Table of Contents

Executive Summary ................................................. 3
Infographic: Key Findings ....................................... 4
Introduction ......................................................... 5
DevOps Security Trends ......................................... 7
Best Practices of Top-Tier Enterprises ..................... 13
Conclusion .......................................................... 14
Executive Summary

The Fortinet 2019 State of DevOps Security Report looks at the risk implications of the rapid rise of the DevOps methodology in enterprises around the world. We surveyed DevOps leaders at large enterprises to get their perspectives, and identified a number of trends:

1. **DevOps is an increasingly visible and important function**, with 69% of DevOps team leaders reporting directly to a member of the C-suite.

2. **Security is becoming a bigger concern for DevOps teams**, but only 19% of DevOps leaders said they were measured on identifying security vulnerabilities.

3. **While the security operations center (SOC) is gaining more visibility into DevOps activities**, only 14% of organizations have enabled full visibility of the DevOps environment from their SOCs.

4. **Even though DevOps teams identify many vulnerabilities before production**, problems persist post-production: 92% of organizations have seen at least one vulnerability slip into production in the past 12 months.

5. **DevOps professionals want security tools that reduce risk without impeding their work**—and their fear is that security solutions will inevitably slow their projects down.

Analyzing the data more deeply, we identified a subset of respondents who reported that no vulnerabilities had made it into production in the past 12 months, and another subset who had seen 10 or more vulnerabilities slip through. We identified these as “top-tier” and “bottom-tier” organizations. Comparison of the two groups shows that top-tier organizations are significantly more likely to follow these best practices:

- Security audit tracking
- Tracking and reporting on compliance with security standards
- Tracking and reporting security compromises
- Dependencies analysis
- Scanning public cloud instances for misconfigurations
- Vulnerability assessment and management scanning
- Monitor and manage code commits

Our findings indicate that traditional approaches to network security are inadequate in a DevOps environment. Like DevOps itself, DevOps security—or DevSecOps, as it is increasingly called—must be scalable, agile, and automated. Network security must be seamlessly integrated into the DevOps infrastructure and processes, with full visibility of the entire attack surface from a single location. Advanced threat detection must be in place to minimize false positives, and response must be automated so that DevOps processes are not slowed down. Organizations that adhere to a holistic, fully integrated approach to security can reap the benefits of DevOps without increasing risk.
Infographic: Key Findings

- 69% of DevOps leaders report to the C-suite.
- 70% of organizations are rolling DevOps security under the CISO (in the next 12 months).
- 14% of organizations have full visibility of DevOps activities in the SOC.

The typical organization experienced 3 to 5 vulnerabilities in production (in the past 12 months).

What DevOps leaders look for in a security solution:
- ✓ risk reduction
- ✓ increased flexibility
- ✓ tighter integration
- ✓ time savings

Compared with bottom-tier organizations, top-tier organizations are:
- 187% more likely to do security audit tracking
- 96% more likely to do dependencies analysis
- 63% more likely to scan cloud instances for misconfigurations
- 45% more likely to monitor and manage code commits.
Introduction

Companies of all types are reinventing their internal processes and systems to stay competitive in a fast-paced and ever-changing market landscape, and an increasing number have embraced DevOps methodologies. DevOps brings together two teams in an organization that have historically worked in silos—software development and IT operations—speeding up each step of the process through integration of effort and automation of processes.

A “DevOps toolchain” typically goes in the sequence of Plan, Create, Verify, Package, Release, Configure, and Monitor, forming a continuous flow through development and operations with the goal of continuous improvement. Optimizing and automating each of these processes has the potential to be transformative for an organization, delivering business agility, faster time to market, the ability to make adjustments on the fly, and shorter time to recovery when problems do occur.

As organizations recognized this potential, DevOps went mainstream in 2017, with 84% of enterprises adopting some DevOps principles and 30% applying them companywide. The trend has continued in 2018. While most organizations have not fully merged their development and operations teams, 70% of organizations now report that they use an automated approach to create and manage code. “DevOps Engineer” as a job title was uncommon two years ago, but now is the most popular description for this type of work. Organizations are clearly embracing DevOps, and many are already realizing significant business benefits from the rapid, streamlined process flow it enables.

