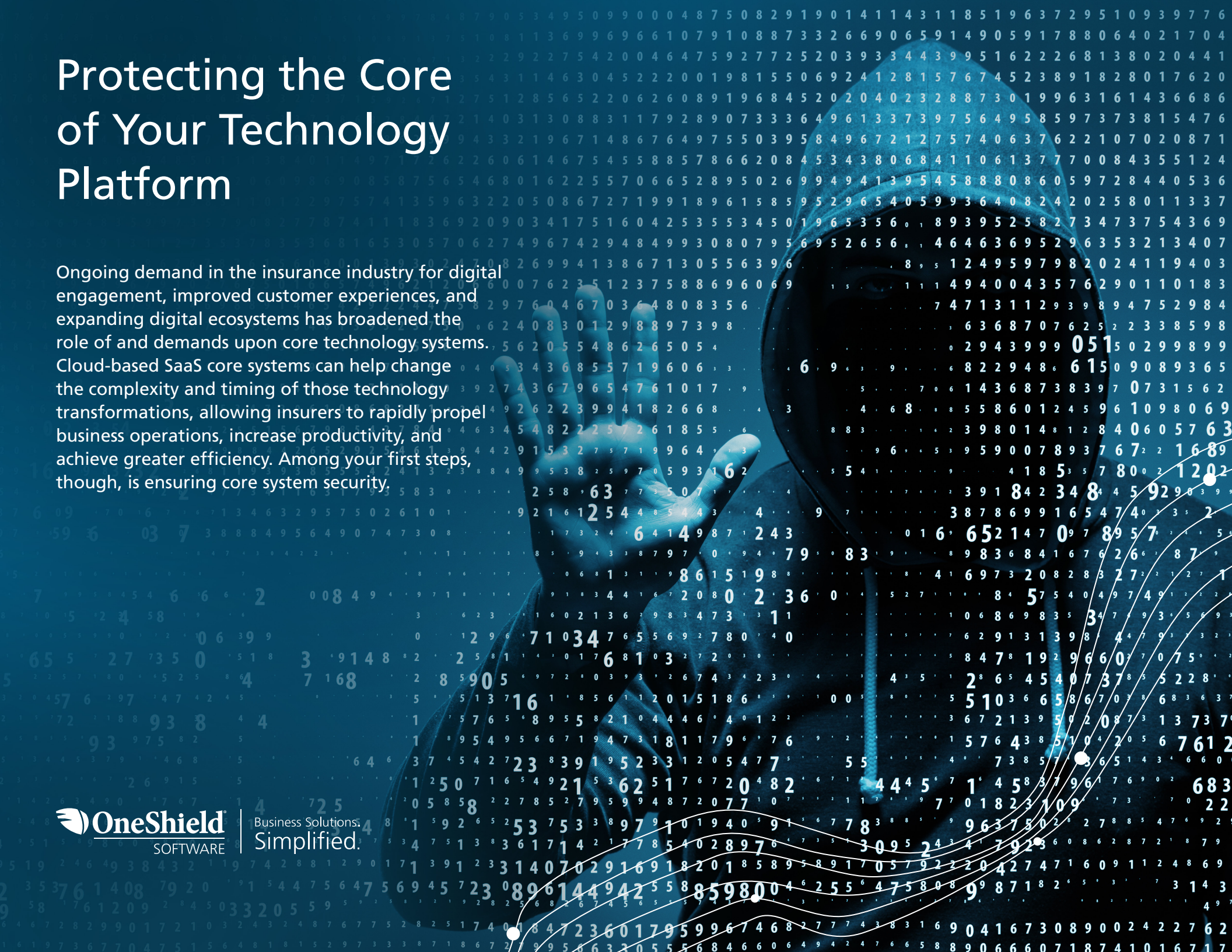
Protecting the Core of Your Technology Platform

Ongoing demand in the insurance industry for digital engagement, improved customer experiences, and expanding digital ecosystems has broadened the role of and demands upon core technology systems. Cloud-based SaaS core systems can help change the complexity and timing of those technology transformations, allowing insurers to rapidly propel business operations, increase productivity, and achieve greater efficiency. Among your first steps, though, is ensuring core system security.



OneShield SOFTWARE | Business Solutions. Simplified.

Protecting the Core of Your Technology Platform

Key Findings

- A robust and secure core system environment not only helps you compete with other tech-savvy carriers, but it also ensures your organization can pivot when the extraordinary happens, such as the recent COVID-19 pandemic and global disruption.
- Increased customer personalization, the flexibility of offerings, real-time pricing changes, consumer-activated insurance, and many other product innovations all require rigorous adherence to industry security standards.
- With the evolution of data governance and consumer privacy concerns, countries have implemented strict security and breach notification laws that require businesses to notify consumers if personal information is compromised, with potentially significant damages to be paid if security due diligence is not maintained and breach notification policies not implemented.
- Security breaches worldwide are increasing at an alarming rate.

