

Security on a budget: Building cyber resilience for resource-constrained teams



Contents

Introduction	03
Patch management	04
Multi-Factor Authentication (MFA)	05
Domain Name System (DNS) Security	07
Backup strategy	09
Next-generation firewalls	10
Threat modeling	11
Partner with the right MSSP	14

Introduction

In today's economic climate, businesses across industries are facing unprecedented challenges. With revenue targets falling short and budget cuts looming over every department, including cybersecurity, organizations are under immense pressure to manage their profit and loss (P&L) effectively.

This pressure is particularly heightened for companies aiming to move closer to an Initial Public Offering (IPO) or Merger and Acquisition (M&A), where the imperative to become Earnings Before Interest, Taxes, Depreciation, and Amortization (EBITDA) positive is paramount.

But that's not it, as regulatory requirements continue to evolve and tighten, organizations are compelled to do more with less, navigating the delicate balance between compliance and cost management.

Mid-market enterprises are at a higher risk of cybersecurity attacks, compared to larger enterprises. But why? Because they are easy targets of cyber criminals, considering their limited budgets and resources.



A whopping 57% of midmarket businesses have been the victims of cyberattacks, and over 60% of those attacked go out of business.

[Click here to read full article](#)

Medium-sized businesses also often experience large financial losses, with cyberattack costs going sometimes as high as \$3 million (Verizon / IBM / Accenture, 2023). This cost includes the costs of looking into the breach, alerting the impacted customers, putting in place the security measures required to prevent similar incidents in the future, and any legal repercussions from the event.

The question is, how should mid-market businesses deploy security on a budget? Well, we are here with this ebook that shares some practical cybersecurity tips to take pressure off the already tight budget.

1. Patch management



Imagine a small-town bakery that prides itself on its freshly baked goods. One day, the owner discovers a small hole in the wall that could allow pests to enter and contaminate the ingredients. Ignoring the issue could lead to spoiled products and damage the bakery's reputation.

In the same way, neglecting software vulnerabilities in a mid-market company's systems is like leaving that hole unpatched. It opens the door for cyber threats to infiltrate and compromise sensitive data, potentially leading to significant financial losses and reputational damage.



Patch management involves the systematic process of identifying, acquiring, testing, and deploying software updates or patches to address vulnerabilities and security flaws in operating systems, applications, and firmware. Its primary objective is to enhance the security posture of systems and mitigate the risk of exploitation by cyber threats.

Why is patch management essential for mid-market companies to keep systems and software up-to-date?



Vulnerability mitigation

Patch management helps mid-market companies promptly address known vulnerabilities in software and systems, reducing the risk of exploitation by cyber attackers.



Protection against cyber threats

Regular patching closes security loopholes that attackers could exploit to gain unauthorized access, install malware, or disrupt operations, minimizing the likelihood of security breaches.



Compliance adherence

Effective patch management ensures compliance with regulatory requirements and industry standards that mandate the timely application of security patches to protect sensitive data.













Business continuity

Patch management contributes to business continuity by preventing downtime caused by security incidents, enabling uninterrupted operations and preserving customer trust and reputation.

Proactive patch management strengthens cybersecurity defenses, reduces the likelihood of security incidents, and demonstrates a commitment to protecting customer data and regulatory compliance.





For effective patch management:

	Establish robust processes for identifying, testing, and deploying patches across IT infrastructure.	
	Regularly monitor for software updates and security patches from vendors.	
	Prioritize patches based on criticality and relevance to the organization's environment.	
	Test patches in a controlled environment before deploying them to production systems.	
	Consider automating patch management tasks to streamline the process and minimize manual effort.	

2. Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) emerges as a cornerstone of defense, offering an additional layer of protection beyond traditional passwords. It requires users to provide multiple forms of verification, such as a password, fingerprint scan, or security token, MFA fortifies access controls and mitigates the risk of unauthorized account access.

Here's an example of how MFA could help:

	Consider that a mid-sized e-commerce company fell victim to a phishing attack when one of its employees unknowingly clicked on a malicious link in an email .	
	The attacker gained access to the employee's credentials and attempted to log in to the company's online payment system to initiate fraudulent transactions.	



However, due to the implementation of **multi-factor authentication (MFA)**, the attacker was thwarted at the login screen. Even though they had the employee's username and password, they couldn't proceed without the **secondary authentication factor**, which saved the company from potential financial losses and reputational damage.



Why implement MFA?



Enhanced authentication

MFA adds an extra layer of security beyond passwords, reducing the risk of unauthorized access to systems and data.



Mitigation of credential theft

By requiring multiple factors for authentication, MFA mitigates the impact of credential theft and phishing attacks, safeguarding sensitive information.



Protection against insider threats

MFA helps prevent insider threats by reducing the likelihood of unauthorized access to critical resources, even in the event of compromised credentials.



Compliance adherence

Implementing MFA aligns with various regulatory requirements and industry standards, demonstrating a commitment to data security and compliance.

Learning by Example

Cybersecurity breaches at industry pioneers due to delays in MFA implementation



Industry giants like [Microsoft](#) experienced breaches due to delayed MFA implementation. These breaches not only resulted in data compromise but also tarnished reputations and incurred substantial financial losses.

Financial technology firms like [Coinbase](#) experienced the harsh reality of Account Takeovers (ATO) firsthand. As a result, they [later implemented measures](#), such as encouraging customers to opt-in for Multi-factor Authentication (MFA), to mitigate the risks associated with unauthorized access.