However, the accelerated timelines brought by DevOps can present significant security risk—especially if speed is valued over security. In a recent survey, 52% of companies admit to scaling back security measures to meet a business deadline or objective. Similarly, 68% say their CEOs demand that DevOps and security teams never slow down a business process. Here, likely the result of these pressures, the speed at which code was published was a factor in high-profile data breaches.

At the same time that companies are sacrificing security for speed, the threat landscape is becoming more complex, faster moving, and automated. In the third quarter of 2018, FortiGuard Labs noted almost 34,000 new malware variants—a 40% increase over the second quarter and a 126% increase over the first quarter. Cyber criminals now use advanced technologies such as artificial intelligence (AI) and swarm technology—as well as DevOps itself—to create single-use malware that targets a particular organization across several points of the attack surface.

These factors make it unsurprising that a term like DevSecOps would become more common. This indicates that companies are realizing the need for a secure approach to DevOps.
Methodology for This Study

The Fortinet 2018 State of DevOps Security Report is based on an October 2018 survey of individuals who:

- Work at companies with more than 2,500 employees
- Have the job title of DevOps manager, director, or vice president
- Are involved with the purchase of security solutions for the DevOps environment

Our respondents come from a variety of industries, including technology, manufacturing, retail, healthcare, and financial services.

This study utilizes data from the survey to identify a number of current trends around DevOps security. We then delve more deeply into the data to identify a subset of organizations that avoided any vulnerabilities being discovered in production over the past 12 months, and looked at what they are doing differently.
DevOps Security Trends

Trend: DevOps Is an Increasingly Visible and Important Function in the IT Group

The fact that job titles using the term “DevOps” are increasingly common means that the methodology is becoming more of a standard in a variety of industries. Where these professionals sit in the organization indicates the importance of the role. Half of our respondents have job grades at the vice president (20%) or director (30%) levels, while the other half are managers and senior managers.

Even more telling is the reporting structure for these professionals. More than two-thirds of our respondents (69%) report directly to a member of the C-suite, while 30% report to a director of IT operations. The most common executive to which our respondents report is the chief technology officer (CTO) (32%), but some report to the CIO (16%), CISO (9%), and others. The DevOps role is clearly seen as strategic and top of mind for company executives.

The DevOps professionals in our survey are clear-headed when thinking of how they can best be successful. While DevOps advocates envision quick adoption of the methodology across an organization, 59% of respondents admit that choosing the right DevOps projects is a top-three issue impacting their ability to be successful. This suggests that organizations are deploying DevOps methodologies using a deliberate, phased approach, and that DevOps professionals are looking for “quick wins” that can bolster organizational buy-in for expansion of the approach.

Immediately below choosing the right DevOps projects, several factors are in a virtual tie for second, and one of those is integration of security into DevOps processes—identified as a top-three concern by 44% of respondents.
Trend: Security Is Becoming a Bigger Concern for DevOps Teams, but They Are Not Measured Directly on Security Metrics

Impending changes at many organizations illustrate that organizations are recognizing the importance of DevSecOps. The CISO currently manages DevSecOps at just one-quarter of organizations, but 70% of respondents said that the CISO would be in charge of that function within the next 12 months.

As a result, while the DevOps professional manages security for his or her environment at 33% of organizations today, two-thirds of those leaders will relinquish the security function to the CISO within a year. Similarly, while 49% of the DevOps professionals in our survey are currently the final decision-makers for DevOps security solutions, this will presumably change at companies where DevOps security is to be rolled under the CISO.

As a result, while the DevOps professional manages security for his or her environment at 33% of organizations today, two-thirds of those leaders will relinquish the security function to the CISO within a year. Similarly, while 49% of the DevOps professionals in our survey are currently the final decision-makers for DevOps security solutions, this will presumably change at companies where DevOps security is to be rolled under the CISO.

