FORRESTER®

Cybersecurity Requires Controls Monitoring To Ensure Complete Asset Protection

Automated Continuous Controls Monitoring Mitigates Cybersecurity Risk

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY PANASEER | JULY 2019

Cybersecurity Requires Controls Monitoring To Ensure Complete Asset Protection

Security leaders employ a variety of tools and technologies to identify risks and test the effectiveness of their security controls. As a result, security teams are left with point-in-time assessments that require them to cobble together data from disparate systems to truly understand the organization's security posture. This approach is reactive, labor-intensive, and insufficient in scale.

In May 2019, Panaseer commissioned Forrester Consulting to evaluate the benefits of automated continuous controls monitoring, a category of solution that provides real-time visibility of assets (e.g., devices, applications, people, data), security controls, and the effectiveness of those controls. Our research found that currently employed technologies don't provide a complete, real-time view of cybersecurity risk.

Key Findings

The abundance of technology investments gives firms a false sense of confidence in their security posture. Their challenges reveal a different story.

Point-in-time visibility of existing tools is limiting. Virtually all survey respondents report challenges with existing tools, including manual reporting, an incomplete view of asset inventory and controls, and insufficient visibility that comes with point-in-time solutions.

Interest is high in gaining real-time visibility of assets and security controls. Virtually all (95%) firms are extremely interested or interested in such a solution.

Overview
Situation
Challenges
Opportunity
Conclusion

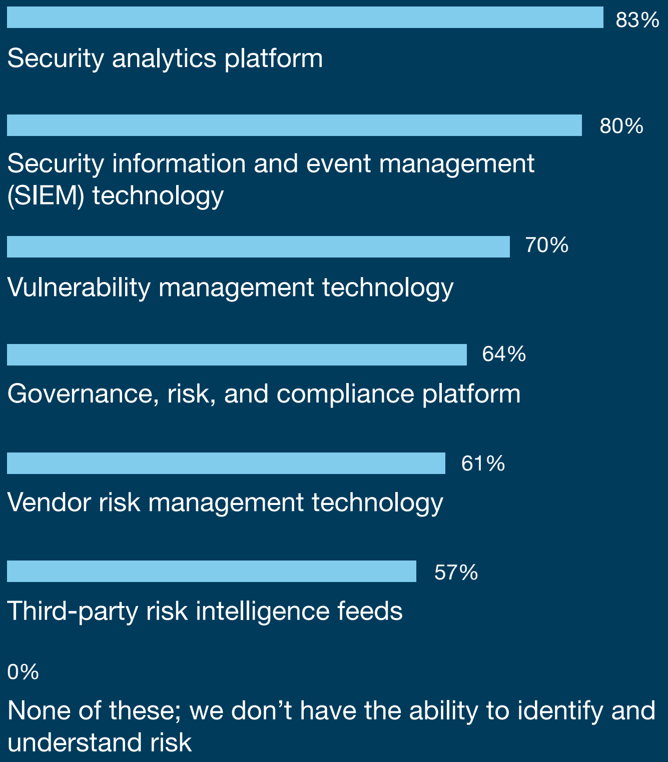
Cybersecurity Remains A Priority And Challenge For Security Leaders

You've heard it before: Cybersecurity risks are mounting as threats become more advanced and attackers savvier. With tensions high, 64% of companies are making it a high or critical priority to implement a risk framework aligning cybersecurity risk and enterprise risk.[1]

Our study found that all companies are prioritizing security and risk programs and investing in security and risk automation. In fact, most companies are using multiple technologies to identify and mitigate enterprise risk, including security analytics; vulnerability management; governance, risk, and compliance (GRC); and vendor risk management platforms.

Increasing the number of security technologies doesn't translate to improved security, however.

"Which of the following technologies, if any, does your company use to identify and understand enterprise risk?"



