IDG
SPONSORED CONTENT

The Future of Security Is Connected

Digital transformation (DX) is accelerating in organizations across virtually all markets and industries. IDC predicts that global spending on digital transformation will reach $6.8 trillion globally by 2023.

As part of their DX efforts, companies are moving more applications to the cloud, refactoring existing applications, and integrating more data sources across the organization. Many are embracing a hybrid cloud infrastructure that spans private and public environments.

However, while DX is delivering many benefits, security is all too often left playing catchup. Traditional cybersecurity models cannot keep up with this rapid pace of change and evolution. That's why security transformation needs to be a foundational component of any DX initiative.

This white paper examines the security challenges businesses face in their quest for DX and uncovers the right strategy and tools for cybersecurity moving forward in a new digitized data-sharing environment.

A WHITE PAPER SPONSORED BY IBM | aws

The Challenges Facing Security Teams Today

As companies pursue DX initiatives, many are refactoring applications to become more modular and containerized. They are also migrating core apps such as email, collaboration, and workforce management to software-as-a-service (SaaS) environments in the public cloud. They're increasingly treating data as a shared resource between departments, partners, and communities and using AI and analytics to find new, previously unexplored value in their data. This broad mix of apps and data tends to be spread across hybrid cloud environments.

Traditional cybersecurity tools weren't built to handle the increased levels of complexity of this hybrid infrastructure. A dizzying number of vendors, security tools, and daily security alerts—combined with an ongoing security skills shortage—can be overwhelming to security teams.

Security leaders need to transform their strategy and tools to reduce vulnerabilities and risk—while still giving the business enough flexibility to innovate. Specifically, security leaders need a modern approach in two key areas:

1. Threat management

In security operations centers (SOCs), analysts are confronted with a steady stream of new and existing threats, multiple tools to manage, and data silos across on-premises and cloud environments.

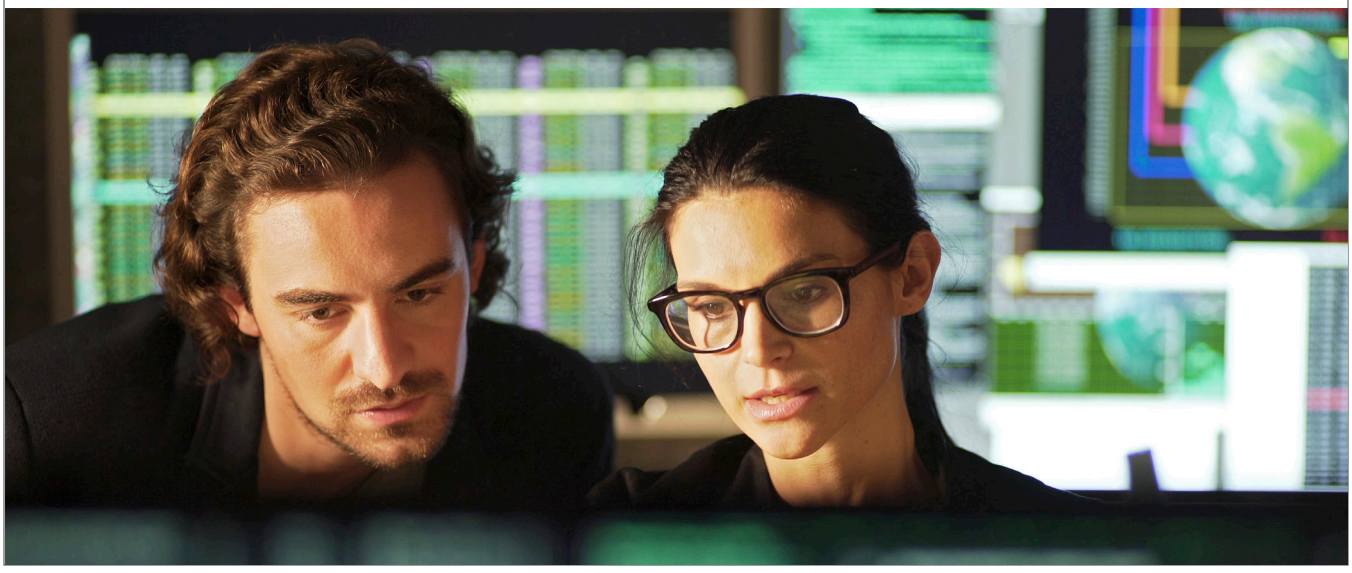
Recent ESG research found that 60% of companies use 25 or more unique security products and 44% do business with more than 10 vendors. A global cybersecurity skills shortage further inhibits analysts from effectively detecting, investigating, and responding to threats, because they're spending too much time manually correlating results or integrating tools.

