Scrut Automation

3 Trends CISOs Can't Ignore

Scrut Automation

Introduction

The cybersecurity landscape is always shifting, and keeping an organization's data secure calls for a constant reevaluation of its security strategy.

Now, the tried-and-true methods of defending an organization's perimeter are falling short. It's become nearly impossible for companies to manage the challenges of ever-evolving compliance regulations, hybrid IT environments, and a distributed workforce. With global cybercrime costs mounting and expected to reach $10.5 trillion a year by 2025, organizations need modern cyberattack prevention and response plans to avoid governance issues.

Did You Know?

Global cyber-crime costs are expected to reach

$10.5 trillion

annually by 2025

In 2023 and beyond, **even the most vigilant SecOps team is at risk of a cyberattack** at any moment. As malicious actors continue to discover new ways to target and capture sensitive data, CISOs must stay on top of the latest cybercrime trends to maintain compliance and protect customers' personally identifiable information.

Securing your IT infrastructure starts with seeing the cybersecurity risks on the horizon. Look out for these three emerging cybercrime trends to ensure your organization is prepared for any attack.

Scrut Automation

Cybercrime as a Service (CCaaS) Gains Popularity

Over the last decade, organizations have invested billions into cybersecurity efforts, driving bad actors to devise increasingly sophisticated cyberattacks. In 2022 alone, companies worldwide spent over $240 billion on cybersecurity solutions, tools, and services to prevent and mitigate notable hacker groups from breaching their organization's perimeter. However, highly accomplished hackers are no longer the primary threat to these organizations.

Now, anyone can commission a targeted cyberattack from skilled hackers, turning cybercrime into a readily available commodity. Cybercrime as a service, or CCaaS, is the latest managed service to gain a foothold in the IT industry, allowing motivated bad actors to outsource a data breach to an experienced "cyber hitman."

The lower barrier to entry offered through CCaaS is compelling for less experienced hackers who want to profit from lucrative sensitive data breaches and claim ransom payments. While some malicious actors may hire a hacker group to conduct an attack and pay them a percentage of the profits, most buy phishing kits or rent pay-per-use malware to deploy themselves against vulnerable small businesses and startups. Multiple small breaches add up to significant profits over time, making them a low-risk, high-reward option for new cybercriminals.

Popular Tools for CCaaS

Hackers have discovered a new way to profit from their work through ransomware subscription services, prepackaged DIY phishing and ransomware kits, and full-service cybercrime platforms.

Most CCaaS is offered through rentable ransomware campaigns, where a buyer pays a one-time fee for single-use malware created by a sophisticated hacker group. These rentable campaigns provide all the information a malicious actor needs to deploy the attack and claim their ransom payment, without the large deposit often required for a hacker-for-hire.

Cybercrime groups like DarkSide can create platforms that allow lower-skill cybercriminals to subscribe and deploy multiple attacks. Using these platforms makes deployment even more foolproof while allowing hacker groups to claim a portion of the profit for every crime conducted through the platform. Many platform services even offer customer support, allowing nearly anyone to deploy a profitable attack.

Yet while ransomware is the most common attack provided as a service, it's far from the only option for budding cybercriminals.

Did You Know?

Rentable botnets allow customers to deploy DDoS attacks for as little as **$15 a week.**

Other criminals are cashing in with rentable trojans-as-a-service or dropper-as-a-service offerings, allowing them to easily distribute malware and collect sensitive data they can sell on dark web marketplaces for a profit.

How to Protect an Organization From CCaaS

Often, hacker groups will target a range of organizations and conduct multiple zero-day attacks once they discover a common software vulnerability. Now, those hacker groups are sharing vulnerabilities with their CCaaS buyers, causing a dramatic increase in successful zero-day attacks.

One of the best ways to protect an organization from CCaaS attacks is knowing the latest vulnerabilities discovered in the industry.