Recommendations

- The more you understand about cybersecurity, compliance obligations, best practices, and the tools available, the more equipped your organization is to move forward in securing business transformation.
- Embracing and championing a culture of strict adherence to security best practices by implementing a security program and framework which improves your products and corporate security posture brings awareness and culture change needed to adapt to the changing landscape.
- A secure core system environment requires a security program that is in alignment with business goals for executive buy-in and investment.
- In addition to understanding the regulatory environment that applies to the security and privacy aspects of your business operations, there are crucial controls that need to be put in place to ensure adherence to compliance and overall consumer confidence in your products.
- Ensuring a secure core system environment begins with choosing a technology vendor and partner that has security uppermost in the design and implementation of your business' digital platform.

Table of Contents

Introduction

If we have learned anything from recent events, it is that the test of an insurance organization's core systems comes not from the ordinary operation but extraordinary unforeseen developments. OneShield has always placed security best practices at the forefront of every aspect of our company culture and software development processes. It is key to helping protect our clients' interests, and to providing solutions that improve the experience between people and insurance products.

The current pandemic and ensuing economic disruption notwithstanding, the increasing demand for digital engagement, improved customer experience, and the need for expanding ecosystems has broadened the role of, and demands upon, core systems in both digital and data directions. SaaS core systems help to change the complexity and timing of technology transformations. This technology allows insurers to rapidly stand up business operations, focusing on their business, not the technology stack. Not only does this help to increase overall productivity and meet the ongoing demands of business operations with greater efficiency, it also facilitates the ability for an organization to pivot when the extraordinary happens.

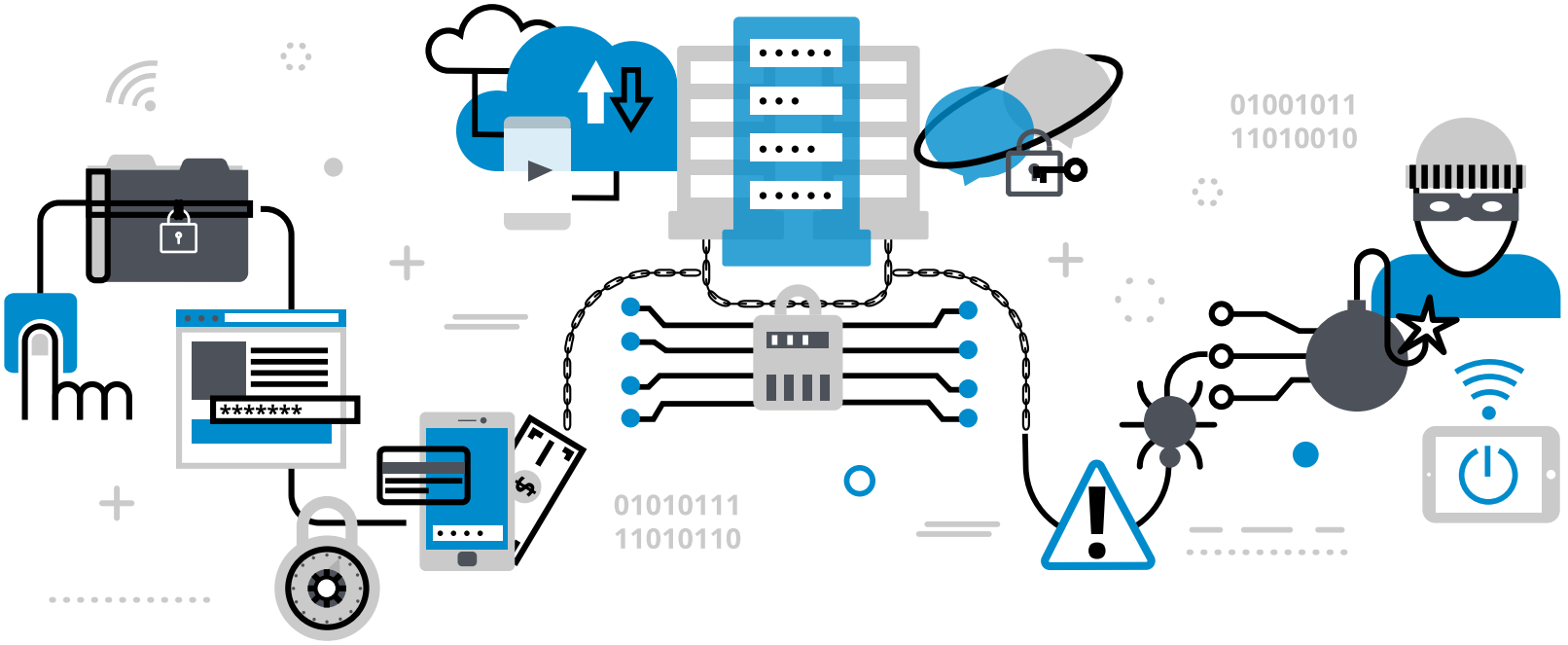
That's why OneShield is committed to system security. We provide built-in security with a framework that exceeds industry best practices and the regulatory compliance needs of our clients. We understand you may be concerned about moving to the cloud or employing SaaS systems, but now more than ever is the time to transform core systems to enable your organization to address business needs quickly. Increased personalization, the flexibility of offerings, real-time pricing changes, consumer-activated insurance, and other product innovations can be the difference in responding to both ordinary market competition and extraordinary market disruptions. The more you are aware of cybersecurity and the tools available, the more equipped you will be to move forward in securing your future transformation.