Base: 254 C-level or VP security decision makers at global enterprises in finance, healthcare, and retail verticals
Source: A commissioned study conducted by Forrester Consulting on behalf of Panaseer, June 2019

Overview
Situation
Challenges
Opportunity
Conclusion

Companies Report Confidence In Security Management Efforts; Their Challenges Suggest Otherwise

Investment in these numerous, disparate technologies has led most companies to be confident in their ability to manage and avoid risk:

- 86% are confident or very confident they have no gaps in their security controls deployed across devices, applications, people, and data.
- 78% say they take a centralized approach for risk management across their organizations. If true, this means they have a common risk taxonomy across the organization, manage technologies centrally, and aggregate and share risk data across business units.

Although most respondents in our study claim to have a common risk taxonomy and share risk data across their organizations, the menagerie of disjointed technologies makes it difficult to aggregate risk data for reporting, often requiring manual effort. This, in turn, hinders them from having insight into their overall risk posture.

As we dive into challenges that companies face with cybersecurity, we learn that their sense of confidence could be misguided. In fact, challenges companies are experiencing indicate a gap in perception versus reality.

Traditional Security Tools Are Insufficient For Proactive Cybersecurity

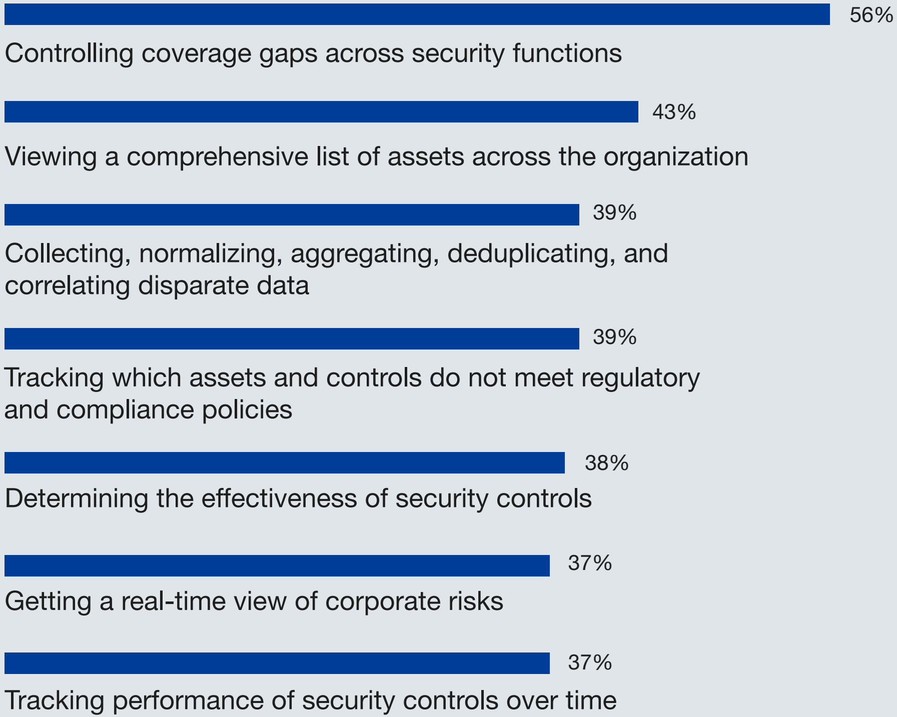
The complexity of today's IT infrastructures and the heterogeneity of enterprise security tools make it difficult for security pros to protect their environments. In fact, 97% experience challenges with their tools because they take a traditional reactive approach to fighting cybersecurity threats featuring:

- **An incomplete view of inventory and controls.** The biggest challenges companies face with their tools are controlling coverage gaps across security functions (i.e., inventory management, vulnerability management, endpoint security, privileged access, identity and access control, patching, application security, and user awareness) and viewing a comprehensive list of assets across the organization (i.e., devices, applications, databases, people, privileges, and vulnerabilities).
- **Point-in-time insight.** Continuous insight is crucial for security teams to prevent and mitigate risk as it happens. Despite its importance, only about a third have real-time insight on understanding whether their security controls are performing within policy. Around half lack real-time insight for their devices, applications, and the security controls they have deployed.
- **Manual reporting across multiple technologies.** With all the disparate security technology companies deploy, they rely on manual efforts to aggregate data for reporting. Over half of companies in our study spend days, weeks, or months on reporting on a quarterly basis. The amount of time security teams spend on this easily automated task could be spent on more strategic security initiatives.