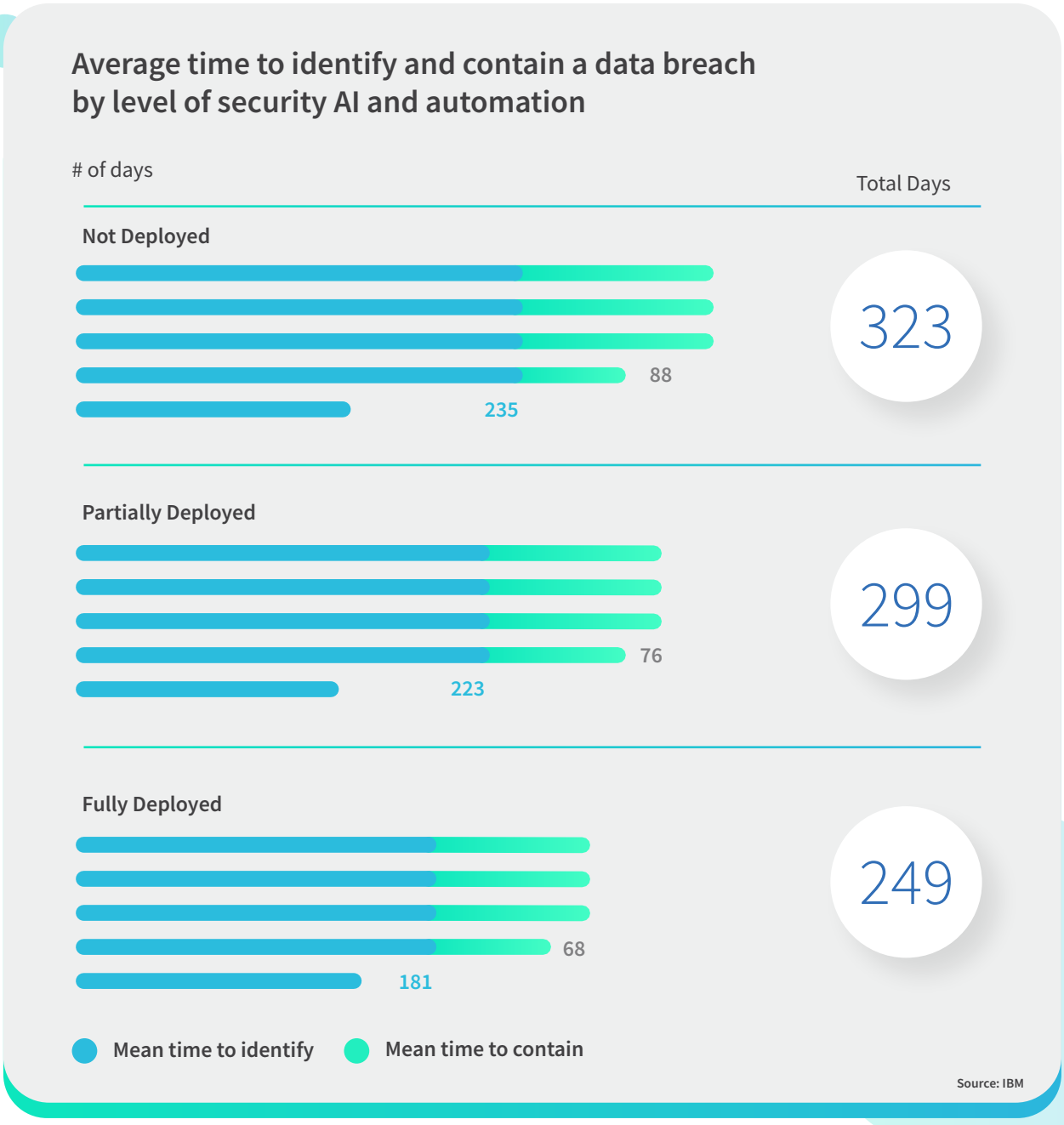
Quick Tip

Checking the MITRE ATT&CK database twice a year and updating your security strategy accordingly is critical to avoid CCaaS attacks.

However, since the database only contains publicly available threat data and incident reports, it's only as valuable as the information that companies share with law enforcement and the public. Better visibility into vulnerable security gaps reduces the likelihood of falling victim to a CCaaS attack, but increasing visibility is every company's responsibility.

Sharing threat information and exposing security vulnerabilities with other private and public organizations allows companies to know what cyberattackers are targeting and where companies need to focus their security efforts. It's equally important for companies to report suspicious activity and breaches to law enforcement to reduce the proliferation of cybercrime.

Introducing automation is another way to protect an organization against CCaaS, strengthen its security posture, and take a proactive approach to threat detection. Automation can streamline monitoring across a company's IT infrastructure, so any size security team can quickly identify irregular behavior, detect potential breaches, and respond to CCaaS attacks faster.



Scrut Automation

Supply Chain Attacks

No company in 2023 operates in a vacuum; since most modern organizations work with multiple vendors and suppliers, it's no surprise that supply chain cyberattacks are increasing dramatically. However, most companies don't know that software supply chain attacks have had a whopping 742% average yearly increase since 2019, with no sign of slowing down.

