herodevs

BALANCING INNOVATION AND SECURITY: HOW OBJECTIVE CORP MAINTAINED COMPLIANCE WHILE NAVIGATING COMPLEX MIGRATIONS

CLIENT PROFILE

Objective Corporation is a global leader in information governance and secure content management solutions, specializing in serving government agencies and corporate customers in highly regulated industries. With approximately 500 employees worldwide and millions of lines of code across multiple product lines, Objective Corp helps organizations manage sensitive information while maintaining strict compliance with industry regulations and security standards.

The company's solutions are particularly critical in government and regulated sectors where information security, governance, and compliance are non-negotiable requirements. Objective Corp's products are trusted across the Asia-Pacific region, North America, and the UK to securely manage some of the most sensitive information in the public and private sectors.

Objective

> **"Our customers operate in environments where security isn't just a feature—it's foundational. When you're handling sensitive government information or regulated corporate data, there are zero vulnerability policies making the stakes for security vulnerabilities extraordinarily high"** — Objective Corp

THE COMPLEX CHALLENGE

SECURITY DURING TECHNOLOGY TRANSITION

Objective Corp faced a multifaceted technical challenge that will resonate with many enterprise software providers. They were navigating a strategic transition from AngularJS to React across their product portfolio while simultaneously needing to maintain stringent security standards for their existing deployments.

This challenge was complicated by several factors:

1. Extended Support Cycles in High-Security Environments

Objective Corp's customers in government and regulated industries often maintain extended deployment cycles, sometimes running the same software version for extended periods of time due to their rigorous certification processes.

> "Our clients may not upgrade software less frequently due to their certification requirements. When you're dealing with sensitive government systems, you can't push updates every month. We need to maintain security for not only current versions, but multiple prior versions that are several years old."
> — Objective Corp

2. Complex and Large Codebase

With millions of lines of code across multiple products and versions, Objective Corp was managing a substantial technical landscape that had evolved over many years.

> "We're looking after millions of lines of code across complex products that have different versions in market simultaneously. Some customers are running very old versions of our software that still need to be protected." — Objective Corp

3. Evolving Technology Stack

The company was strategically transitioning from a diverse technology ecosystem (including Angular, AngularJS, Ember, Nuxt, and more) to standardize on React. However, this migration represented a significant undertaking that couldn't happen overnight.

> "We settled on React as our platform going forward, but we still have systems on AngularJS that need to be maintained securely during this transition period. We can't just drop everything and rewrite all our software at once." — Objective Corp

4. Stringent Compliance Requirements

As a provider to government agencies, particularly in the Asia-Pacific region, Objective Corp needed to maintain IRAP (Information Security Registered Assessors Program) accreditation—a rigorous security assessment framework that demands addressing all known vulnerabilities.

> "We weren't looking for new features in our existing code. We were specifically looking to have those vulnerabilities addressed to maintain our security posture, especially for our IRAP accreditation in the APAC region." — Objective Corp

THE STRATEGIC DILEMMA

Objective Corp faced a classic technology management dilemma with significant business implications. They needed to:

1. **Address security vulnerabilities** in their existing AngularJS-based applications
2. **Maintain compliance certifications** crucial for their government customers
3. **Continue their strategic migration** to React for future development
4. **Preserve development resources** for forward-looking initiatives

The traditional approach would have required dedicating a full engineering team for 6-12 months to accelerate the migration from AngularJS to React—a significant diversion of resources from their product roadmap and innovation initiatives.

> "We estimated that a full migration would require a dedicated team for six to twelve months—effectively losing a team for that long was not an option. That's a substantial impact on our roadmap and ability to deliver new capabilities to customers." — Objective Corp

THE SOLUTION

STRATEGIC SECURITY MAINTENANCE

After evaluating their options, Objective Corp partnered with HeroDevs to implement a focused security solution that would maintain the integrity of their AngularJS-based systems while allowing their strategic migration to continue at an appropriate pace.

The HeroDevs solution provided:

1. **Targeted Security Patching:** HeroDevs' Never-Ending Support for AngularJS addressed specific vulnerabilities in third-party components without requiring wholesale changes to the application code.
2. **Compliance Maintenance:** The solution ensured that applications remained compliant with security standards required for government certification.
3. **Resource Optimization:** By adopting this approach, Objective Corp could maintain a small team focused on security while keeping most resources dedicated to strategic initiatives.

> "We prefer to address technical debt in a coordinated manner alongside adding new capabilities. HeroDevs allowed us to maintain security while continuing our migration at a pace that makes sense for our business and customers." — Objective Corp

IMPLEMENTATION

MINIMAL DISRUPTION, MAXIMUM IMPACT

The implementation of HeroDevs' solution was remarkably efficient, requiring changes primarily to build environments for two of Objective Corp's main products. The process was completed within a couple of sprint cycles, with minimal disruption to ongoing development efforts.

