solarwinds

eBOOK

Turning Data into a Game Changer for Your Organization

Many organizations don't understand the risk to their data

Data can be a business' most valuable resource—but data is also valuable to cybercriminals. Whether they want to lock an organization's data to demand a ransom or exfiltrate it to sell on the dark web, cybercriminals have options for making money off this precious resource.

To top it off, breaches have become more numerous in recent years—2018 was the ***second most active year for data breaches***[1].

While data carries risks for an organization, it also presents major opportunities for cybersecurity professionals to demonstrate their significance. This eBook looks at some of the high-level elements you should think about when protecting your data—and it discusses how to use data-protection activities to help advance your team's credibility within your organization.

1 "Data Breach QuickView Report, Year End 2018 – Data Breach Trends," Risk Based Security. https://pages.riskbasedsecurity.com/2018-ye-breach-quickview-report (Accessed February 2019).

Determine Areas of Greatest Risk

Protecting your organization's data starts with mapping risks. You will need to define the level of security for data assets based on their risk levels. Define your mission-critical data and put appropriate safeguards in place. If you work for a bank, for example, financial data would need a high level of protection, such as requiring high levels of user privileges for people to access. Map these out and develop a plan to keep them safe.

Define the level of security for data assets based on their risk levels.

Additionally, define which employees represent the most risk, most often users with access to the sensitive data you've already mapped out. Enforce policies to keep these employees from unintentionally opening the organization to a data breach risk. For example, while an individual contributor using the corporate network may only need to log in using their username and password, you may want stricter requirements for high-risk c-level employees with access to sensitive data. This might include requiring multifactor authentication or asking them to use a VPN when accessing systems offsite.

Leverage Fundamentals to Fight Back Against External Threat Actors

Once your riskiest areas are defined, start implementing security fundamentals, like:

ANTIVIRUS

With new malware strains appearing online at a rapid clip and devastating ransomware attacks abounding, data protection absolutely requires strong antivirus (or even full-blown endpoint protection built on collective intelligence). Don't simply rely on signature-based scans; these are necessary but can't help with emerging threats. Make sure whatever solution you choose can look for elements that look like malware, like attempts to edit a system registry.

PATCHING

Software vulnerabilities leave an open door for cybercriminals to step through. Make sure you set up automation to keep patches current across your user base.

BACKUP AND DISASTER RECOVERY

When it comes to protecting data, there may be nothing more important than backup. A good backup solution should help you schedule backup jobs on autopilot. Additionally, you should be able to quickly back up to the cloud—and back up locally if you want a second copy (which is highly recommended for redundancy). Search for something optimized for the cloud. It should use techniques like compression and deduplication for fast transfers, and it should offer strong data encryption both in transit and at rest.

Beyond these technical solutions, user security training is a must. Email attacks, for example, often kick off larger data breaches and network compromises. Run regular trainings to keep employees from accidentally falling victim to phishing scams or malicious downloads. Also, during these trainings, emphasize other sound security practices, like setting strong passwords and enforcing multifactor authentication.

Many organizations see these trainings as a way of checking a box. **Don't fall into this trap.** Security trainings offer an excellent opportunity for your team to reinforce their value. Try to make the training as engaging as possible—choose your best speaker, have a slick presentation, offer handouts to improve retention, and maybe even consider running prize giveaways for people who answer questions correctly. You want people walking away not only remembering how to secure their data (and avoid falling victim to phishing scams), but also recognizing your team's importance.

Reduce the Risk of Insider Breaches

Insiders often know where you keep the most sensitive data. Current or former disgruntled employees could easily damage the organization by stealing or deleting important data—and let's not overlook the possibility of accidental data corruption or deletion due to simple employee error.

Start by making sure no one has excessive access privileges. As organizations grow, it's not uncommon for early employees to have "God mode" access to sensitive data. Employees that change roles often maintain their old privileges as well. A developer who once worked on the billing system shouldn't retain access to the old code and database if they move to a purely front-end developer role.

To combat these potential threats, adopt an access rights management system to help keep user privileges in check. This requires a few things. First, look for one that allows data owners across the organization to set up and manage privileges. The burden of managing and maintaining user access privileges shouldn't fall squarely on the shoulders of the IT staff. Managers usually know who needs what—so let them take responsibility for setting up, maintaining, and modifying accounts in their area.

Adopt an access rights management system to help keep user privileges in check.

That being said, you should also look for a solution that monitors for potential threats to internal data. For example, it should monitor and alert you to potential changes to Active Directory® structures or changes to Windows® file share or users who attempt to delete or transfer large swaths of files at a time. Also, regular audits can help. It's smart to periodically check to make sure data owners have been vigilant about policing user privileges.

Detection

Even the best laid defenses have gaps—clever cybercriminals can still break through. Whether it's a new ransomware strain or someone falling for a phishing attack, threats do sometimes slip by preventive measures.