Supply chain attacks—or attacks that target a third party to gain access to their clients' or users' systems and sensitive data—resulted in 62% of all system intrusions in 2022. A single supply chain attack can have far-reaching effects and impact multiple organizations at once, making it a lucrative target for today's cybercriminals. Plus, identifying and containing a supply chain attack in 2022 took organizations 303 days on average, allowing cybercriminals ample access to an organization's network and sensitive data.

Since most companies maintain various vendor relationships and use myriad third-party applications, it's difficult to find the source of these system intrusions. Many of these attacks mimic trusted access patterns and data-sharing pathways vendors commonly used to distribute malware or gain access to sensitive data, making attacks even harder to trace. Other attacks leverage vendor relationships to create compelling phishing attacks and gain access to client credentials, which can put even more sensitive data at risk.

These types of data breaches can be particularly devastating for companies in finance and healthcare, which store huge volumes of valuable personally identifiable information (PII) like bank account information, health data, and social security numbers. Often, cyberattackers sell this data on the dark web, which exposes a company's customers to the risks of identity theft and fraud.

Examples of Notable Supply Chain Attacks

One example of a supply chain attack with a huge impact was December 2021's Log4j vulnerability. Hackers discovered a vulnerability within the popular open-source logging library that allowed them to trigger harmful code from external databases and servers. Malicious actors around the world deployed millions of cyberattacks every hour, impacting almost every company using Java applications.

Similarly, the notorious SolarWinds breach introduced malware into the IT environments of 18,000 organizations through a routine update to its SolarWinds Orion software. Even organizations known for their strong cybersecurity strategies—like Microsoft, Mandiant, and government agencies—fell victim to the attack. SolarWinds reports that the malicious actors who compromised their software may have accessed their network through a third-party vulnerability, too.

Sometimes, cyberattackers directly target vendors that collect multiple companies' sensitive data to provide services. An example is the Practicefirst breach, where malicious actors gained unauthorized access to health information for 1.2 million people by attacking a medical managed services provider. Since the companies that work with the vendor weren't directly breached, they had no way of knowing their customers' data was compromised until Practicefirst discovered the breach.

Notable breaches

solarwinds	About 18,000 customers installed updates that left them vulnerable to hackers.
Practicefirst	Health information of 1.2 million people was leaked, through its managed service providers.

How to Protect an Organization from a Supply Chain Attack

For the vast majority of organizations, the vendors they partner with are an essential component of their supply chain to deliver products and services. However, companies must go the extra mile to perform due diligence on the third parties they choose to work with.

A secure vendor risk management strategy and procedure is the first step organizations should take to prevent a supply chain attack.

Organizations should partner with their vendors and maintain a vested interest in the vendor's security posture to reduce the likelihood of a supply chain attack. Alongside downloading all of the vendor's latest security patches, organizations should also check and ensure that vendor software is secured against recently reported common vulnerabilities and exposures (CVEs).

Conducting regular vendor security assessments and checking their compliance reports is a great way for companies to confirm the software they use is secure. In some cases, these assessments may expose security gaps that the vendor isn't aware of. Mitigate the risk of an attack by partnering with vendors to reveal these security risks and encouraging vendors to prioritize addressing these risks.

Automation for Regulatory Compliance

Compliance regulations require companies to ensure all company data is accounted for and sufficiently protected. However, maintaining compliance and keeping track of exponentially increasing data volumes is nearly impossible to do manually. Now more than ever, companies need compliance automation to ensure ongoing compliance with national and international regulatory bodies.

Compliance automation is a series of tools and technologies that allow organizations to meet compliance requirements and streamline auditing by creating and distributing policies, automating security training deployment and tracking, and automated evidence collection and reporting. Some tools also offer monitoring capabilities to detect compliance risks to better support compliance task automation.

Benefits of Compliance Automation

Complying with regulatory requirements like **HIPAA, PCI DSS, GDPR,** and **ISO 27001** involves regular auditing and reporting to show a company's security controls are operating correctly. Automation makes managing compliance workflows much more efficient, reducing the time security teams spend on collating data and compiling reports for each regulating body. Some organizations report spending up to 50% less effort to meet compliance requirements when they introduced modern automation tools.

Compliance automation integrates well with tools for cloud security posture management (CSPM), cyber asset attack surface management (CAASM), and risk management. Asset discovery and monitoring gives teams deeper insight into information security risks they may otherwise overlook, allowing teams to detect vulnerabilities faster. Then, compliance automation tools can automatically remediate incidents when data is exposed, reducing both the impacts and costs of noncompliance.

Plus, compliance automation offers better observability into an organization's security controls. Visibility into control performance helps companies identify when they're not operating in compliance so they can avoid or mitigate the impacts of a breach. It can also help your team achieve and demonstrate compliance by showing the controls you've already implemented and their success.