These challenges impede companies from effectively controlling cybersecurity and result in repercussions.

Overview
Situation
Challenges
Opportunity
Conclusion

“What challenges is your company experiencing with the security tools you have in place today?”



Top 3 biggest repercussions

Increased risk of breaches

Difficulty understanding enterprise risk

High level of manual effort required to aggregate data and produce reports

Base: 254 C-level or VP security decision makers at global enterprises in finance, healthcare, and retail verticals
Source: A commissioned study conducted by Forrester Consulting on behalf of Panaseer, June 2019

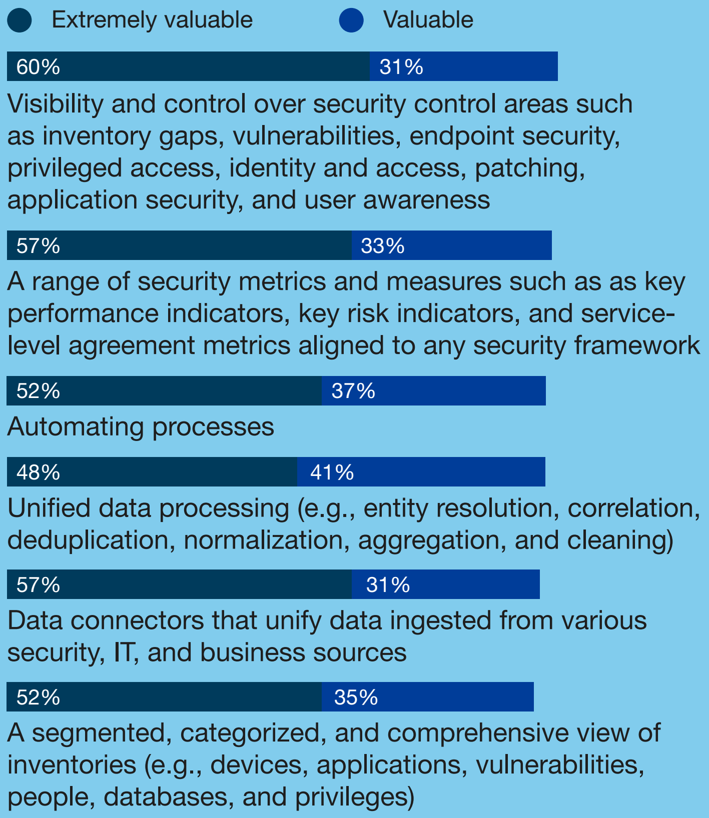
Overview
Situation
Challenges
Opportunity
Conclusion

CCM Tools Provide Comprehensive, Real-Time Visibility Into Cybersecurity Posture

A proactive cybersecurity program requires real-time visibility of IT assets and continuous monitoring of security controls to help identify, prioritize, and remediate risks. Solutions that provide the visibility and efficiency, like continuous controls monitoring (CCM), already exist.

It's no surprise that 95% of security decision makers in our study are interested in a solution that provides real-time visibility of assets (e.g., devices, applications, people, data), security controls, and effectiveness of those controls. While all recognize the need to automate, they also realize it's crucial to do so with the right tools. Respondents tell us they value numerous capabilities in a cybersecurity solution, including visibility into security control areas, automated processes, unified data processing, and a comprehensive view of inventories.

"How valuable are the following capabilities in a cybersecurity solution?"



