



5 + 1 Ways to Reduce Your Cybersecurity Risks

5+1 Best practices to bolster customer
privacy and protect your brand value

Table of contents

Introduction: Adapt to a new digital world	3
Protect your endpoints	6
Create a culture of security	8
Manage vendor risks	10
Bolster firewall protection	12
Monitor log files	14
Mitigate risks	16
Achieve lasting business value	18

Introduction

Adapt to a new digital world

The rapid spread of digital technology is enabling organizations to quickly roll out new products and services to meet shifting customer demands. Although the digital world offers boundless possibilities for growth and value creation, it comes with its own set of challenges and risks. Wider interaction capabilities increase the number of touch points and the amount of personal data that must be secured. For hackers, the digital age opens up a virtual playground of opportunities to penetrate security defenses and gain access to customer data, intellectual property, and other assets. While some security breaches gain widespread publicity, others are sneaky enough to remain hidden for extended lengths of time. Whether caused by human or technical failure or a deliberate strike, a single security breach can be catastrophic for a business. According to data reported in SAI Global's Consumer Trust Index, 43 percent of consumers indicated they would never return to a company if their private data had been breached. But it's not just the potential loss of revenue that can be so damaging. If a company loses the trust of its customers, prospects, partners, or investors, the results can be devastating. Data breaches produce immediate public perceptions that can severely impact an organization's brand and reputation — and the damages can persist for years after a breach.

Building a solid foundation for good security requires an IT infrastructure and operating culture that not only safeguard data and minimize risk but help make the business more agile, responsive, and transparent.

Keep pace with persistent threats

Today's trends can make it tougher to stay secure: the adoption of cloud, mobile, and other digital technologies has increased the potential attack surface. Next-generation customer experiences leverage the Internet of Things (IoT) to create convenience and satisfaction among shoppers. However, the devices that connect consumers to networks also increase the number of customer touch points, integration intersections, and personal data that must be secure. At the same time, IT security teams are engaged in an intensive war against clever enemies as they struggle to keep pace with the rapidly evolving threat landscape.

Ransomware is a good example. When ransomware gets into your network, it encrypts all your files with what is essentially an impenetrable code. The only way to unlock files is to pay a ransom. For the victim, agreeing to pay ransom often appears to be the only viable option. The lesson? It doesn't matter what type of information or security controls you have in place; cybercriminals will target any vulnerabilities they can find.

Even as companies recognize the importance of data security, many struggle to implement effective programs without detracting from other business priorities. Rather than seeking a "quick-fix" solution, IT professionals should start by building an integrated, comprehensive data security strategy. Without proper planning and a defined roadmap, organizations can end up with a mishmash of technologies from different vendors that don't integrate well, offer poor visibility, and leave systems and infrastructure vulnerable to hackers.

Building a solid foundation for good security requires an IT infrastructure and operating culture that not only safeguard data and minimize risk but help make the business more agile, responsive, and transparent. The challenge is striking the right balance among protection, cost, speed and agility, and user flexibility. For security teams, a good starting point is to identify and mitigate risk wherever possible. Accepting the fact that breaches are going to happen is a hard pill to swallow. How can you get ahead of such a large issue? Building a security fortress for your business is more than just building strong walls. A strong security infrastructure is critical to a strong cybersecurity posture. How can you see invaders coming before they appear on the horizon, before all your walls are in place or before they are replaced with stronger, better blocks? What are the best items to include in your security posture strategy? Try these 5 + 1 ways to build up your walls as well as also keep your eyes on the horizon for intruders.

Protect your endpoints

The escalating danger and devious nature of today's threats make the deployment of advanced endpoint protection more critical than ever. The first step to addressing endpoint security is identifying precisely what types of endpoint connections you have.

