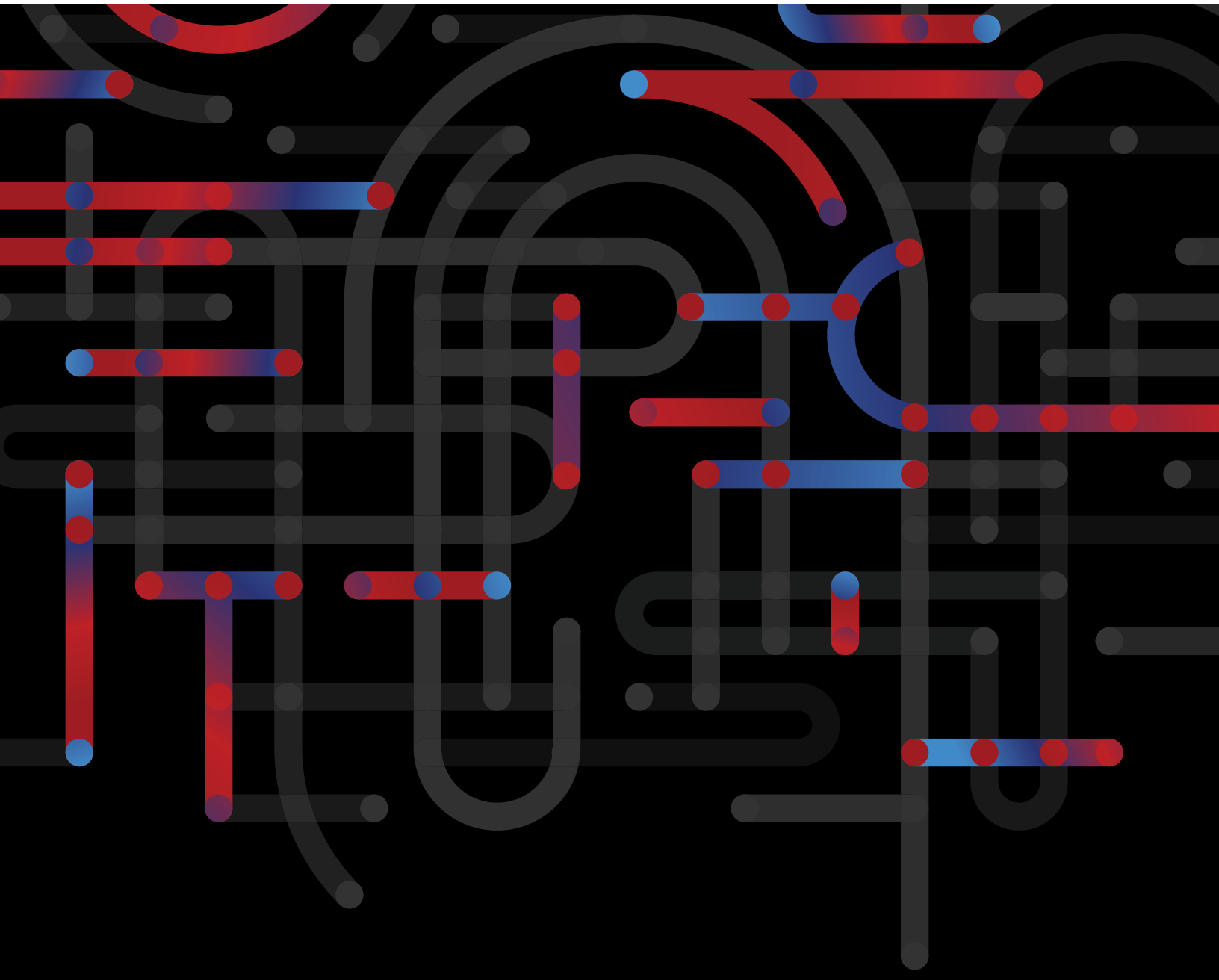
panaseer

DARKREADING



Control failures:
The Cybersecurity Industry's Dirty Little Secret?

There's a dirty little secret in cybersecurity these days: despite rising security budgets and many state-of-the-art solutions, most breaches are achieved by relatively unsophisticated hacks. Even after faithfully following vendor advice, security teams on the front lines keep getting blindsided because the security industry continues to sell tools that work in silos, which creates gaps and leads to those tools failing.