The measure of a good team lies in how well they detect threats and respond to them. You can't deal with what you can't see, so you need to consistently monitor and review logs. However, collecting, normalizing, and reviewing logs can quickly consume your team (and prevent them from properly separating the signal and the noise.) Staffing and skills shortages across the industry can add to this overwhelm.

Implement a strong security information and event management (SIEM) tool.

To deal with this, find and implement a strong security information and event management (SIEM) tool. These tools can ingest logs from across the enterprise, normalize them so they're easy to process, and help teams make sense from the information flood. Beyond that, they often use automation or artificial intelligence to bubble up the most important security events and notify the team, so they can investigate further (saving important time in the day-to-day).

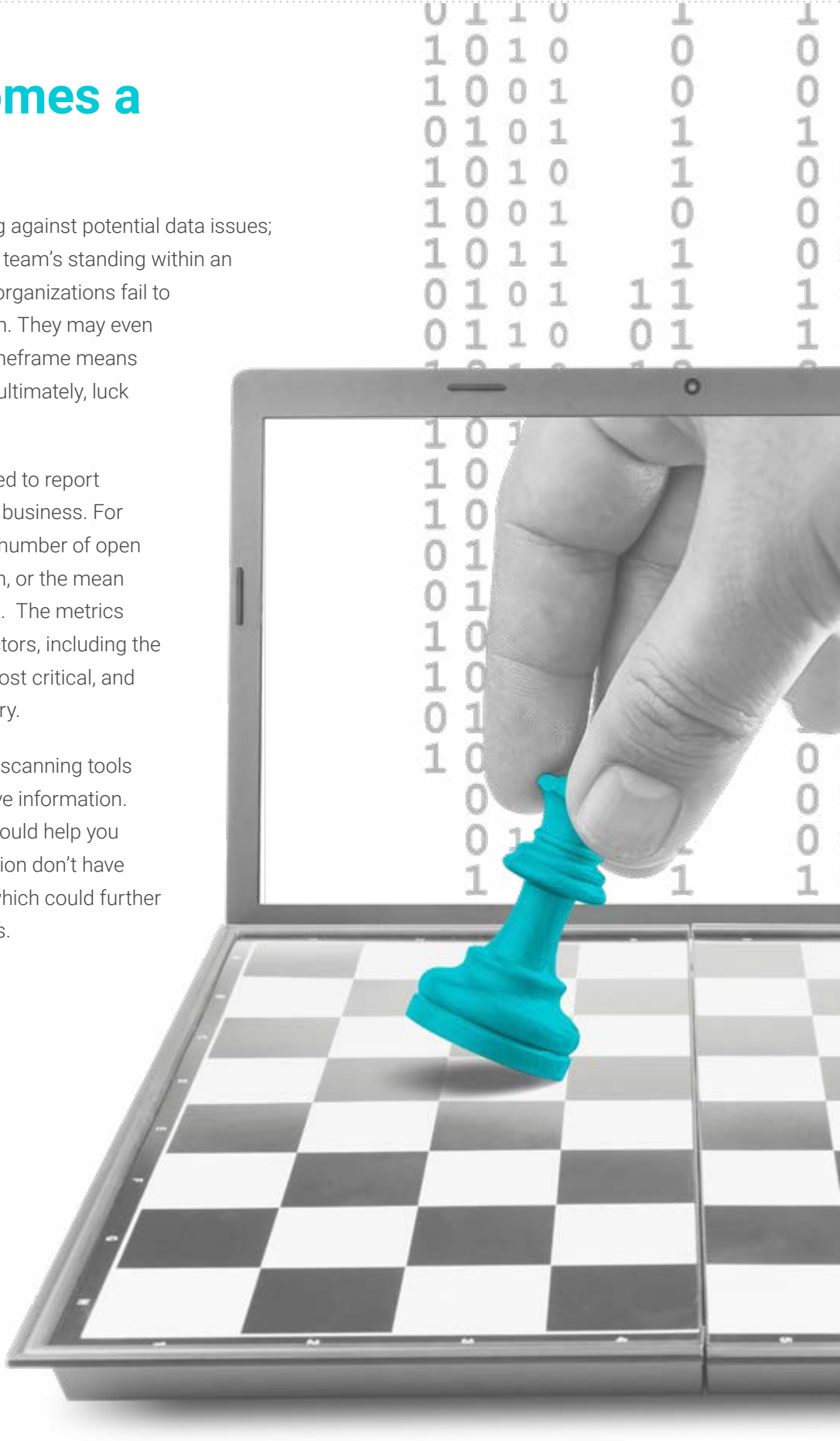
The right SIEM tool goes beyond log management—it also provides deeper context to the information your team receives. For example, it should compare the logs from systems like Active Directory, routers, firewalls, and intrusion detection systems, and make calculated decisions based on this. Many systems also integrate threat intelligence feeds to help better detect issues. This can help your team reduce the number of false positives and negatives over time.

