

ServiceMaster deploys cyber-safeguards to enable DevOps speed

Transforms applications using HPE Security technology

Objective

Protect business reputation by reducing the risk of cyber-security breaches while deploying new application functionality daily

Approach

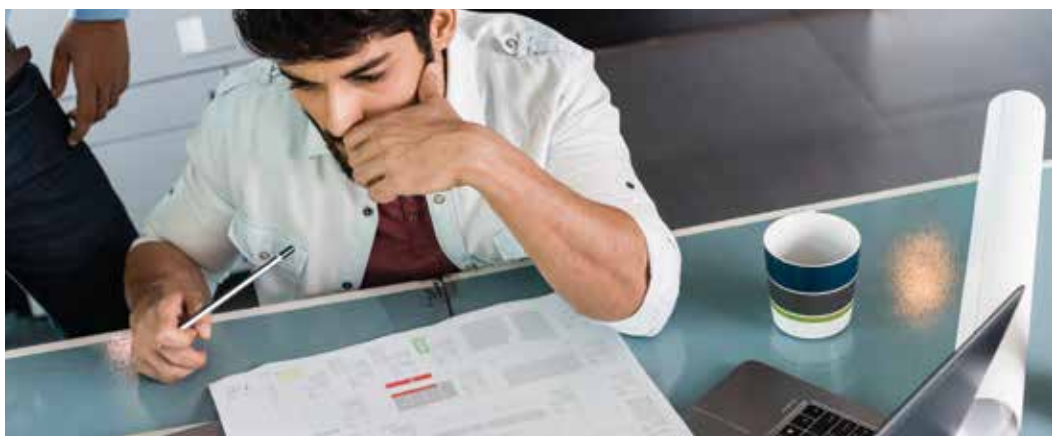
Integrate application security into the software development lifecycle (SDLC) and DevOps deployment process, so that ServiceMaster produces more secure software, and detects and defends against application attacks

IT Matters

- Identifies risk of applications and deploys appropriate defensive measures
- Fully integrates into the SDLC
- Tests software within 24 hours, allowing rapid development
- Provides static and dynamic testing, reducing vulnerabilities and threats to the business's reputation
- Allows applications to detect and block cyber-attacks, protecting operations
- Reduces configuration requirements, improving security

Business Matters

- Enables rapid software development and deployment via DevOps, so the business can be more agile
- Increases security without adding more employees
- Improves developers' programming skills, reducing risks to the business's reputation



ServiceMaster Global Holdings, Inc. has been in business for more than 85 years and provides services to more than 75,000 homes and businesses across North America each day. Through the company's seven brands, including Terminix, Merry Maids and American Home Shield, ServiceMaster cleans properties, protects them from pest infestation, restores them

after disasters, and provides other services. In 2016, *Fortune* magazine named ServiceMaster one of its World's Most Admired Companies.

With customers and competitors gravitating to doing more of their business online, ServiceMaster wanted to re-energize the business with a major digital transformation that embraced social media, mobile, and the web. But as cyber-security breaches increased, the management team decided to further invest in protecting the company's reputation. Security products could reduce these risks, but it might also be costly and disruptive to operational business plans.

“Executive support and buy in across the business has been critical to our success. Development and Security working together to ensure we do the right thing for our customers and our business is key. Discovering vulnerabilities up front in the development process and educating developers to think “secure” while delivering their work is changing the way we work and deliver. This journey has been a huge team win for partnership WITH Security, culture change to an agile mindset and creating a better, sustainable process for the future.”

– Jennifer Cole, CISO, ServiceMaster

As part of ServiceMaster’s digital transformation in cyber-security, the company is also overhauling its approach to operations and application development. ServiceMaster has focused development teams working on features such as online bookings and mobile apps, and connecting disparate back-end systems to increase business and operational efficiency. Also, security is built into the development lifecycle without having to hire a full in-house security testing team.

The company has achieved this by implementing and using Hewlett Packard Enterprise (HPE) Security Fortify on Demand and HPE Security Fortify Application Defender, which protect code without slowing down the business.

The opportunity

ServiceMaster’s “digital first” strategy is transforming the way it does business—giving consumers the ability to interact with the company when, where and how they want. This involves a major push to re-engineer legacy systems in a way that improves efficiency and supports new ways of doing business online. For example, mobile apps will help sales people be more effective, better back-office systems will allow projects to be approved and funded faster, and online bookings will enable ServiceMaster to cross-sell the services of the company’s various brands.

“We want to be recognized as the leader in home services,” explains the company’s Director of Information Security, Thomas Davis.

To do this, ServiceMaster has shifted to a much faster way of creating and deploying software, embracing DevOps methods, so the company can respond swiftly to new business opportunities. For example, this might allow ServiceMaster’s Terminix business to act quickly in response to new pest control problems.

Undergoing such a digital transformation, ServiceMaster has the potential to increase its exposure to application security risks. Experts estimate that a high percentage of all business software has security vulnerabilities, and these can go unpatched for weeks or even months. And although network firewalls and intrusion detection systems protect a company’s network perimeter, application vulnerabilities can present a gap in security defenses. Cyber-attack techniques such as SQL injection target this security blind spot.