> **"9 out of 10 security leaders state that failure of an expected control is the primary reason for breaches."**

The Panaseer 2023 Security Leaders Peer Report[1] revealed that 79% of enterprises were victims of cyber incidents that could have been prevented with existing controls. Surveys reveal[2] that 62% of organizations are not confident in their security posture, and 58% are aware of fewer than 75% of the assets on their network. Ninety percent of security leaders state that failure of an expected control is the primary reason for breaches.

The result? Deficiencies, business risk, resource drain, and regulatory consequences. In short, millions are being spent, but security remains broken. And security teams feel the pain. The proper controls are allegedly in place, but breaches continue even at the most well-equipped enterprises staffed by the best security talent. Our conclusion? Control failure is the mother of all failures—and it requires immediate attention.

1. https://panaseer.com/reports-papers/report/2023-security-leaders-peer-report/
2. https://securityboulevard.com/2022/02/report-62-organizations-are-not-confident-in-their-security-posture/

The Frustration of IT & Security Teams

Businesses are bombarded by intrusion attempts every day. In response, companies have acquired an extensive array of sophisticated security tools. But incidents continue to surface due to inadequate tool deployment.

Security leaders realize that current tools provide a false sense of confidence. Due to control failures organizations don't know where they have weaknesses in their security posture, which makes it impossible to prioritize tasks accurately. And security teams get frustrated because they lack insight into what assets need to be protected and when.

> **"An endpoint protection system only protects endpoints where it is deployed - it can't and won't protect where you haven't deployed it."**

The causes of control failures can be broken down into:

Configuration Management Database (CMDB) limitations: This includes incomplete or poor quality data, lack of automation, and CMDB integration difficulty. Also, a CMDB can become overly complex, making it difficult to navigate and use effectively.

Asset ambiguity: Shadow IT (unauthorized software, apps, cloud services, and unmanaged IoT) leads to ambiguity. Obsolete assets, legacy systems, and third-party add-ons can create confusion. Finally, inconsistent access control policies can generate further uncertainty, which increases the risk of asset breach.

Tool deployment gaps: Misconfiguration, incomplete deployment, lack of integration, and alert fatigue can lead to the underutilization of controls. Conversely, too many security tools without proper coordination can lead to inefficiency and confusion among security personnel.

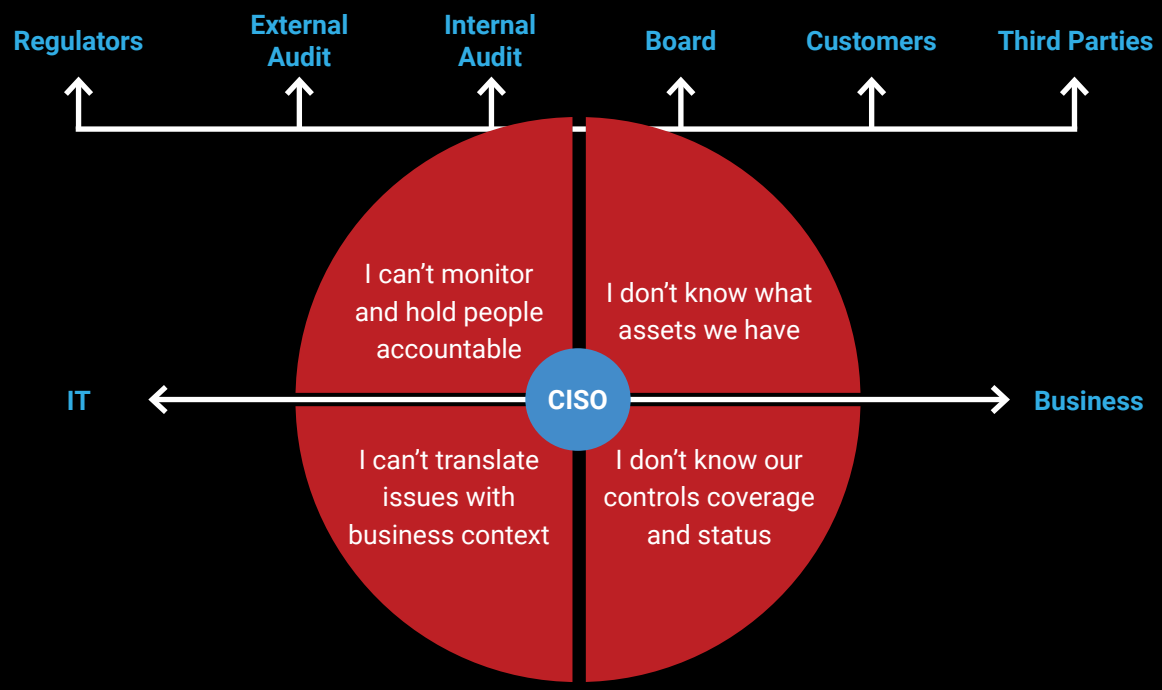
Silos & competing interests: IT may prioritize system uptime and performance at the expense of security measures. Procurement may prioritize cost savings and convenience over thorough security evaluations. Meanwhile, poor coordination and competition between SecOps and Incident Response can delay mitigating threats.