Without complete visibility, it's difficult to identify vulnerabilities and determine security effectiveness. Endpoint monitoring solutions allow you to efficiently monitor network activity and identify anomalies that point to potential threats so you can shut them down before they become a full-blown breach. Best practice protective measures include:

- Keeping patches current: Cybercriminals are continuously on alert as weakness are exposed and will attempt to exploit any security gaps they can find. Make sure your policies include automated enforcements that keep network systems current with the latest vulnerability patching.
 - Implement advanced authentication: Once a single employee account is compromised, a hacker will often reuse the password to access other systems. Advanced authentication will thwart these attempts no matter how the hacker gained access to the password.
 - Employ encryption: Encryption safeguards the information in transit and on the endpoint devices, preventing attackers from copying or transferring that data. For even greater protection, consider full-disk encryption, which encrypts the complete hard drive, protecting the data as well as the applications and operating system.
- Apply application controls: Application controls help prevent prohibited users from launching or downloading applications on the endpoint device. They also protect the network from possible security threats with the ability to block departing employees from access to critical business systems and applications.
 - Gain holistic perspective: Use internal and external penetration testing to identify vulnerabilities, and actively exploit them to provide attack vectors against your security infrastructure.

Without complete visibility, it's difficult to identify vulnerabilities and determine security effectiveness.



Create a culture of security

As digital trends continue to reshape markets and industries, business leaders should also continue reevaluating their organizational approach to security. Technology plays a vital role, but the importance of creating a strong security culture cannot be overlooked. Hackers are continuously finding new ways to penetrate your defenses, which is why creating a culture with a consistent awareness of threats is so critical. Workers can't apply effective security measures if they aren't well-informed of security practices and policies or the latest threats and how to spot them. Teach employees about safe internet practices and how to identify social engineering and phishing attacks.

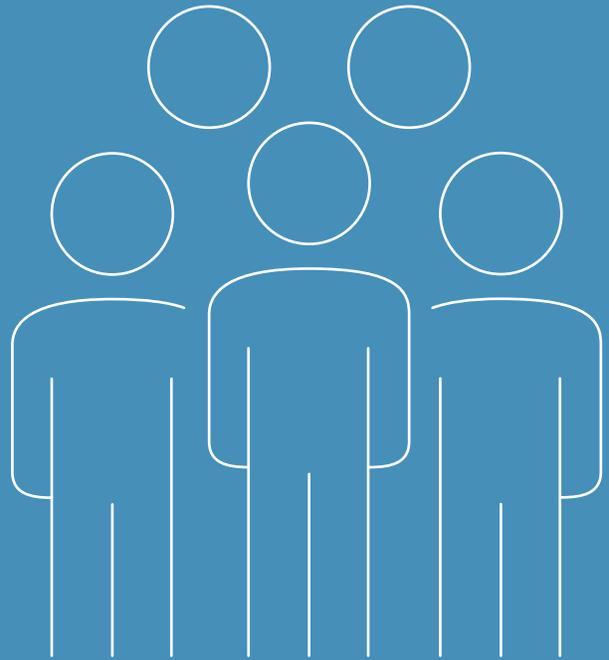
Test their security awareness with mock attacks, simulations, and interactive security activities.

Consider gamification techniques as a way of motivating team members and educating them on best practices.

Rather than attempting to be all-encompassing and trying to accomplish too much too fast, focus on incremental progress and quick wins. The primary goal is to implement change and gain buy-in from those involved—with a clear understanding of the results that can be achieved. Identify the behaviors your organization wants to promote and align them with business goals. This will help employees better understand the value security has within the organization.



Identify the behaviors your organization wants to promote and align them with business goals. This will help employees better understand the value security has within the organization.



Manage vendor risks

Organizations are increasingly expanding their third-party relationships beyond core infrastructure and application outsourcing. As vendor access to customer data increases, organizations need to apply the proper level of scrutiny to ensure sensitive data remains protected in a way that complies with applicable legal and regulatory requirements. Organizations have often relied on third-party vendors to provide vital security protections, but yet haven't completed risk assessments to identify any security gaps that may exist within the vendor's security program. According to a 2017 survey, 51 percent of respondents reported they rely on ad hoc or basic risk governance processes to manage supply risk, indicating a general level of immaturity in this area. Despite this lack of proficiency, they viewed their capacity to effectively manage risk to be sufficient.