Business Benefits Of Security Compliance Automation

- Avoid non-compliance fines and penalties
- Maintain customer trust
- Protect brand reputation
- Better data management
- Increase business efficiency
- Enhance security posture
- Improve access controls and accountability

Challenges of Compliance Automation

Even with automation playbooks out of the box for common compliance regulations, compliance automation software can't be plug-and-play because each company has unique compliance needs. That means that companies need strong procedures and regularly updated controls to maintain compliance and stay secure year after year.

While compliance automation software can help organizations introduce common controls in most IT environments, these automations still require a human touch to ensure they're working correctly. Any implementation involving a human touch risks information being input incorrectly, which can impact the success of compliance controls and the accuracy of the software's reporting.

The Role of Integrations in Compliance Automation

Successful compliance automation starts with seamless integrations. Observability across a company's cloud environments, databases, servers, applications, containers, and other elements of its IT infrastructure allows automation software to monitor the success of its security controls, regardless of where data is in motion or at rest.

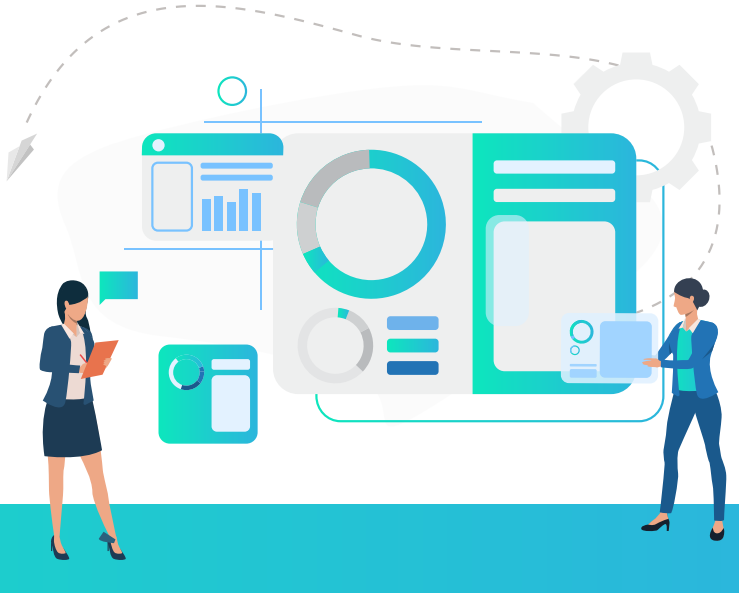
Limited visibility causes security teams more manual work compiling data from siloed sources, with no insight into whether controls are working as designed. Companies need comprehensive, end-to-end observability to automate compliance efforts, and the right software provides that by integrating every aspect of the company's IT infrastructure into a single dashboard view.

Out-of-the-box integrations with an organization's tools are crucial to show compliance with different regulatory requirements. For example, combining compliance automation with your Master Data Management (MDM) tools can simplify device compliance. Meanwhile, other integrations can support other compliance priorities, like integrating automation capabilities with your human resource management system (HRMS) to trigger security trainings for new employees.

The Future of Compliance Automation

With data volumes exploding and cybercrime on the rise, modern organizations can't afford to waste precious time and resources on compliance audits, risk analysis, and reports anymore. These companies need streamlined ways to manage ever-changing compliance needs and ensure that their security controls are working as expected. That's where Scrut Automation comes in.

Scrut Automation makes it easy to integrate all compliance workflows—including SOC 2, HIPAA, ISO 27001, GDPR, PCI DSS, and CCPA—into one comprehensive platform. Scrut automatically maps relevant information from 75+ integrations to relevant regulatory standards, saving security teams thousands of hours each year on compliance reporting and auditing. Through a single unified dashboard, organizations gain full end-to-end observability to see that their security controls are working exactly as intended.



Keep Your Security Controls in Check with Scrut Automation

There's no doubt that staying up to date on the latest cybersecurity and cybercrime trends can be daunting. The security landscape is rife with change, and CISOs need to know the lay of the land to ensure their organization stays secure. These three trends won't be disappearing anytime soon, so now is the time for CISOs to prepare by updating their security strategy and controls.

Thankfully, managing controls and preventing cybercrime doesn't have to be difficult.

Scrut Automation is here to help organizations simplify compliance, reduce risk, and protect their sensitive data. Teams who use Scrut report reducing manual effort by 70% to maintain compliance with HIPAA, ISO 27001, GDPR, SOC 2 and other common compliance standards.

Schedule a demo to see how Scrut can strengthen your security and compliance strategy today.