How Data Becomes a Game Changer

The previous advice refers to defending against potential data issues; however, data protection can change a team's standing within an organization. Unfortunately, too many organizations fail to see the true value of their security team. They may even assume a lack of an attack during a timeframe means everything is working correctly (when, ultimately, luck plays a major role).

To demonstrate your value, you will need to report regularly on clear metrics that help the business. For example, you may choose to track the number of open vulnerabilities, the time it takes to patch, or the mean time to identify and respond to a threat. The metrics you choose will depend on multiple factors, including the size of your organization, data that's most critical, and whether you work in a regulated industry.

Additionally, you may want to use data scanning tools to demonstrate you've secured sensitive information. Your access rights management tool could help you show that people within your organization don't have privileges beyond what's necessary—which could further demonstrate the value of your activities.



The Role of Compliance

Security investments are often driven by regulations. One recent example was the scramble for businesses to meet the requirements of the General Data Protection Regulation (GDPR). Businesses often have to keep up with changes to existing regulations, like HIPAA in healthcare, SOX in finance, or PCI DSS in retail.

Cybersecurity teams play crucial roles in meeting these regulations. These teams need solutions to help them demonstrate compliance and due diligence where needed. For starters, they need simple, easy-to-understand reports in case of an audit. For an access rights management solution, you'll want simple, audit-ready reports that can demonstrate who has access to what (and demonstrate you're taking proper steps to implement "least privilege.")

Additionally, a SIEM tool is paramount for compliance efforts. A SIEM tool can help you show you're taking proper measures to safeguard data, but it should also help you in the event of a breach you need to report. When reporting a breach, you'll need to explain what was affected, who was affected, and what steps you took to mitigate the damage. The ability to track down this information requires strong forensic tools—and a way to easily search logs to make sense of them after an attack.

Finally, teams should make sure they never just "meet compliance" regulations. Cybersecurity should never be about checking a box. Criminals evolve their attack methods so frequently, many regulations simply can't keep up. To help mitigate risk, cybersecurity teams should modify their defenses accordingly—and demonstrate to their organization they're staying way ahead of the cybercriminals.

SolarWinds Access Rights Manager

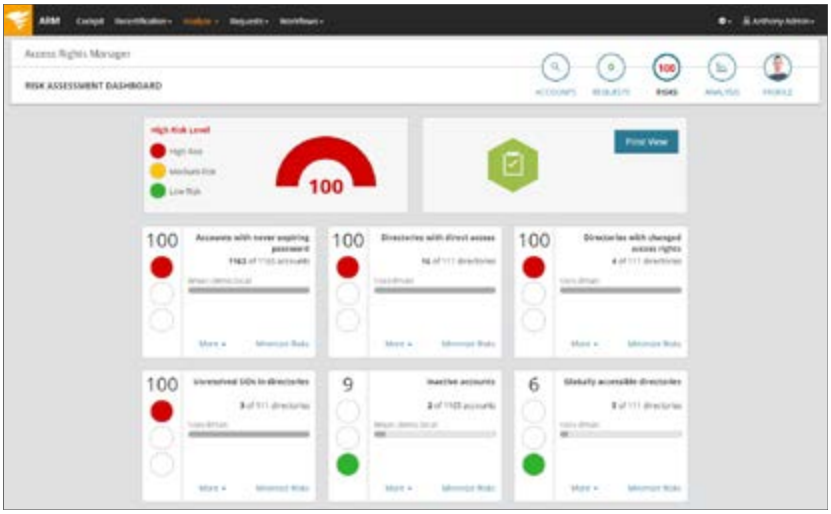
Data sits at the heart of everything you do.

If businesses want to truly protect their data, they will need near-comprehensive layered security to fight back against the bad guys. That means cyberhygiene measures, like patching and antivirus, and advanced threat detection for threats that slip past the first few layers of protection. However, insider threats—either malicious or accidental—can pose serious risks to the organization.

TRY IT FREE

30 days, full version

SolarWinds® **Access Rights Manager (ARM)** is designed to help businesses prevent data leaks by streamlining the user permissions process. With ARM, the IT team can outsource user provisioning to data owners across the organization, typically team leads or managers, while allowing for department-specific templates to help keep user accounts and permissions consistent (and secure) across the business. The system monitors changes to systems like Active Directory®, SharePoint®, Windows File Share, and Microsoft® Exchange™ to assist in preventing attacks. Additionally, ARM allows users to quickly audit permissions across the organization and produce reports designed to help demonstrate compliance. These reports can also help illustrate the value of your data protection work, turning your business' data into a game changer for your team.



Your organization's data is too valuable to leave vulnerable to insider attacks. SolarWinds Access Rights Manager is designed to help.

Learn more by visiting **solarwinds.com/access-rights-manager**.