Cyber Security Defined

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. These malicious attacks (cyber-attacks) are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

The need for stronger cloud security has never been greater. Implementing effective cybersecurity measures is particularly challenging today because not only is the industry dealing with unprecedented – if, likely, short-term – economic disruption, there are more devices than people, and attackers are becoming more innovative. There are many new and evolving security tools and best practices to better understand the breadth of security controls available to help protect your organization's data. It's important to increase your security posture; and secure your apps, data, and network across cloud and hybrid environments.

A successful cybersecurity approach has multiple layers of protection spread across the whole of an operation — computers, networks, programs, and data. In an organization, the people, processes, corporate culture, and technology approach must all complement one another to create an effective defense from cyber-attacks.



Worldwide spending on cybersecurity is forecast to reach

$133.7 billion in 2022.

(Gartner)

68% of business leaders

feel their cybersecurity risks are increasing.

(Accenture)

Data breaches exposed

4.1 billion records

in the first half of 2019.

(RiskBased)

More than

77% of organizations do not have a cybersecurity incident response plan.

What's worse? An estimated 54% of companies say they have experienced one or more attacks in the last 12 months.

(Hiscox Cyber Readiness Report)

Security breaches have increased by

11% since 2018 and 67% since 2014.

(Accenture)

The average lifecycle of a breach was

314 days

(from the breach to containment).

(IBM)

The average cost of a data breach is

$3.92 million as of 2019.

(Security Intelligence)

The Evolving Set of Rules and Regulations Informing How We Move Forward

There is no single principal data protection legislation in the U.S. Rather, there is an uncoordinated collection of hundreds of laws enacted at the federal and state levels to serve and protect personal data of U.S. residents. All 50 U.S. states, as well as the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands, have breach notification laws that require businesses to notify consumers if their personal information is compromised. These new and amended state data breach laws expand the definition of personal information and specifically mandate that certain information security requirements are implemented.

There are several cyber protection laws to understand and monitor as they continue to evolve and impact your data management obligations:

- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)
- Australia NDB Scheme
- New York Department of Financial Services cybersecurity regulation 23 NYCRR 500

Risks Are Great and Responsibilities Even Greater

Understanding their implications and adhering to their standards to protect corporate and personal data is necessary. In the case of both General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), there are many consumer privacy implications that were introduced with these laws. How you collect, store, report on, and delete consumer data has never been as important as it is today. Consumer data rights continue to be at the forefront for lawmakers and their constituents. These rights translate into business requirements, which are only going to be more stringent as time goes on. Having a core system that is configurable and flexible is critical to ensuring you can keep up with the changing requirements and meet the challenges of tomorrow.

Security Starts with You

Embracing and championing a culture of strict adherence to security best practices through awareness and training is the best preventative medicine. In a mobile world, security awareness has never been as important as it is today. With an uptick in phishing and malicious activities to the tune of 700% since the COVID-19 government stay at home order, all employers and employees need to be diligent. You must know your obligations to your employers through policy reviews. Your new core systems projects must incorporate industry and compliance obligations to ensure that the workflows you customize align with security and business goals.

And, it is important to understand that this is not a once-and-done task – security practices must adjust as the possible risk to the environment changes. Again, flexibility from a core system is key.

What Keeps You Secure?

Keeping your organization's operations secure requires a series of disciplines, protocols, and practices. There are many types of security measures you can employ:

1. Secure Development Program

A software development program based on proven industry secure frameworks and controls with security checks throughout the software development lifecycle.

