solarwinds

eBOOK

Help Protect Your Company from a Data Breach

A guide for IT professionals

Introduction

HELP PROTECT YOUR ORGANIZATION FROM A POTENTIALLY DEBILITATING DATA BREACH

According to The Ponemon Institute in its annual study, the average cost of a data breach is roughly $3.86 million USD, or an average of $148 USD per data record stolen[1]. This number has increased from the previous year's report, showing that breaches are growing costlier to businesses that get successfully attacked. Perhaps even scarier, the report claims that the mean time to identify a breach was 197 days. That's almost 200 days that a cybercriminal can have access to someone's data.

If businesses want to avoid ending up on the wrong side of a breach, they will likely need to increase their security measures, particularly around threat detection.

If businesses want to avoid ending up on the wrong side of a breach, they will likely need to increase their security measures, particularly around threat detection.

Until recently, many software tools on the market that can help businesses detect and remediate threats to their networks (and ultimately their data) have been cost- prohibitive. As a result, these critical offerings have remained out of reach for many technology professionals. Not anymore.

SolarWinds® Security Event Manager (SEM) was built to help make security services accessible for companies of nearly any size by reducing the cost and complexity of threat detection, response, and reporting. SEM allows businesses to deploy advanced security detection to help reduce the risks to their networks, IT assets, and data.

TRY IT FREE

30 days, full version

However, before we get into the nuts and bolts of SEM, we should start by looking at the idea of cyber-risk in general.

CYBER-RISK: A RISK TO YOUR NETWORK IS A RISK TO YOUR DATA

Cybercriminals try to use an employee's good will or naiveté to harm companies by sending emails that contain viruses, malware, or ransomware that could potentially and accidentally be distributed throughout the organization.

*For years, one of the greatest sources for data risk has come from **email**.*

[1] "2018 Cost of a Data Breach Study: Global Overview," Ponemon Institute and IBM. https://www.ibm.com/security/data- breach (accessed September 2018).

There are also employees with bad intentions who look to personally profit by stealing corporate data and selling it to external parties. Social media and other messaging channels provide more methods for malicious insiders to distribute information than ever before, making this perhaps a greater risk than it was in the past.

Data risk often starts with your network. If a cybercriminal can gain a foothold in your network, they may have free reign with your data. Depending on the extent of the intrusion, cybercriminals could make off with sensitive customer data, employee data, health information, intellectual property, or financial records. This in mind, it's absolutely crucial to make sure you have strong protection to keep your network safe if you want to keep your data safe as well.

If a cybercriminal can gain a foothold in your network, they almost have free reign with your data.

LAYERED SECURITY CAN HELP

In this age of ransomware and malicious code, technology professionals usually know that security is about more than antivirus. You need layers to protect your business effectively.

For starters, businesses need to remain up-to-date with the latest security patches. Cybercriminals can find exploits in software and then automate their attacks to search for vulnerable software. As a result, staying up to date with patches is security 101. A good patch management solution can automate a lot of the manual process of keeping software up to date, making it a potential quick win for many businesses.

A good patch management solution can automate a lot of the manual process of keeping software up to date, making it a potential quick win for many businesses.

As mentioned before, email security matters a great deal. A robust email security solution can potentially help prevent a good portion of threats. Not to mention, user awareness training—teaching people to take precautions when receiving a new email to avoid phishing or spear-phishing—can also potentially help.

Yet these two examples only take you so far. What happens when your email security does falter? What happens when an exploit is discovered and used against you before there's an available patch?

TRADITIONAL LAYERED SECURITY IS ONLY PART OF THE SOLUTION

When traditional layered security measures fail to prevent an intrusion, businesses need to be able to detect the intrusion quickly. One way to do this is via proactive security monitoring, which adds an additional sophisticated layer to your security.

*While your other measures can be your “locked doors” and “barred windows” to keep intruders out, **proactive security monitoring can be your alarm system** if someone does break in.*

SolarWinds Security Event Manager was designed to help you proactively monitor your environment to help you see anomalies that arise based on vulnerabilities and thresholds. SEM correlates event log activity across your organization and alerts you to suspicious activity that could pose a risk to your network and, ultimately, your data assets. This is designed to provide valuable insight to help maximize security visibility across your environment, while allowing you to help safeguard and manage your IT assets.

By alerting you to the presence of potentially damaging behaviors, SEM was built to help you avert or minimize their impact. You can correlate and store logs from multiple sources and perform full-text searches across large numbers of events. Almost any log or event type is supported, so there is no need for multiple applications or extra bandwidth for pushing and pulling logs to multiple locations.

SEM provides a mechanism to help shut down potential breach activity before it becomes a breach, and also provides an information trail designed to help defend against heavy fees and penalties imposed when a sustained breach occurs. With SEM, you get email notifications when suspicious traffic shows up on your network to potentially help you stop a breach *before* it happens.

By alerting you to the presence of potentially damaging behaviors, SEM was built to help you avert or minimize their impact.

Ultimately, SEM is designed to provide:

- Centralized security monitoring across your network
- A seamless experience for your end users
- Advanced search and forensic analysis
- Audit trails, near real-time alerts, anomaly detection, and more
- Automated responses against threats

With SEM, you get email notifications when suspicious traffic shows up on your network to potentially help you stop a breach before it comes to fruition.

QUICKLY PRODUCE A COMPREHENSIVE UNDERSTANDING OF THE IT ENVIRONMENT

Whether you are faced with PCI DSS, HIPAA, FFIEC, SOX, or other compliance regulations, SolarWinds Security Event Manager is intended to help you prevent potential violations via audit-ready reports.

SEM offers help with centralized IT compliance with multi-conditional, cross-correlated alarms with customizable actions and on-demand or scheduled reporting. This allows you to summarize and identify important events from one location and dashboard. Intrusion detection includes Snort and access to the Emerging Threats rule server for threat intelligence. With SEM, you can also integrate with a wide range of existing IDS/IPS solutions to provide log normalization and correlation—and vulnerability reports can be ingested through any of our predefined connectors.

*Get SIEM capabilities and detailed compliance reports so you can demonstrate to assessors that you are **working to meet requirements.***

MITIGATING CYBER-RISK THROUGH PROACTIVE SECURITY MONITORING

Providing proactive protection can help demonstrate value to your stakeholders. SEM was designed to tell you when an attack may be happening so you can mitigate and minimize the impact.

The security landscape changes on almost a daily basis. Understanding your organization's vulnerabilities and the potential risks to your network (and your data) allows you to react accordingly and efficiently, preemptively addressing risks before they become a probSEM and having the right visibility into when a breach may be occurring.

Now is the time for a flexible and scalable SIEM platform that you, as a technology professional, can implement and use almost immediately to start safeguarding your IT landscape. SEM was designed to empower any organization to quickly deploy a robust SIEM platform—scaling for growth as it occurs while using existing resources.

Implementing your layered security approaches and using the appropriate tools can potentially allow you to stay up-to-date in this ever-changing security horizon.

Implementing your layered security approaches and using the appropriate tools can potentially allow you to stay up-to-date in this ever-changing security horizon.

solarwinds

For additional information, please contact SolarWinds at 866.530.8100 or email sales@solarwinds.com.
To locate an international reseller near you, visit http://www.solarwinds.com/partners/reseller_locator.aspx