Top Three Success Measurements for DevOps Leaders

- Efficiency/Productivity Gains: 51%
- Cost Reduction: 50%
- Software Code Issues: 42%
- Alignment with Business Priorities: 41%
- Time to Market: 39%
- Velocity of Software Updates/Releases: 32%
- Volume of Software Updates/Releases: 26%
- Security Vulnerabilities Found: 19%

Rank 1st more than others
One thing hopefully will not change: the DevOps professional regularly provides input into security purchase decisions at 75% of organizations. At least some aspects of DevOps security are included in risk scores reported to executive management at 99% of organizations, and DevOps security is a part of what is reported to the CISO at 62% of organizations.

These findings confirm that security is a significant part of the day-to-day work of the DevOps leader. However, security is less prevalent in these professionals’ job descriptions and success measurements. Fewer than half of respondents (48%) reported that embedding security within DevOps processes is a part of their responsibilities. And that number will likely shrink as the CISO assumes responsibility for DevSecOps.

When it comes to how DevOps professionals are measured, security represents an even smaller slice of the pie. Only 19% of respondents indicated that identifying security vulnerabilities in DevOps releases was among their top three success measurements. Instead, the most common success measurements are efficiency/productivity gains, cost reduction, and time to market—all of which could potentially incentivize the DevOps leader to take security shortcuts.

Responsibilities of DevOps Professionals

- Design, Build, and Manage DevOps Operations: 72%
- DevOps Team Supervision: 70%
- Select and Manage DevOps Tools: 67%
- Lead the Use of DevOps Frameworks: 49%
- Manage Automated Workflow Capabilities+: 49%
- Embedding Security within DevOps Processes: 48%
- Manage Production and Development Server Operations: 37%
- QA for Site/Software Testing: 36%
Trend: The Security Operations Center (SOC) Is Gaining More Visibility Into DevOps Activities, but Visibility Is Far from Complete

The SOC has become more involved in DevOps security of late, and 53% of our respondents report that the SOC tracks all DevOps activities from a security perspective. An additional 42% of organizations report that the SOC tracks some of these activities. However, our other findings in this regard show that organizations have a long way to go to bring the full DevOps environment under the protection of security operations teams.

For example, only 14% of organizations say that the SOC has centralized visibility into all DevOps activities. This suggests that if the SOC truly tracks all DevOps activities, a large amount of manual work must be done to bring the required visibility. This increases risk from threats that move at machine speed and creates the potential for security incidents arising from human error.  

A small majority of organizations (51%) report that most DevOps activities are centrally visible within the SOC, but even these organizations can have significant gaps that pose risk to the organization. And for more than one-third of organizations (35%), half or less of DevOps activities are visible from the SOC.

On a positive note, security issues arising in the DevOps environment are tracked and reported at a solid majority of organizations. This tracking includes security compromises (73%), compliance with regulations (63%), compliance with standards (60%), and vulnerabilities (56%).

![DevOps Activities Centrally Visible in SOC](image)

<table>
<thead>
<tr>
<th>DevOps Issues Tracked and Reported</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Compromises</td>
<td>73%</td>
</tr>
<tr>
<td>Compliance with Industry Regulations</td>
<td>63%</td>
</tr>
<tr>
<td>Compliance with Security Standards</td>
<td>60%</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>56%</td>
</tr>
<tr>
<td>Results of Penetration/Intrusion Tests</td>
<td>36%</td>
</tr>
</tbody>
</table>
Trend: DevOps Teams Identify Many Vulnerabilities Before Production, but Large Gaps Remain

As DevOps security becomes a more visible concern, DevOps teams are getting somewhat better at identifying vulnerabilities before releases go into production—but they still need to make significant progress. While 58% of our respondents report that a majority of vulnerabilities are identified before production, and an additional 24% say they identify approximately half of them, it goes without saying that catching most vulnerabilities means that some do get through.

Indeed, our survey finds that eight in 10 organizations (80%) have discovered at least three vulnerabilities after a release was in production in the past 12 months, and only 8% of organizations have caught all vulnerabilities before production over that time span. Each vulnerability that makes it into newly developed code presents risk to an organization, so a substantial problem still exists.