Poor reporting: If reporting isn't scalable, reliable, and actionable, it's useless. Heavy reliance on manual processes, frequent false positives and negatives, and lack of context and prioritization leave the SOC in the dark about security gaps.

Real-world control failure impact

From the boardroom to the security team floor, there is a perception gap between the money invested in security tooling and the subsequent efficacy of the solutions in place. Corporate IT resources are limited, so maximizing what you already have provides the highest degree of protection.

Security controls fail because CISOs don't have access to high quality control measurement & fail to influence



> **Companies used to get breached because they lacked security controls. Now they get breached because of control gaps and failures.**

Control failures have led to serious incidents worldwide. The victims aren't necessarily irresponsible, and the tools they deploy are frequently best-of-breed. The problem remains in tool orchestration. And security breach headlines are more common than ever.

T-Mobile Says Hack Exposed Personal Data of 40 Million People

Control failure: Unprotected network access device

Hackers Release L.A. School District Data Over Failure To Pay Ransom

Control failure: Unpatched critical vulnerabilities on staff equipment

Cyberattack Forces a Shutdown of a Top U.S. Pipeline

Control failure: Password policy not met

Chinese hackers breached US government emails via Microsoft Cloud exploit

Control failure: Unpatched critical vulnerability on critical system

Inside the Big Facebook Leak of 553 million people across 106 countries

Control failure: Unpatched critical vulnerability on critical system

Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit

Control failure: Unpatched critical vulnerability on critical system

A single source of trusted, validated data

The confusion and frustration facing security professionals translates into real-world damage. Companies, clients, communities, and even national security are at risk. Therefore, it's crucial to understand what lies at the heart of the issue: a data science and measurement problem.

A single source of data isn't enough, since security tools often give an incomplete and inaccurate view. Instead, security teams need to combine data from across different tools, and use automation to continuously clean, correlate and validate it. This means you can make huge improvements to the quality and completeness of your data.

> **"A solution must emerge through the integration of readings from diverse security tools, a function carried out by Continuous Controls Monitoring."**

What would such a solution look like? The characteristics of this single source of trusted, validated data should include:

Automation: By taking over data collation, presentation, and reporting tasks, automation removes most errors generated by manual tooling. The result is more integrity, minimized error, and higher efficiency across the security spectrum. And with security teams spending 45% of their time on this task, automation reduces the risk of burnout and allows them to spend their valuable time on something more important.

Actionable metrics: A definitive framework of best practice security metrics and measurements should be provided. This means clear metric identification and automated data collation with continuous measurements and insight. Reporting should occur within an easy-to-grasp business context instead of a confusing mass of unorganized and unprioritized data. Metrics such as "Systems with Ineffective Malware Protection" should be viewed in real-time with trending visualizations.

Continuous: This provides a near real-time view through automated and continuous ingestion of data that includes details on individual assets. Metrics on all assets should be viewable in granular detail within a business context to show the effectiveness of controls across the estate, with the additional benefit of historical data. This allows you to view trends and track change over time.

Proactive: The right solution must focus on identifying indicators of exposure not indicators of compromise. This comes well before the SecOps responsibility of threat detection and response. And it makes incident recovery a rarity.

Continuous Controls Monitoring fills the data gaps

The answer to the security industry's dirty little secret lies in Continuous Controls Monitoring (CCM). CCM platforms ingest data from security, IT, and business tools, including HR platforms and proprietary systems, whether on-premises or in the cloud.