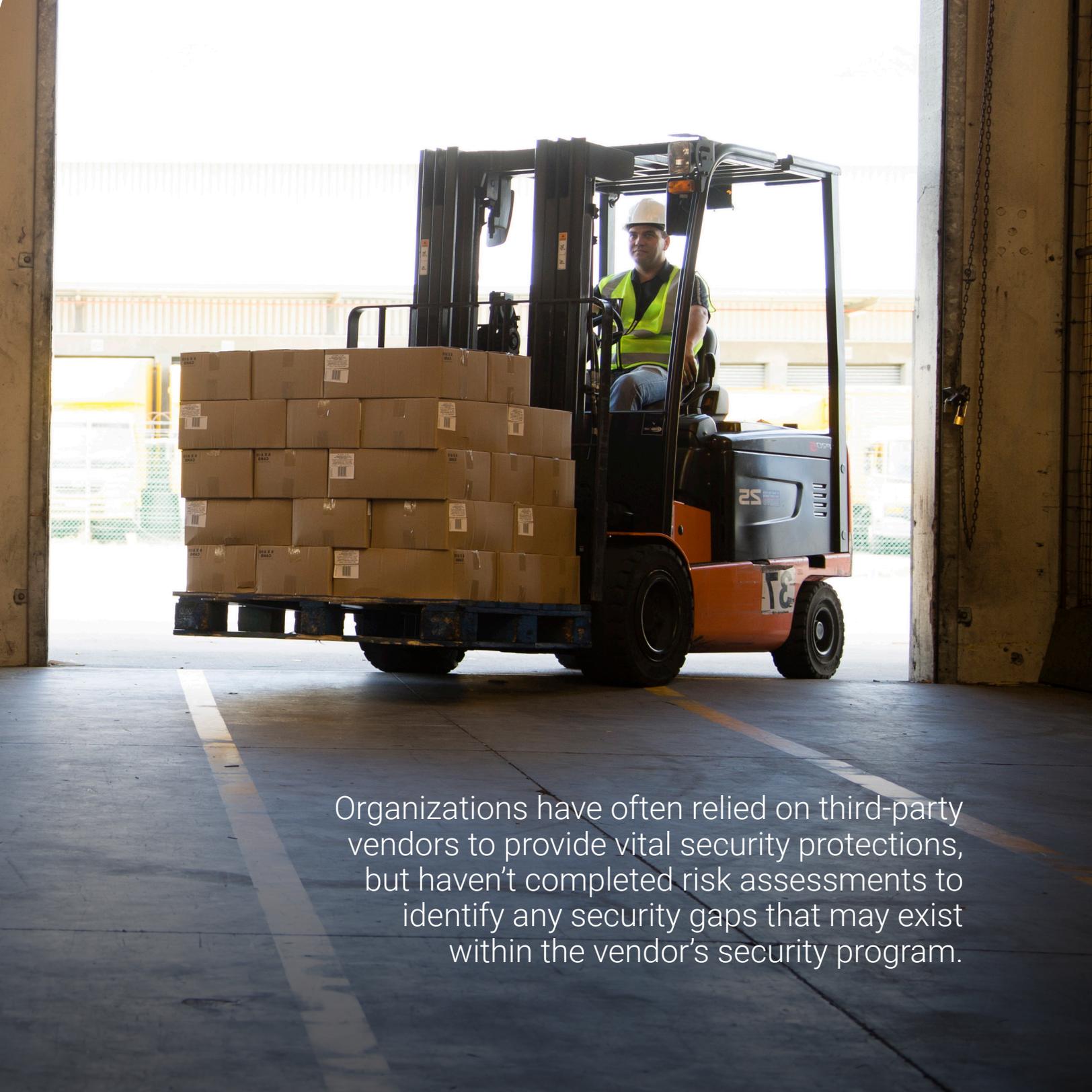
All IT service provider contracts should be examined to ensure that adequate protections and processes are in place.