To ensure that the company can identify and fix vulnerabilities in real-time, its IT project teams have moved away from a “waterfall” approach (an extended period of programming leading up to the delivery of code for testing) and moved to the Agile and DevOps methods. This switch allows teams to work on software in increments and perform rapid development ‘sprints’ with daily releases. With the DevOps approach, risks

are minimized by reviewing flaws, bugs and vulnerabilities in the development lifecycle prior to release. Automation has played a key role in enabling the process, code verification and release into production.

Solution and benefits

Finding vulnerabilities quickly

ServiceMaster has taken a comprehensive approach to application security, making it an integral part of the company's software development lifecycle (SDLC). Attention is paid to correctly training developers and providing them with appropriate architectural standards and technologies so they can create more secure applications. The approach includes analyzing the security of applications at the design stage and analyzing static code to minimize vulnerabilities during development. After the application is deployed, dynamic analysis (provided by HPE), penetration testing, and runtime application self-protection (RASP) can also identify vulnerabilities or defend against threats, further reducing the risk of breaches.

“I think it's been a good partnership because HPE is listening.”

- Thomas Davis, Director of Information Security, ServiceMaster

Additional security tools, such as intrusion prevention systems (IPS), intrusion detection systems (IDS), and security information and event management (SIEM), combined with application security tools, help reduce risks.

ServiceMaster uses HPE Security Fortify on Demand, an online service that tests code very quickly, so that ServiceMaster's security teams can focus on other key security functions. By doing so, ServiceMaster can perform testing 24x7 and scale testing demand as needed for DevOps, while minimizing the number of vulnerabilities and risks to the company's reputation.

“We wanted a program, not a security tool.”

- Thomas Davis, Director of Information Security, ServiceMaster

Key to this success has been the short timeframe for testing. ServiceMaster's developers can upload their code at the end of the day and receive a report the next day detailing vulnerabilities and how to fix them.

Because test results arrive soon after developers write the code, it is easier to address and correct vulnerabilities early on. This allows the company to act faster to execute business plans.

HPE and its partner Saltworks Security work closely with ServiceMaster to ensure the application security process has a minimal impact on the developers. Saltworks Security's founder Dennis Hurst and HPE representatives attend regular developer meetings at ServiceMaster to ensure everything is on track, and Saltworks is providing full-time resources to act as a Security Scrum Master, ensuring that application security requirements are met throughout the SDLC, minimizing re-work and delays to production.

“We didn't want a bolt-on solution, we wanted a program,” Davis says. “We've got every tool in the world here, but that doesn't do you much good. You have to get business value out of it.”

Reducing risk

Testing at other points throughout the cycle helps proactively identify security risks. HPE Security Fortify on Demand tests static code during development, and dynamically tests live web and mobile applications after deployment. This continuous testing and feedback streamlines operations, allowing developers to move at a much faster pace.

Developers are also learning from the test results how to write more secure code. Fewer identified vulnerabilities means greater protection for ServiceMaster's reputation.

Customer at a glance

Application

Vulnerability testing and application self-protection for application security

Software

- HPE Security Fortify on Demand
- HPE Security Fortify Application Defender

“If you don’t have this protection, you can’t release software rapidly and confidently.”

– Dennis Hurst, founder, Saltworks

The company’s developers are embracing this security-focused mindset. ServiceMaster gamified the Fortify on Demand criticality metrics and developers are competing to earn five star ratings. “That caught on with the developers and now they are saying ‘how do I get the five stars?’. They’ve really taken ownership of the code and the issues,” Davis says.

Protection from within the application

As well as reducing vulnerabilities during the programming stage, ServiceMaster is taking another important step: arming its Security Operations Center (SOC) with visibility to see potential application-targeted attacks, and allowing applications to block attacks themselves.

By using HPE Security Fortify Application Defender, developers can easily add security instrumentation to the application’s runtime environment. This means that ServiceMaster’s defenses do not need to eliminate all software vulnerabilities before deployment. If a vulnerability exists in production, Application Defender can detect potential exploits, alerting the SOC, and it can block attempts to exploit it.

Even with HPE Security Fortify Application Defender only partially deployed, ServiceMaster’s developers are already finding it takes only a few seconds to add the security to the runtime environment.

“If you don’t have this protection, you can’t release software rapidly and confidently,” says Saltwork’s Hurst.

This confidence and enhanced visibility allow ServiceMaster to save time by re-deploying code. “It lets them use web services in a lot of different ways,” says Hurst. “They’re not fragile; they’re resilient to attack. Otherwise there would be additional concerns, costs, stress, and time.”

Re-energizing the business

With ServiceMaster developers moving fast, the company’s digital transformation continues to move ahead. American Home Shield is leading ServiceMaster’s digital transformation; sales through the American Home Shield’s e-commerce channel grew by nearly 45 percent in 2015, and the number of sales leads have also increased. Digital engagement was a key factor in generating new leads and increasing customer loyalty.

ServiceMaster’s new development and deployment methods are even beginning to play a leading role in the company’s IT recruiting strategy. ServiceMaster has released a video promoting the company as a dynamic place to work.

Davis credits HPE for not just providing a security product, but helping to enable a faster way of working. “I think it’s been a good partnership because HPE is listening,” he says.

As a result, developers can uphold ServiceMaster’s brand values. “We want our brand to mean something. We want it to be strong. You can’t have a digital first strategy and it not be resilient,” he says.

Learn more at
hpe.com/software/fortify



Sign up for updates

★ Rate this document