

A Custom Technology Adoption Profile Commissioned By BMC Software | October 2017

Overcoming SecOps Hurdles Decreases Risk While Increasing DevOps Efficiency

GET STARTED ▶



A Custom Technology Adoption Profile Commissioned By BMC Software | October 2017

Overcoming SecOps Hurdles Decreases Risk While Increasing DevOps Efficiency

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

Overview

Organizations struggle to keep up with security and compliance requirements that often result in changes to infrastructure. Making the matter worse, the ability to not only identify but prioritize and remediate risks becomes even more complex as organizations increasingly pursue and adopt hybrid cloud architectures. Security and IT operations (SecOps) teams today need to enable location agnostic policy automation and remediation across bare metal, private cloud, public cloud, and hybrid environments.

BMC Software commissioned Forrester Consulting to evaluate enterprise SecOps maturity and better understand the challenges and benefits of increasing SecOps maturity.



US respondents

100% in IT, security, and operations roles



Respondent role

- › 74% Director level or higher
- › 47% Primary decision maker for security operations
- › 53% Provide significant input to final decision maker



Industry

- › 19% IT
- › 19% Manufacturing/materials
- › 17% Financial services/insurance
- › 8% Healthcare



Company size

- › 49% 1,000 to 4,999 employees
- › 25% 5,000 to 19,999 employees
- › 26% 20,000 or more employees

Overcoming SecOps Hurdles Decreases Risk While Increasing DevOps Efficiency

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

1 2

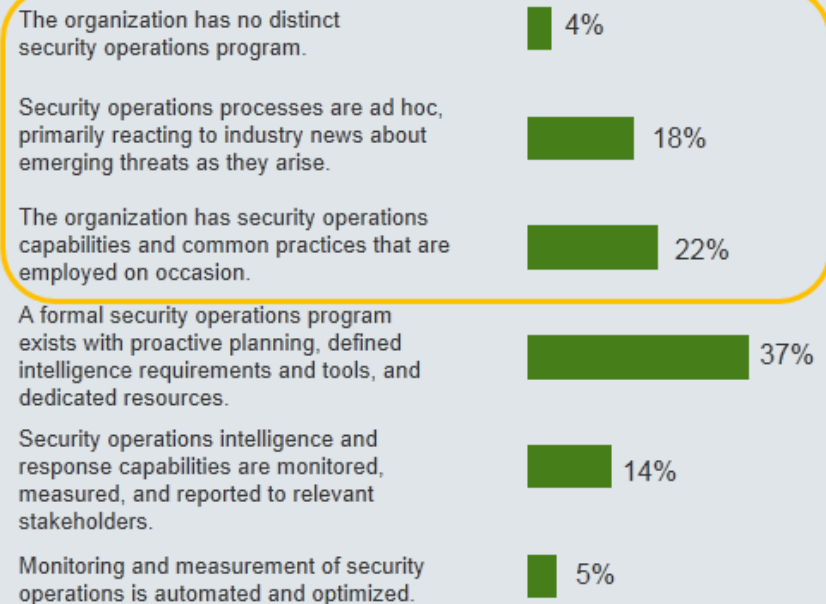
Forty-Four Percent Of Enterprises Have No Formalized SecOps

Security and IT operations managers report that enterprise organizations have different levels of SecOps maturity.

- › 44% have either no SecOps program, ad hoc processes, or practices deployed only occasionally.
- › Only 5% report that monitoring and measurement of SecOps is automated and optimized.

Now is the time to act. It's time to formalize a program, and if you have a formal SecOps plan, now is the time to optimize.

“How would you characterize your organization’s maturity level in regards to security operations?”



Base: 100 security and IT operations managers in US enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, August 2017

Overcoming SecOps Hurdles Decreases Risk While Increasing DevOps Efficiency

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

1 2

Improving Threat Intelligence And Compliance Critical Security Priorities

Enterprises are prioritizing IT security initiatives in the coming year in order to eliminate risks associated with applications.

- › 71% report that improving advanced threat intelligence capabilities is a critical or high priority.
- › 70% are complying with security requirements mandated by business partners, while 68% are working toward regulatory compliance.