2. Secure API

75% of the most recent cyber attacks have targeted the business logic and API in general. Given this vulnerability OneShield uses automation to test the security of its API and microservice architecture throughout the software development lifecycle. This is because security testing most often is limited to penetration tests, Static Application Security Testing (SAST), and Dynamic Application Security Testing (DAST) that does not address the growing concerns with API breach and RBAC (Role-Based Access Control).

3. Authentication

Authentication services are key to controlling who has access to your systems. You can use OneShield's native authentication or integrate another preferred Identity Provider (IDP). OneShield supports many Multifactor Authentication (MFA) options and a range of modern security factors for implementation flexibility.

4. Web Service Security

All OneShield web service integrations with external systems are built using transport confidentiality, server authentication, user authentication, transport encoding, and message integrity. Web services are encrypted using TLS with certificates from trusted providers, as well as digital certificates for files and documents.

5. Single-Sign-On (SSO)

Integrate your software applications with a single sign-on portal through SAML 2.0 integration for secure identity management.

What Keeps You Secure?

6. Object-Level Authorization

Establish specific role-based authorization and access for users and groups. Authorization can be controlled down to the level of every business object.

7. Transaction Security

Ensure you have native support for TLS 1.2 or above encryption and run-time validation of user actions. Built-in SOA framework for integration with external authorization and custom authorization rules. Application logic is carried out through stored procedures based on internally generated session ID, action ID, and object ID that are validated by the workflow engine.

8. Secure Client Data

Data masking can be utilized to hide original data in configurable fields to protect personal information, which is completely customizable.

9. Logs and Audit Trails

In addition to producing logs and audit trails, ensure these logs and audit trails are properly secured, maintained, or for as long as the customer requires, and are accessible for forensic investigation.

10. Data at Rest

Data at rest or data stored in persistent storage should be encrypted using the Advanced Encryption Standard (AES).

11. Key management

With native integrations to industry-leading key management solutions, be sure to have secure keys and tokens to protect sensitive data.

What Keeps You Secure?

12. Firewalls

Implement Web Application Firewalls (WAF) and Next-Generation firewalls with an enhanced level of filtering and control. Intrusion detection system (IDS) and intrusion prevention systems (IPSs) can monitor all traffic to and from the application.

13. Latency

Worldwide data center support for OneShield Cloud implementation allows us to meet region-based regulatory requirements and lower latency for global customers.

14. Regulatory Requirements

Regulators around the world are hyper-aware of threats to data and are placing increased demands on the industry. Staying abreast of pertinent existing and changing regulations strengthens our security strategy.

The OneShield Perspective

Since its inception, OneShield has maintained that security is paramount to providing exceptional solutions for insurance providers. Through the solution delivery process, we work with our partners to provide world-class applications and infrastructure that allow our clients to rest easy and focus on the business of their business.

As a software vendor, we secure our environments, data, clients, and employees. As well, we ensure we develop our software products to abide by and support robust security practices. At OneShield, we embrace a security culture, employing a new level of documentation and process to the organization and continuously introducing new improved methodologies to ensure our security practices are top-notch. We regularly roll out company-wide training programs for all employees and conduct security tests randomly.

From a development perspective, we introduced new methodologies, such as OWASP application security verification standards, that provide a basis for testing web application technical security controls, including giving developers a list of requirements for secure development, aligning with the PCI – PA-DSS standard, scanning all libraries at build time, conducting vulnerability checks, developing new security recommendations, and much more.

Conclusion: Security Empowered Clients

The flexibility of our platform allows OneShield to adapt very quickly to changes in the dynamic cybersecurity environment, including changes to regulations and privacy laws. Whether it is a workflow change to address concerns of the California Consumer Privacy Act, new object encryption based on expanding private data definitions, or substantive change to the overall market environment, OneShield's platform provides the tools necessary to adopt rapid change.

There are many considerations when approaching core system transformation. Security is one of them, but it should not steer your organization away from cloud solutions employing SaaS systems. OneShield's SaaS solutions enable insurers to rapidly propel business operations, increase overall productivity, and meet the ongoing demands of business operations with greater efficiency.

About OneShield Software

OneShield provides solutions for insurers of all sizes. Deployed in the cloud, our portfolio of standalone, subscription, and As-a-Service products include enterprise-class policy management, billing, claims, rating, product configuration, business intelligence, and smart analytics. OneShield automates and simplifies the complexities of core systems with targeted solutions, seamless upgrades, collaborative implementations, and lower total cost of ownership.

With corporate headquarters in Marlborough, MA, and offices in India and Canada, OneShield has 50+ products in production across P&C and specialty insurance markets.

Ready to transform your business?
Contact us today at info@oneshield.com
www.oneshield.com