In terms of security tools that might help improve these numbers, DevOps professionals report that most of the tools they care most about are already in place. By far the most common deployment is security analysis functionality within DevOps tools—in place at 73% of organizations. Five other solution types were also in use at more than half of the organizations surveyed. However, significant gaps remain, as basic functionality like automated security scanning and vulnerability assessment and management scanning is present at barely half of organizations.
**Trend: DevOps Professionals Want Security Tools That Reduce Risk Without Impeding Their Work**

Respondents have some negative feelings about security technology in general—perhaps because their success measurements focus on speed and efficiency over security. Specifically, when asked how security solutions can negatively impact success, respondents’ biggest complaints were business concerns: slowing of development cycles, increased complexity, and adoption of challenging security standards. Another way to phrase their concern is to say that a siloed and tactical approach to security is not agile enough for a DevOps environment—especially with an ever-changing and accelerating threat landscape.

Yet, it would be hard for these professionals to deny that DevOps security issues that are not managed effectively also have a negative impact on time to market. In their responses to a series of questions about what they are looking for in a security solution, DevOps professionals paint a picture of a security architecture that provides real protection without sacrificing the agility they need to do their job.

Specifically, DevOps leaders seek security vendors that save time, reduce effort, and provide easy access to security information. Operationally, respondents value integration, organization, and simplification. Strategically, the most important elements are risk reduction and flexibility. And with regard to vendor relationships, responsiveness and expertise are most sought after.

In general, DevOps leaders indicate that a new approach to security is required to support and protect their new approach to application development. A fully integrated and automated approach to security will protect the DevOps environment along with the rest of the network.

<table>
<thead>
<tr>
<th>STRATEGY</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Reduction</td>
<td>46%</td>
<td>20%</td>
<td>25%</td>
</tr>
<tr>
<td>Flexibility</td>
<td>26%</td>
<td>33%</td>
<td>20%</td>
</tr>
<tr>
<td>Reach</td>
<td>16%</td>
<td>19%</td>
<td>32%</td>
</tr>
<tr>
<td>Component Quality</td>
<td>12%</td>
<td>27%</td>
<td>23%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PRODUCTIVITY</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Savings</td>
<td>33%</td>
<td>16%</td>
<td>25%</td>
</tr>
<tr>
<td>Reduced Effort</td>
<td>18%</td>
<td>21%</td>
<td>23%</td>
</tr>
<tr>
<td>Information Access</td>
<td>26%</td>
<td>19%</td>
<td>13%</td>
</tr>
<tr>
<td>Decreased Hassles</td>
<td>11%</td>
<td>25%</td>
<td>18%</td>
</tr>
<tr>
<td>Transparency</td>
<td>9%</td>
<td>19%</td>
<td>21%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OPERATIONS</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration</td>
<td>21%</td>
<td>29%</td>
<td>12%</td>
</tr>
<tr>
<td>Organization</td>
<td>21%</td>
<td>18%</td>
<td>21%</td>
</tr>
<tr>
<td>Simplification</td>
<td>22%</td>
<td>19%</td>
<td>11%</td>
</tr>
<tr>
<td>Configurability</td>
<td>14%</td>
<td>11%</td>
<td>21%</td>
</tr>
<tr>
<td>Connection</td>
<td>13%</td>
<td>15%</td>
<td>17%</td>
</tr>
<tr>
<td>Availability</td>
<td>9%</td>
<td>8%</td>
<td>18%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VENDOR</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration</td>
<td>30%</td>
<td>25%</td>
<td>25%</td>
</tr>
<tr>
<td>Organization</td>
<td>30%</td>
<td>23%</td>
<td>19%</td>
</tr>
<tr>
<td>Simplification</td>
<td>13%</td>
<td>26%</td>
<td>19%</td>
</tr>
<tr>
<td>Configurability</td>
<td>15%</td>
<td>20%</td>
<td>24%</td>
</tr>
<tr>
<td>Connection</td>
<td>11%</td>
<td>8%</td>
<td>13%</td>
</tr>
</tbody>
</table>

Most Important Factors When Selecting Security Vendors
Best Practices of Top-Tier Enterprises

While the vast majority of enterprises still discover vulnerabilities in DevOps projects after they go into production, 8% of our respondents (the “top-tier” organizations) report that no security issues made it into production in the past 12 months. On the other hand, 13% of our respondents (the “bottom-tier” organizations) had 10 or more vulnerabilities sneak into production before they were discovered. In this section, we look at the disparities between these two groups to identify best practices that can help organizations bring their DevOps security to the next level.