With 77% of enterprises using cloud services, threats become more important.

“Which of the following initiatives are likely to be your firm's/organization's top information/IT security priorities over the next 12 months?”



Base: 100 security and IT operations managers in US enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, August 2017

Overcoming SecOps Hurdles Decreases Risk While Increasing DevOps Efficiency

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

1 2

Improving SecOps Is Challenging

As enterprises work to improve their security operations, they will likely face challenges including:

- › Staffing challenges such as understaffed teams and difficulties finding staff with the right skills.
- › Compliance challenges around regulations and potential violations moving from development into production.
- › Time challenges as day-to-day activities take up available resource time.

In addition to these challenges, half (48%) of enterprises find coordination between security and IT operations challenging.

“How challenging are each of the following as your organization works to improve your security operations?”



Base: 100 security and IT operations managers in US enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, August 2017

Overcoming SecOps Hurdles Decreases Risk While Increasing DevOps Efficiency

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

1 2

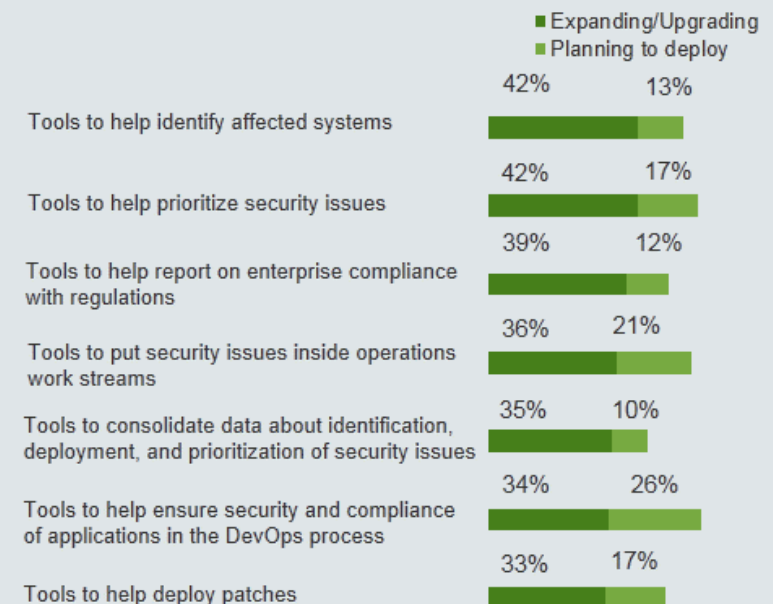
To Overcome These Hurdles, Enterprises Deploy Tools To Improve SecOps

Security and IT operations managers are deploying or planning to deploy tools to help identify and prioritize vulnerabilities and manage compliance.

- › 42% of enterprises are expanding or upgrading tools to help identify affected systems, and an additional 13% plan to in the next 12 months.
- › 42% are expanding or upgrading prioritization tools, while an additional 17% plan to implement in the next year.
- › 39% are expanding or upgrading tools to help report on enterprise compliance with regulations.
- › 39% are expanding or upgrading tools to help report on enterprise compliance with regulations.

To achieve better identification and remediation of vulnerabilities, 60% of security and IT operations managers report they are upgrading, expanding, or planning to deploy tools to help ensure security and compliance of apps in the DevOps process.

“What solutions are you deploying/planning to deploy for SecOps?”



Base: 100 security and IT operations managers in US enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, August 2017

Overcoming SecOps Hurdles Decreases Risk While Increasing DevOps Efficiency

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

1 2 3

Visibility Into Unpatched Systems Is A Barrier To Advancing SecOps

As enterprises work toward improving their SecOps maturity, they face three key barriers:

- › More than a third report a lack of visibility into unpatched systems and the volume of systems that still need to be patched.
- › In addition, security issues are not consistently placed in the operations work stream.
- › 28% of IT security and operations professionals are unable to fit required changes into maintenance windows.

39% of organizations struggle to get visibility. Gaining visibility into risky, unpatched systems can help improve prioritization and planning for vulnerability remediation.

“What are the challenges with advancing SecOps maturity?”