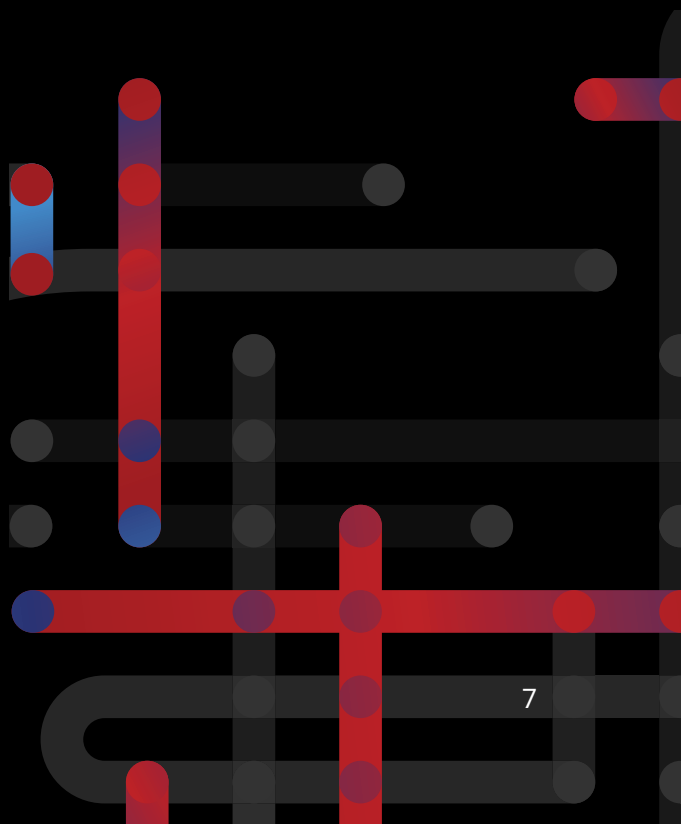
The analytics engine then normalizes, augments, and correlates this data, giving you:

- Continuous, accurate visibility of assets and controls status.
- Actionable insights on where to prioritize resources.
- Automated reporting that translates security posture into business risk.
- Improved decision making and cyber hygiene, reducing cyber and business risk.

> **"Comprehending the precise location of your controls, their operations, and implementing measurements over multiple security domains can prevent most cyber incidents from occurring. This drastically diminishes the need for detection, response and incident recovery."**

Continuous Controls Monitoring also enables the optimization of controls over critical security domains:

- **Vulnerability analysis**
- **Endpoint analysis**
- **Patch analysis**
- **Identity and access management**
- **Privileged access management**
- **Security awareness analysis**
- **Application security analysis**
- **Cloud security**



The Four Pillars of CCM

1 Cyber Asset Management
Data is normalized and verified in real-time. Reporting is context-rich, such as in assigning business criticality and ownership details.

2 Security Controls Management
Coverage and effectiveness of security controls are measured using best practice metrics, all aligned to security frameworks across the most critical security domains, as opposed to relying on a single choke point that may fail and expose the entire network.

3 Efficient reporting and risk prioritization
CCM identifies critical risks requiring immediate action, enabling integrated risk triage from multiple security domains.