1. Top-tier organizations are almost three times as likely to do security audit tracking.

Security audits use established regulations and standards to measure an organization’s security posture objectively. While audits and compliance can be seen as a checkbox, the standards they are based on are actually designed to make an organization more secure. Automated tracking generates reports on a scheduled basis, and issues that are identified are more front of mind—and thus more likely to be dealt with. Notably, top-tier organizations are 187% more likely to have automated security audit tracking than bottom-tier organizations.

2. Top-tier organizations are 45% more likely to track and report on compliance with security standards.

As with audit tracking, tracking an organization’s compliance with security standards such as those of the National Institute of Standards and Technology (NIST)—and remediating instances of noncompliance—makes an organization more secure. Organizations that measure themselves against standards that are not required by regulations show maturity in their security posture.

3. Top-tier organizations are 63% more likely to track and report on security compromises.

As the old business adage goes, “What gets measured gets improved.” While tracking and reporting on security issues seems very basic from an IT security standpoint, this is not always a standard process in a DevOps setting. Here, it should not be surprising that top-tier organizations are much more likely to have introduced this practice in the DevOps environment.

4. Top-tier organizations are almost twice as likely to do dependencies analysis.

Like software development projects in general, DevOps projects use a lot of third-party and open-source code—and most organizations have no idea what dependencies their applications have. Failing to account for dependencies has the potential to introduce vulnerabilities that originated outside the company. In this case, top-tier organizations are 96% more likely to have an automated way to check for dependencies.

5. Top-tier organizations are 63% more likely to scan public cloud instances for misconfigurations.

Incorrectly configured public cloud instances are the root cause of many data breaches. With most organizations operating dozens of services in multiple clouds, many of which support DevOps, automatic scanning is the only workable way to identify these issues before they cause a problem. Top-tier organizations tend to follow best practices more fully in this regard.

6. Top-tier organizations are 45% more likely to do vulnerability assessment and management scanning.

While many organizations have a vulnerability scanning solution in place, scanning is only one element of a comprehensive vulnerability assessment. From a DevOps perspective, this can be the difference between a vulnerability being caught before production and one that is missed.

7. Top-tier organizations are 45% more likely to monitor and manage code commits to protect data.

Every code commit that is added to a repository can potentially introduce a vulnerability to the final version of the code that goes into production. Top-tier organizations are more likely to have an automated way to monitor and manage the code history and versions to ensure that vulnerabilities are discovered and remediated.
Conclusion

DevOps offers organizations significant advantages, including the opportunity to accelerate digital transformation and meet business objectives faster. But DevOps also presents serious security challenges. When the right security architecture, technologies, and processes are in place, organizations can manage their DevOps risk posture—proactively and effectively. This is corroborated with a comparison of top- and bottom-tier organizations in the study:

- They monitor their overall security posture with as many scans, assessments, and analyses as possible.
- They report security metrics to the larger organization, including on security standards that are not required by regulations.
- They have technology in place to automate these processes and provide real-time information about vulnerabilities, compliance, and an organization’s overall network security posture.

Survey findings also reveal that organizations are recognizing the need to manage DevOps security risks centrally and are making it the responsibility of the CISO. Traditional approaches to network security simply do not have the agility to support a DevOps environment.

But with or without DevOps, organizations need to develop integrated and automated network security simply to address the current threat landscape—in which cyber criminals are also using advanced technologies such as artificial intelligence and swarm technology to create customized threats that move at machine speed. Ideally, the demands of the DevOps environment might motivate organizations to make changes that make the entire organization more secure.
Reference List