Lack of visibility into unpatched systems and volume remaining to be patched

39%

Security issues are not placed in operations work stream

29%

Inability to fit required changes into maintenance windows

28%

Base: 100 security and IT operations managers in US enterprises

Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, August 2017

Overcoming SecOps Hurdles Decreases Risk While Increasing DevOps Efficiency

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

1 2 3

Improving SecOps Drives Business Benefits

The biggest business benefits for those enterprises improving SecOps include fewer security breaches and fewer security distractions, allowing staff to focus time and energy on other initiatives.

- › More than two-thirds of security and IT operations managers see fewer security breaches and distractions.
- › 49% see a decrease in the cost of patching, while 47% see a decrease in the cost of compliance.

DevOps is a key application release accelerator for many companies. Nearly half (47%) of enterprises predict improved SecOps will drive efficiency between the development and operations teams.

“What do you see as the top business advantages for improving security operations?”



Base: Variable 100 IT security and operations managers in US enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, August 2017

Overcoming SecOps Hurdles Decreases Risk While Increasing DevOps Efficiency

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

1 2 3

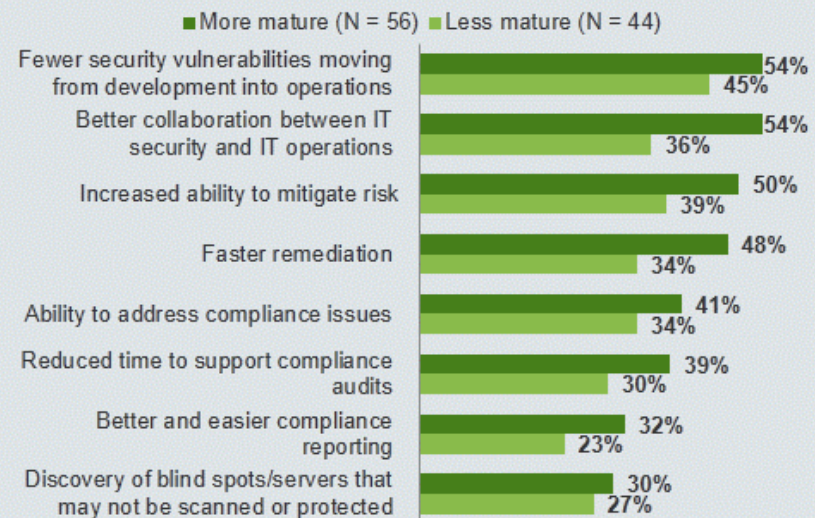
SecOps Maturity Drives Collaboration Between Security And IT Operations

Enterprises that have more mature SecOps — having a formal security operations program including proactive planning, monitoring, response capabilities, and some degree of automation and optimization — are more likely to receive benefits.

- 54% of enterprises with mature SecOps have better collaboration between security and IT operation teams.
- 54% experience fewer security vulnerabilities, compared with 45% of less mature organizations.
- 50% of those with more mature SecOps have an increased ability to mitigate risk, and 48% experience faster remediation.

Improving SecOps maturity clearly enables an increase in your security posture.

“What benefits have you achieved, or do you expect to achieve, by improving your security operations?”



Base: 100 security and IT operations managers in US enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of BMC, August 2017

A Custom Technology Adoption Profile Commissioned By BMC Software | October 2017

Overcoming SecOps Hurdles Decreases Risk While Increasing DevOps Efficiency

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

Conclusions

As security and IT operation professionals work to stay ahead of emerging threats due to unpatched systems:

- › The majority of organizations do not have the staff, ability to prioritize, or ability to effectively comply with regulations.
- › Security and operations professionals are planning to deploy a myriad of tools to gain visibility of vulnerabilities and effectively remediate them.
- › Improving security operations maturity brings benefits such as fewer security breaches, fewer security vulnerabilities moving from deployment into production, and increased communication between security and operations professionals.

METHODOLOGY

This Technology Adoption Profile was commissioned by BMC Software. To create this profile, Forrester Consulting completed a custom survey of 100 IT security and operations decision makers working within enterprises with more than 1,000 employees in August 2017.

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

© 2017, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to forrester.com. [1-1426DC8]



Project Director

Lisa Smith
Principal Consultant, Market Impact