and securing your data throughout the user's experience, from login to data entry, and data transport to inter-app operability.

IDENTITY AND ACCESS CONTROL
- Secure session cookies
- Hard-coded credentials
- Incorrect authorization
- Encrypted connection strings
- Strong password hashes

MOBILITY
- Device-to-backend access token security
- Secure device keystore
- Ciphered local storage
- Obscured mobile libraries
- Compromised device detection
- TouchID authentication
- App switching privacy screen
- MAM/MDM compatibility

THREAT AND VULNERABILITY MANAGEMENT
- Content security policies
- Code injection
- Unvalidated redirects
- Unvalidated forwarding
- Path equivalences
- Relative path traversal
- Absolute path traversal
- Cross-site scripting (XSS)
- Basic cross-site scripting
- IMG tag attribute cross-site scripting
- Web page attribute cross-site scripting
- Open URL redirects

CONTROL AND ERROR HANDLING
- Missing custom error page
- Improper input validation
- Error conditions without actions
- File descriptor leak
- Externally controlled references
- XML external entity references
- Unrestricted DTD references

APPLICATION LOGIC FLAWS
- Use of incorrect operators
- Dead code
- Unused variables
- Expression is always false
- Expression is always true
- Improper following of specifications
- Object reference to content comparison
- Double-checked locking
- Always false control flow
- Incorrect order of arguments
- One-way hash with no salt
- One-way hash with predictive salt
- XML entity expansion
- Operator precedence error
- Deadlocks
- Infinite loops
- Improper resource shutdown
- Improper resource release
- NULL pointer dereferences
- Unthread-safe singleton pattern
- Out-of-bounds protection

Data Protection

Proper data handling, storage, transmission, and destruction are critical to ensuring application data security.

ENCRYPTION
- Cloud-data-at-rest encryption
- Data encryption components
- SHA512 hashing algorithms
- Proper encryption for ecommerce data

HANDLING
- Deserialization of untrusted data
- Exposing information in log files
- Labeling, handling, and securing data and objects
- No replicating production data to non-production
- Definition of data stewardship
- Secure disposal and removal of data
- Safe destruction of temporary data
- Data and object classification

Continuity and Availability

Ensure maximum uptime and availability through proactive planning and service level determination.

HIGH AVAILABILITY / DISASTER RECOVERY
- Redundant equipment located at a reasonable distance
- Cloud database backups
- Distributed database replication
- Distributed front-end replication

POLICIES AND PROCEDURES
- Geo-specific business impact assessment
- Regular business continuity plan (BCP) audits
- Consistent BCP framework
- Regular BCP response testing
- Regular security incident response testing
- BC during equipment maintenance
- Defined impact analysis methodology
- List of assets with criticality and SLAs

Infrastructure Protection

Shore up the security of the backend with authentication, authorization, validation, and auditing to prevent security incidents.

THREAT AND VULNERABILITY MANAGEMENT
- DDoS attack
- IP spoofing
- Port scanning
- SQL injection
- User-level brute force attacks
- IP-level brute force attacks
- HTML injection
- JavaScript injection
- Command injection
- OS command injection

APIs
- Internal access for SOAP web services
- Basic authentication for REST APIs
- Client-side certificates
- Custom authentication methods for REST APIs
- Detailed API call audit logs
- Internal access for REST APIs
- OAuth 2.0 authentication for REST APIs
- SSL REST APIs

ENVIRONMENTAL
- Separation of production and non-production environments
- External control of file name or path
- Custom auditing engine
- Protection from known vulnerabilities
- ASP .NET environment misconfigurations
- Security misconfigurations
- Dedicated virtual private clouds
- Antivirus and intrusion detection

ENCRYPTED TRANSIT
- Use of HTTPS
- SOAP web services via SSL
- SSL pinning
- HTTP strict transport security (HSTS)
- HMACSHA1 encrypted REST cookies
- AES-128 CBC encrypted REST logins
- IPSec VPN connections to cloud

IDENTITY AND ACCESS CONTROL
- Multi-factor authentication access
- Integrated authentication for web apps
- Role-based access control
- Single sign-on support
- Native authentication
- Active directory authentication and authorization
- LDAP authentication
- External authentication integration
- Internal access configuration
- End-user access auditing
- Authentication for mobile backend endpoints
- Simple user decommissioning
- Developer action audit logs

OUTSYSTEMS ACTIONS
- Enforces
- Flags
- Implemented
- Prevents
- Provides

OUTSYSTEMS PLATFORM AVAILABILITY
- Cloud, Sentry, and On-Premise
- Cloud and Sentry
- Sentry Only

OutSystems

Automatic Risk and Security Controls

outsystems