IT STAFF CAN VERIFY WHETHER THE VENDOR HAS

1. Established a secure environment
2. Employed competent, well-trained security personnel
3. Implemented internal governance processes needed to reduce the risk of data breaches and other intrusions

BEST PRACTICE MEASURES INCLUDE

- Knowing what type of data resides in your organization, which vendors have access to the data, and what protective measures are in place to safeguard it
- Spelling out in detail in every vendor contract who, how, and why each vendor will access your data
- Tiering your vendors based on their criticality and applying scoring to identify which vendors should be reviewed more regularly
- Conducting regular data security audits with your vendors and reviewing your contractual provisions for potential issues before they escalate into bigger problems
- Enforcing compliance — specify measures that protect your company data and shield you against any breach or loss as a condition of doing business



Organizations have often relied on third-party vendors to provide vital security protections, but haven't completed risk assessments to identify any security gaps that may exist within the vendor's security program.

Bolster firewall protection

The digital age is driving a shift in focus from securing network perimeters to protecting data distributed across devices, operating environments, the cloud, and emerging IoT environments. The first layer of defense is an up-to-date and optimally configured firewall. Thanks to improvement in firewall protection capabilities, achieving effective network security without giving up performance is attainable and affordable.



Next-generation firewalls have been designed with an enterprise focus, including advanced features like intrusion prevention, application-level inspection, and granular policy control. These firewalls can detect intrusion attempts, stop malware from penetrating the network, identify unauthorized traffic access, and apply application-specific and user-specific security policies.

Many traditional security solutions are effective at stopping illegitimate traffic and provide network-level security, but don't have the ability to detect and stop other attacks resulting from vulnerability inherent in web applications. Web application firewalls (WAFs), on the other hand, offer an effective solution for detecting threats examining incoming HTTP requests before they reach the server. Depending on the selected options, the WAF can block the traffic, challenge the visitor by asking to input a CAPTCHA, or instruct the server to simulate an attack.

Poorly configured firewalls, and a lack of internal network segregation could leave you exposed to a potential cyber attacker and unable to monitor traffic traversing the network for intrusions, malware and malicious applications. An internal segmentation firewall can help address this issue. Deployed between two or more points on the internal network, the internal segmentation firewall is designed to allow visibility, control, and mitigation of traffic between those segments.

Whether hardware- or software-based, firewalls are a critical component of any network security system. They can be installed inside the network as core firewalls to segregate traffic, or at the edge.

Whether hardware- or software-based, firewalls are a critical component of any network security system.