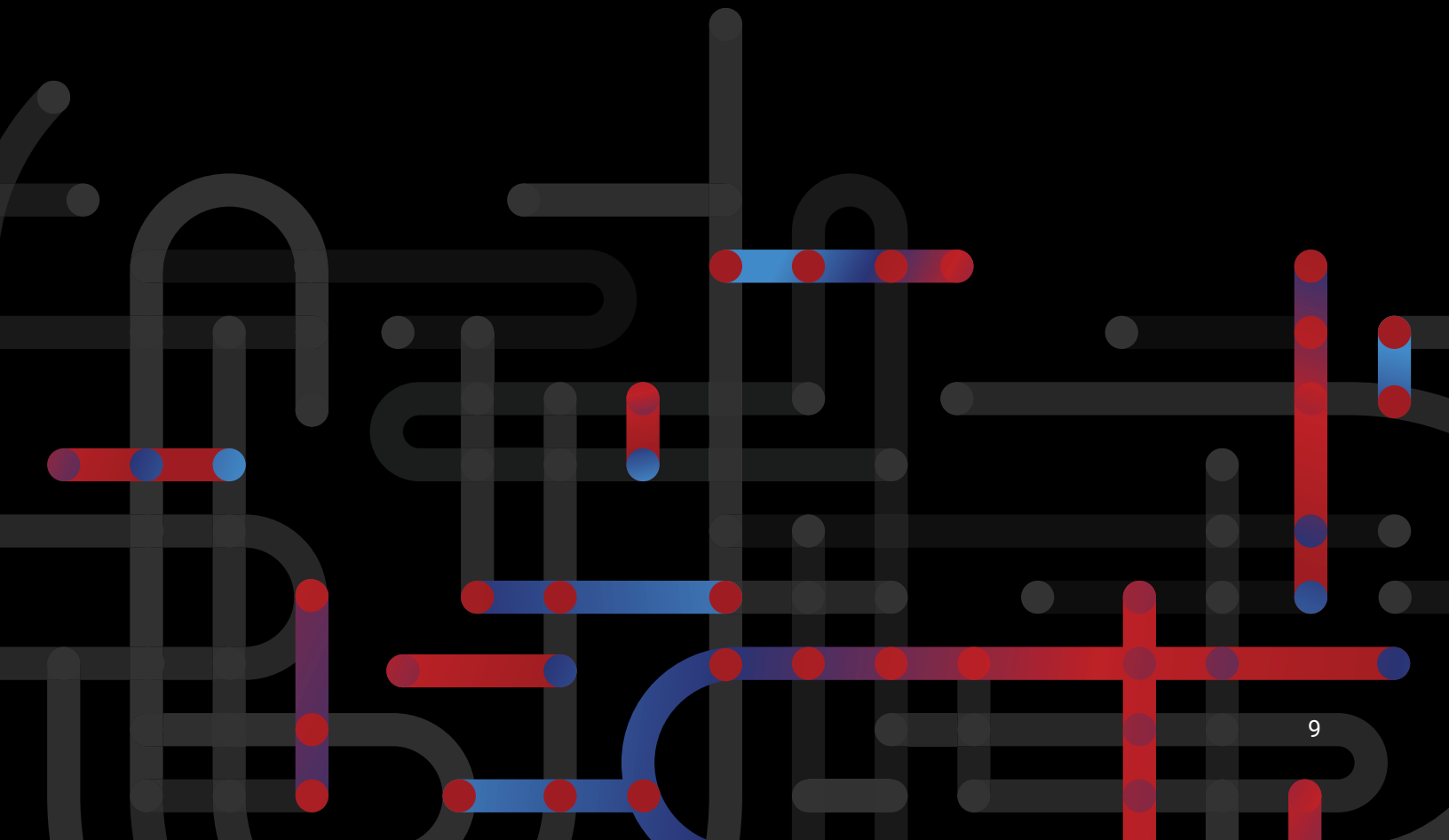
4 Evidenced remediation
Data from your existing security tools is used to confirm when issues have been fixed, allowing you to track remediation against your own policies and SLAs to improve accountability.

Continuous Controls Monitoring fixes upstream tool deficiencies intruders use to gain access

Among some cybersecurity sectors, there's a pernicious trend attempting to diminish breach prevention efforts and focus more on threat response and incident recovery. It seems like a new, premium tool is always needed, but the breaches keep coming. Some take it for granted that hackers will always have the upper hand in gaining access to your systems and networks.

This security approach, however, leads to the dramatically rising cost and impact of cyber breaches worldwide. And with more attacks targeting critical infrastructure, a "catch-them-on-the-inside" emphasis is fraught with danger.

While post-breach efforts are indispensable, this defeatist attitude gained popularity partially due to a lack of solutions that adequately measure and monitor controls and tools. It's time to regain confidence in your cybersecurity. Continuous Controls Monitoring makes it possible to measure and continuously monitor where tools are deployed and remediate gaps as a priority, ensuring your security team isn't blindsided by preventable attacks.



panaseer

Panaseer is an enterprise cybersecurity automation and data analytics company that helps organizations adopt proactive security posture management by ensuring security controls are fully deployed and working effectively – maximizing their security investments and resources through better prioritization. It gives CISOs a continuous measure of their security posture, enabling them to provide trusted updates to senior leaders, board members and regulators.

Panaseer's Continuous Controls Monitoring platform gives a complete, trusted view of security controls, with metrics and measures guidance aligned to best practice frameworks. With $262 billion spent on cybersecurity tools in 2021, CCM means organizations can do more for less by getting the most out of their existing security investments.

Learn More

Content produced by Dark Reading