A modern SOC can improve threat management capabilities by:

- **Integrating events and alerts to provide a single view across the enterprise, with intelligence to help prioritize the greatest threats**
- **Quickly navigating incident detection and response across multiple tools and data sources**
- **Using automation capabilities to reduce manual processes to keep teams focused on mission-critical objectives**

The goal is to identify and mitigate threats faster. A modern SOC offers deep threat insights, including indicators of compromise, incident type, and severity. Intelligence and automation capabilities combine to automatically assign the appropriate teams and stakeholders to a case, based on incident types so that it can be addressed sooner, with due dates so teams can manage expectations for remediation.

The modern SOC must also include a thorough visual experience, with dashboards that contain clear KPIs and metrics and that offer incident details so analysts can uncover threat campaigns early as well as identify patterns for use in future strategy.



2. Data security management

Organizations are producing a staggering amount of data. Data sprawl has become a major area of focus for teams overseeing data security, privacy, and other compliance requirements. In a recent IDC survey, more than 37% of the participating organizations said the growing complexity of security solutions is a significant challenge that often impedes data governance and policy enforcement.

Specific data management challenges involve the following:

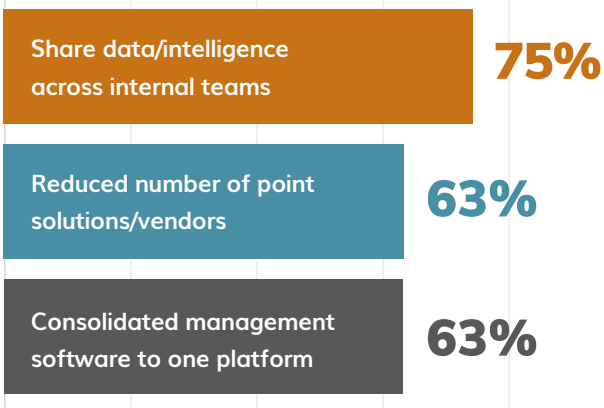
- **Identifying where data is being stored and how it is being accessed**
- **Uncovering deviations in data access and control policies that suggest potential risks**
- **Proactively mitigating issues to avoid potential breaches**

Managing security in this level of complexity is confusing at best. Siloed setups force security teams to navigate data risk without a clear end-to-end picture. It's critical to have full visibility to manage data in a holistic, centralized way that maintains compliance posture, both on-premises and in cloud-hosted environments.

A modern data security strategy must not only provide full data protection but also include audit capabilities, real-time controls, and automated workflows that span many different data environments. The strategy also must be flexible enough to account for the ever-increasing number of hybrid, multicloud environments.

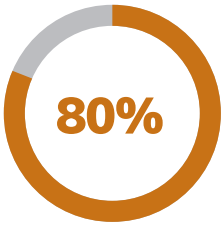
A Unified Approach to Security Is Essential

Simplifying the ecosystem is a demonstrated best practice for enhancing security. In fact, research from Forrester found that security champions—those most effective at simplifying their ecosystem—have the following strategies for streamlining their security management:

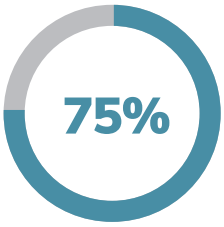


And clearly this consolidation/simplification is paying off. Forrester found that 80% of the organizations it surveyed are satisfied with their threat detection efforts and 75% are satisfied with their level of threat response.