Monitor log files

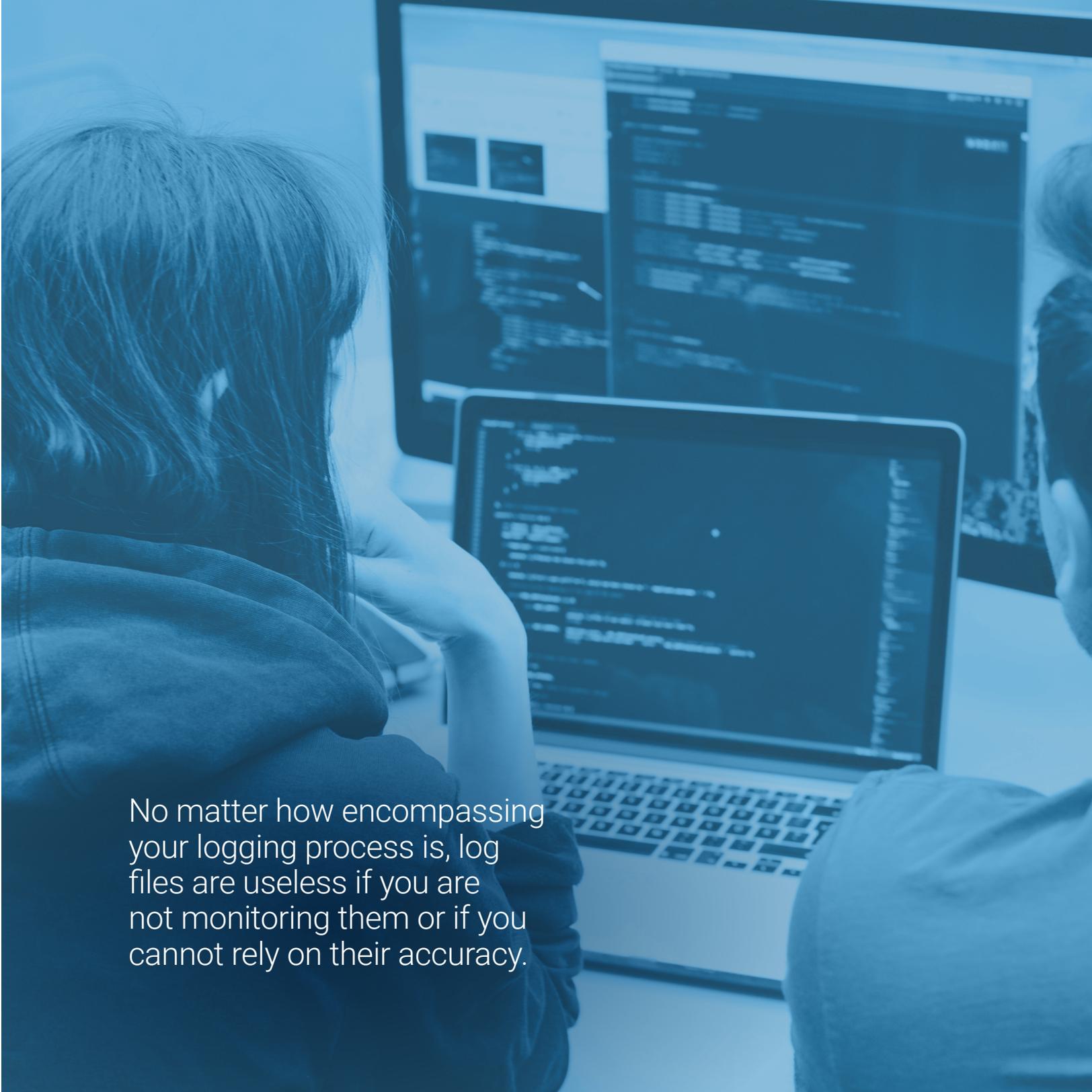
At the heart of network security is the ability to record events and execute actions based on those activities. Log monitoring pinpoints the root cause of any application or software error – typically the analytics component is part of a larger platform/system that includes log monitoring. Monitoring provides safeguards against gaps in application and perimeter defenses by notifying you of issues so defensive actions can be employed before any serious damage occurs.

A security information and event management (SIEM) solution can be an important instrument in your security toolkit. SIEM platforms operate as your team's central nervous system to alert and enact countermeasures when a threat is looming. SIEM platforms recently evolved further to collect data about users' behaviors and data access. SIEM platforms may collect data from hundreds of sources, including hardware devices, virtual machines and applications such as Microsoft Exchange and Oracle databases.

Even smaller networks can produce too much data to be analyzed manually. Log analyzers play a vital role by automating the analysis and auditing of logs. Consistently collecting this information will help in monitoring access controls and can provide an accurate audit trail when investigating an incident. The feedback can also help improve firewall rule sets and intrusion detection system (IDS) signatures. Regularly tuning your devices improves their accuracy in recognizing valid threats, helping reduce the number of erroneous notifications.

No matter how encompassing your logging process is, log files are useless if you are not monitoring them or if you cannot rely on their accuracy. Hackers will frequently attempt to modify log files to conceal their tracks. To defend against this, you should download log files locally as well as to a remote location. This redundancy adds an extra layer of protection, enabling you to compare the two log sets with one another – any variations will signify suspicious activity.





No matter how encompassing your logging process is, log files are useless if you are not monitoring them or if you cannot rely on their accuracy.