Base: 254 C-level or VP security decision makers at global enterprises in finance, healthcare, and retail verticals
Source: A commissioned study conducted by Forrester Consulting on behalf of Panaseer, June 2019

Overview
Situation
Challenges
Opportunity
Conclusion

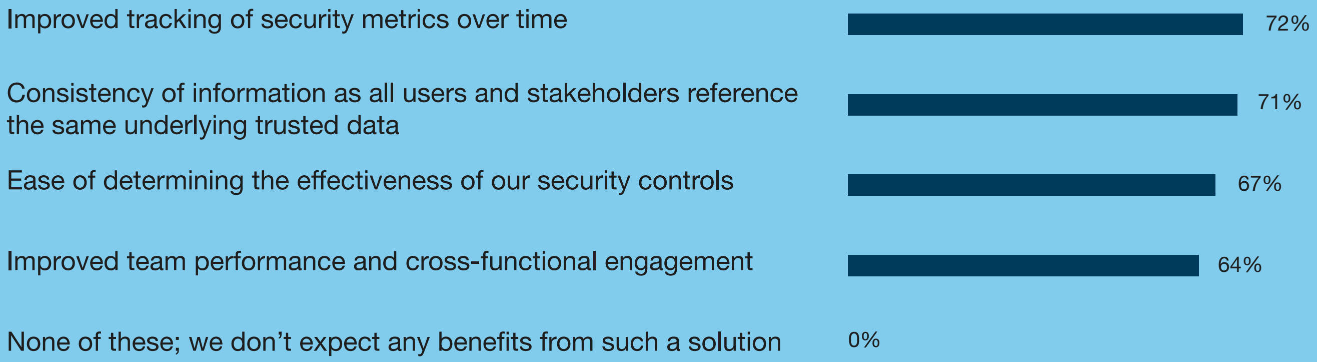
Investment Into CCM Tools Pays Off

If companies had a cybersecurity solution like CCM, 91% say having all those capabilities would have significant or substantial positive impact on their ability to proactively identify, prioritize, and remediate risk.

And 100% expect benefits from proactive and continuous risk identification, prioritization, and remediation, primarily with improved tracking of security metrics and consistency of information for all users. As one risk and cybersecurity senior advisor at one of the largest banking enterprises in the world put it:

“Continuous controls monitoring is the next evolution in security controls assessment. It means getting on top of issues before a controls incident becomes a security incident.”

“What benefits do you anticipate from proactive and continuous risk identification, prioritization, and remediation?”



Base: 254 C-level or VP security decision makers at global enterprises in finance, healthcare, and retail verticals
Source: A commissioned study conducted by Forrester Consulting on behalf of Panaseer, June 2019

Overview
Situation
Challenges
Opportunity
Conclusion

Conclusion

Cybersecurity has never been more critical to a company's business success than it is today. The rate of cybersecurity incidents is compounding, attackers are getting savvier, and each new breach draws headlines threatening company reputation.

Rightfully, companies are prioritizing their security and risk initiatives and investing in multiple technologies. Unfortunately, technology investments have provided a false sense of confidence in their security posture. Security leaders must understand that a proactive approach to cybersecurity requires:

- The right tools, not more tools.
- Real-time visibility of security posture.
- Automated reporting and dashboards across the enterprise.

Project Director:
Andia Tonner, Senior
Market Impact Consultant

Contributing Research:
Forrester's Security &
Risk research group

Methodology

This Opportunity Snapshot was commissioned by Panaseer. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of security decision makers at global enterprises. The custom survey began in May 2019 and was completed in June 2019.

ENDNOTES

[1] Source: Forrester Analytics Global Business Technographics® Security Survey, 2018

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.

Demographics

GEOGRAPHY

US: 53%

UK: 21%

Germany: 14%

France: 12%

INDUSTRY

Financial services: 47%

Retail: 37%

Healthcare: 16%

LEVEL & DEPARTMENT

C-level executive: 78%

Vice president: 22%

IT: 84%

Security/risk: 16%

SECURITY STRATEGY RESPONSIBILITY

Final decision maker: 91%

Part of team making decisions: 9%

FORRESTER®