Modern security requires a unified approach. Adding more tools and solutions without end-to-end integration will only create more data silos across on-premises and multicloud environments. This piecemeal approach leads to gaps in visibility across threats and risks, increased cost to integrate tools and migrate data, and complexity that hinders efficiency and operations.



Satisfied with threat detection efforts



Satisfied with level of threat response

To implement a unified approach, teams need a common control plane where they can openly connect data and workflows. This platform should enable shared data, analytics, and common services that can break down the silos between teams and tools across several areas:

- Threat management
- Data security
- Identity and access management (IAM)

They also need an open ecosystem and modular capabilities that give organizations the flexibility to adapt as their needs change and to connect with third-party and homegrown tools.

A unified approach can offer better outcomes with major pain points.

These improved outcomes include:

Faster incident response and threat hunting

With a unified approach, SOC teams can streamline threat management across detection, investigation, and response, reducing wasted time and increasing the efficiency of analysts.

The benefits of an integrated approach and technology such as real-time detection, automation, federated search, and orchestration ultimately help a team cut through the noise and respond more quickly to threats.

Full visibility of data security

With a unified approach, security teams can understand their risk holistically and across disparate environments. A unified approach ensures that they can automatically discover and centrally visualize risk across on-premises and cloud-based data repositories and actively monitor and report on activities over long time periods for compliance. A unified approach also enables teams to find risk-based insights to analyze and actively apply data access controls and policies—or escalate issues as threats emerge.

The Solution to Modern Security Management

The future of security is connected. IBM Cloud Pak for Security provides a single highly automated and extensible security platform that operates across on-premises and Amazon Web Services (AWS) environments—helping simplify operations and enhance your security posture. IBM Cloud Pak for Security enables businesses to:

- Expand visibility and insights
- Accelerate security workflows
- Modernize architecture

With IBM and AWS, organizations can benefit from these capabilities:

Threat management

Prioritize the most-relevant threats by leveraging detailed, actionable threat intelligence derived from all data sources and environments. Specific capabilities include:

- **IBM Security Data Explorer**—enables analysts to perform federated investigations across IBM, AWS, and third-party data sources, including SIEM, EDR tools, data lakes, and more. This reduces investigation time by enabling them to query multiple data sources with the simple query builder and one workflow seen in IBM Cloud Pak for Security.
- **IBM Security SOAR**—empowers incident responders by automating common security operations and incident response (IR) processes, guiding them through the necessary steps to resolve complex cases. Teams can quickly access important security information, which promotes accurate decision-making and decisive action.
- **IBM Security Threat Intelligence Insights**—offers detailed, actionable threat intelligence that helps organizations identify and prioritize the threats most relevant to them, based on their organizational profile and environmental telemetry.

Data security

Establish proactive security measures by leveraging advanced analytics, advanced automation, and artificial intelligence to strengthen security posture across on-premises and AWS environments. Specific capabilities include:

- **IBM Security Guardium Insights**—built as a collaborative, comprehensive data security platform to help unify and modernize the SOC. The platform consolidates visibility across on-premises and cloud databases, retains data security and audit data for years, and leverages machine learning and analytics to surface key insights and anomalous behavior and uncover hidden threats.

IAM

Integration with AWS Identity and Access Management enables management access to AWS services and resources remotely. Using IAM, managers can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources.

By aligning with an AWS Security Competency Partner such as IBM, which augments AWS native security with end-to-end capabilities and services, organizations can more efficiently close the cloud security readiness gap and navigate their cloud journey with confidence.

Take the next step with IBM's Cloud Security Maturity Assessment for AWS to help identify gaps in your security posture.

You also can deploy IBM Cloud for Security with an **AWS Quick Start** to rapidly expand and streamline your security posture across on-premises and cloud environments. IBM Cloud Pak for Security comes with out-of-the-box, interconnected security applications for threat investigation, risk management, orchestration, and automation.

IBM | aws