Mitigate risks

In terms of security breaches, it's not if, but when. No matter how strong your defenses are, cyberattackers will find ways to access what they're after. Although perimeter defenses are essential to help prevent intrusions, organizations need to go further to identify, prevent, and eliminate the attacks in near-real-time as they occur. This requires new methods of threat detection, analysis, and elimination, as well as clear frameworks and action plans that govern the reaction in case of a breach.

Expert testing and research can help you understand where you are most likely to be attacked so you can create a methodical plan to deal with most security breaches. The key is to have a strategy that includes people, processes, and technology to spot problems, respond effectively, and minimize impact. Since there is no one solution and strategy to defend against all security threats, businesses must assess their ability to effectively react to and mitigate an incident.

- Containing a problem rapidly and effectively can make all the difference
- Carefully evaluate your capabilities to determine if your organization is adequately prepared to respond effectively to a breach by an advanced threat
- Update technologies, processes, and skills needed to detect when a compromise occurs
- Equip first responders with the tools they need to react quickly and investigate the source and impact of security breaches, compromises, and incidents

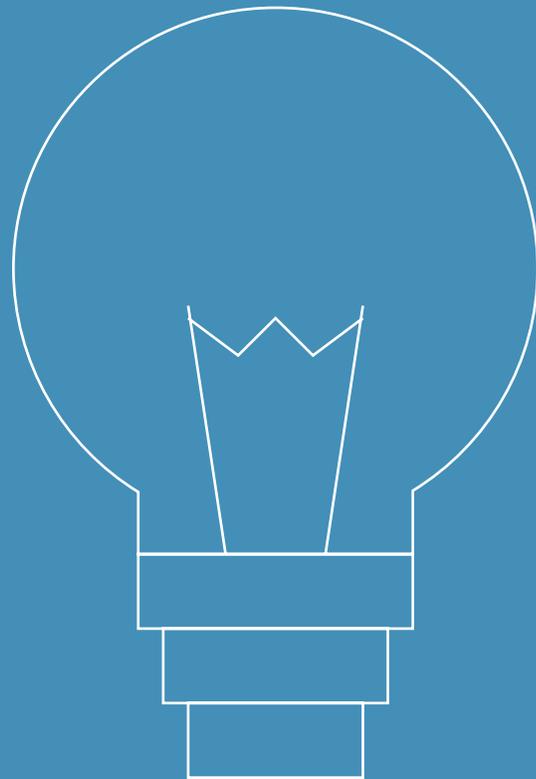


Achieve lasting business value

As improvements in network connectivity continue to provide vast benefits, organizations are increasingly challenged by high-level attacks designed to disrupt operations, diminish performance, and compromise data. Striking the optimum balance between data security and user flexibility is no easy task.

The good news is that with the right mix of technology, internal processes and an embedded security culture, higher performance and better security are possible. Through a combination of hardware, software, services, and best practices, organizations can minimize their risks and reduce the attack surface that their business presents to the world.

How can your organization take advantage of the important benefits of digital technology and bolster its protection against cyberattacks? A smart first step is to seek out an expert risk management consultant for guidance.



Next steps and resources

[From Spreadsheets to Software: The Intelligent Way to Manage Third-party Risk](#)

[Managing Your IT GRC Programme: Third-party Risk](#)

[Prepare for Cyber Attacks: How SAI Global Helps You Prepare for the Inevitable](#)

[More about IT Vendor Risk Management](#)

For more information, contact SAI Global by visiting www.saiglobal.com

About SAI Global

SAI Global helps organizations proactively manage risk to create trust and achieve business excellence, growth, and sustainability. Our integrated risk management solutions are a combination of leading capabilities, services and advisory offerings that operate across the entire risk lifecycle allowing businesses to focus elsewhere. Together, these tools and knowledge enable clients to develop an integrated view of risk. To see our tools in action, request a free demo.

We have global reach with locations across Europe, the Middle East, Africa, the Americas, Asia and the Pacific.

For more information visit www.saiglobal.com.