Technical Implementation

The implementation focused on updating dependencies in the build process to use HeroDevs' secured versions of AngularJS components. Here's a simplified example of the implementation approach:

```
// Before: bower.json with vulnerable AngularJS dependency {
"dependencies": {
"angular": "1.6.9",
"angular-route": "1.6.9",
"angular-sanitize": "1.6.9",
"angular-resource": "1.6.9"
// other dependencies
}
}

// After: Using HeroDevs NES secured versions via npm // package.json
{
"dependencies": {
"@herodevs/angular": "1.6.9-nes.1",
"@herodevs/angular-route": "1.6.9-nes.1",
"@herodevs/angular-sanitize": "1.6.9-nes.1", "@herodevs/angular-resource": "1.6.9-nes.1"
// other dependencies
}
}

// Example: Main application file
// The AngularJS application code remained unchanged angular.module('objectiveApp', [
'ngRoute',
'ngSanitize',
'ngResource',
'objectiveApp.documents',
'objectiveApp.workflow'
])
.config(['$routeProvider', function($routeProvider) { $routeProvider
.when('/documents', {
templateUrl: 'views/documents.html',
controller: 'DocumentListCtrl'
})
.when('/documents/:id', {
templateUrl: 'views/document-detail.html',
controller: 'DocumentDetailCtrl'
})
.otherwise({
redirectTo: '/documents'
});
}]);

// Example controller - secure without any code modifications angular.module('objectiveApp.documents',
[])
.controller('DocumentDetailCtrl', ['$scope', '$routeParams', 'DocumentService', '$sce',
function($scope, $routeParams, DocumentService, $sce) { var docId = $routeParams.id;
// Load document content
DocumentService.getDocument(docId)
.then(function(response) {
$scope.document = response;
// Use $sce.trustAsHtml - now secured without code changes
$scope.documentContent =
$sce.trustAsHtml(response.content);
})
.catch(function(error) {
$scope.error = 'Failed to load document: ' +
error.message;
});

// Document permissions
$scope.canEdit = false;
DocumentService.checkPermissions(docId)
.then(function(permissions) {
$scope.canEdit = permissions.write;
});
}
]);
```

copy

This approach allowed Objective Corp to address security vulnerabilities without disrupting their application code or requiring extensive testing cycles.

> "The implementation required minimal effort. We made changes to our build environments for our two primary products, and that was essentially it. The solution integrated seamlessly with our existing codebase." — Objective Corp

RESULTS

SECURITY, COMPLIANCE, AND STRATEGIC FOCUS

The implementation of HeroDevs' solution delivered immediate and substantial benefits for Objective Corp:

1. Maintained Security Posture

The solution effectively addressed critical vulnerabilities in AngularJS components, ensuring that Objective Corp's applications remained secure even as they continued their strategic migration to React.

2. Preserved Compliance Certification

By eliminating known vulnerabilities, Objective Corp maintained its compliance with stringent government security standards, particularly the IRAP accreditation crucial for its government clients in the Asia-Pacific region.

> "Maintaining our security posture, especially for our IRAP accreditation in APAC, is absolutely critical to our business. HeroDevs helped us achieve this without disrupting our development roadmap." — Objective Corp

3. Resource Optimization

Instead of dedicating a full team for 6-12 months to accelerate migration, Objective Corp was able to address security concerns with minimal resources while keeping their strategic initiatives on track.

4. Business Continuity

The company could continue serving its government and regulated industry clients with confidence, knowing that its applications met the necessary security standards despite using frameworks that had reached end-of-life. New customers evaluate the company’s security posture and having a secure version where vulnerabilities are remediated immediately resolves that concern for them, strengthening the potential relationship.

> "For us, it's about zero tolerance on third-party vulnerabilities. Having that black-and-white assurance lets us confidently say 'yes' to customer security requirements and move on—especially since most customers won't even discuss functionality until security is checked off." - Objective Corp

WHY THIS MATTERS

THE CONFLICT BETWEEN INNOVATION AND SECURITY

The Technical Debt Balancing Act

Objective Corp's experience highlights a universal challenge facing technology organizations: balancing the need to address technical debt with the imperative to innovate and move forward.

"Every CTO faces the same fundamental question," reflects Objective Corp. "How do you allocate limited resources between maintaining existing systems and building the future? When those existing systems support critical business functions, you can't simply abandon them, but you also can't let them consume all your development capacity."

This tension is particularly acute for organizations serving government and regulated industries, where extended support cycles and rigorous security requirements create a long tail of maintenance responsibilities that can span years or even decades.

Breaking the Binary Choice

The traditional approach to this challenge presents a binary choice: either divert substantial resources to accelerate migration and modernization, or accept increasing security risk and potential compliance issues. Objective Corp's experience demonstrates that this binary framing is unnecessarily limiting.

"What we learned through this process is that technical debt management doesn't have to be all-or-nothing," explains Objective Corp. "You can take a more nuanced approach that addresses critical security concerns while still advancing your technical roadmap."

This insight has profound implications for how organizations approach technology evolution:

Strategic Prioritization

"We've shifted from thinking about technology migration as a monolithic project to viewing it as a series of strategic decisions where security, business value, and technical advancement are weighted appropriately," notes Objective Corp. "Not everything needs to move at the same pace."

Compliance as an Enabler

Rather than viewing security compliance as a constraint, Objective Corp has repositioned it as a business enabler. "By ensuring our existing systems remain secure and compliant, we actually create more space for innovation elsewhere. We're not constantly fighting security fires or rushing migrations to address vulnerabilities."

Partner-Enhanced Capabilities

"Working with specialized partners like HeroDevs has expanded how we think about our capabilities," shares Objective Corp. "We don't have to build every solution in-house. For specialized needs like framework security, the right partner can deliver better results more efficiently than we could internally."

THE PATH FORWARD FOR ENTERPRISE SOFTWARE

For other organizations maintaining complex software portfolios while serving security-conscious customers, Objective Corp's approach offers valuable guidance:

1. **Disaggregate security from feature development:** Address security vulnerabilities separately from functional enhancements to enable more focused, efficient solutions
2. **Plan migrations strategically, not reactively:** Create migration timelines based on business value and strategic priorities rather than framework end-of-life dates
3. **Leverage specialized expertise** for targeted challenges rather than diverting internal resources from strategic initiatives
4. **Quantify the full business impact** of different approaches, including opportunity costs of delayed innovation

> "The most valuable insight from this experience is that maintaining security and compliance doesn't have to come at the expense of innovation and progress. With the right approach and partners, you can do both effectively. For organizations serving government and regulated industries, this balance isn't just technically important—it's a strategic business advantage." — Objective Corp