Here's how to implement MFA effectively:



Assess the need

Determine which systems and applications require additional security layers and where Multi-Factor Authentication (MFA) would be most beneficial.



Choose the right solution

Select an MFA solution that aligns with the company's budget, technical requirements, and user experience expectations.



Implement gradually

Roll out MFA gradually across different systems and user groups to minimize disruption and ensure smooth adoption.



Educate users

Provide comprehensive training and support to users on how to set up and use MFA effectively to enhance security without hindering productivity.



Monitor and adjust

Continuously monitor MFA usage, gather feedback from users, and refine policies as needed to optimize security posture over time.

Implementing MFA can present challenges, particularly in ensuring consistent application across organizational systems. OAuth login approaches offer a streamlined solution, allowing organizations to leverage existing authentication mechanisms to enforce MFA.

By integrating OAuth protocols, such as those offered by Google Workspace, businesses can standardize MFA implementation while enhancing user experience. This approach not only simplifies access management but also bolsters security by preventing unauthorized access post-termination.

3. Domain Name System (DNS) Security

Using security protocols such as DNSSEC, enforcing strict DNS logging, and setting up redundant DNS servers are just a few of the overlapping barriers that make up a successful DNS security approach.

Security was not a priority while designing DNS, and numerous attack methods have been developed to take advantage of these flaws. Here's why DNS security is essential:

- ✓ Helps thwart DNS spoofing, cache poisoning, and unauthorized network access, businesses can **fortify their defenses against malicious actors.**

- ✓ DNS security also aids in blocking access to malicious domains hosting malware and phishing sites, **reducing the risk of data breaches.**
- ✓ Employing encryption protocols like DNS over HTTPS (DoH) or DNS over TLS (DoT) **enhances data privacy by safeguarding communications** from eavesdropping and spoofing attempts
- ✓ Detecting and blocking suspicious DNS traffic indicative of command and control (C2) communications **helps prevent malware from exfiltrating data or receiving instructions from attackers.**

Here's how to implement DNS security effectively:

	Evaluate DNS infrastructure Conduct a thorough assessment of current DNS infrastructure to identify vulnerabilities and weaknesses.	
	Implement DNS security solutions Deploy DNS security solutions such as DNS firewalls, DNSSEC, and DNS filtering to protect against various threats like DNS spoofing, cache poisoning, and DDoS attacks.	
	Monitor DNS traffic Utilize DNS monitoring tools to analyze DNS traffic for suspicious activities and potential signs of compromise.	
	Educate employees Provide training and awareness programs to educate employees about DNS security best practices and the risks associated with malicious DNS activities.	
	Regular updates and patching Ensure that DNS servers and associated software are regularly updated with the latest patches and security updates to address known vulnerabilities and maintain a strong defense posture against emerging threats.	
	Employ resilience measures Resilience measures such as redundant servers, rate limiting, and traffic filtering mitigating the impact of DNS-based Distributed Denial of Service (DDoS) attacks, ensuring uninterrupted online services and regulatory compliance.	

4. Backup strategy

A backup strategy and a disaster recovery plan together make up an organization's comprehensive business continuity plan, which serves as a guide for surviving a cyberattack and recovering from it with the least amount of harm to its operations, reputation, and data.

Here's why a backup strategy is crucial:



Data protection

A backup strategy involves regularly creating and securely storing data copies offsite or in the cloud, ensuring recovery from ransomware, hardware failures, or human errors.



Ransomware mitigation

A comprehensive backup strategy serves as a ransomware defense, enabling data restoration without paying ransoms.



Ransomware attacks on mid-market businesses increased dramatically by 151% in 2023 compared to the previous year, which is a cause for concern.

[Click here to read full article](#)



Business continuity

Backup strategies facilitate quick data recovery during unforeseen events, minimizing disruptions to operations and revenue.



Regulatory compliance

Backup strategies help meet regulatory requirements for data protection and retention, avoiding fines and penalties.



Customer trust and reputation

Demonstrating commitment to data protection enhances customer trust and business reputation, preserving goodwill and credibility.



Cost-effectiveness

While backup setup incurs initial costs, the long-term benefits surpass expenses, mitigating data loss and downtime costs.

Here's how to effectively implement a backup strategy:



Identify critical data

Determine which data is critical for business operations and prioritize it for backup to ensure continuity in case of data loss or system failure.



Choose backup solutions

Select reliable and cost-effective backup solutions tailored to the company's needs, considering factors like data volume, frequency of backups, and storage requirements.



Develop backup policies

Establish clear backup policies outlining the frequency of backups, retention periods, and procedures for data restoration to ensure consistency and compliance.



Test backup systems

Regularly test backup systems and procedures to verify data integrity, backup reliability, and the organization's ability to recover data in various scenarios.



Offsite storage and redundancy

Implement offsite storage solutions and redundancy measures to safeguard backups against physical disasters, cyber threats, and other risks, ensuring data availability and resilience.

5. Next-generation firewalls

When mid-market companies seek cybersecurity insurance coverage, many insurers now mandate the adoption of a **next-generation firewall (NGFW)** as a policy requirement.

NGFWs offer enhanced functionalities beyond traditional firewalls, including **application control**, **integrated intrusion prevention systems**, and **cloud-based threat intelligence**. A leading NGFW solution delivers **comprehensive network visibility and rapid threat detection capabilities**, essential for bolstering cybersecurity posture.

Why next-generation firewalls are important:



Enhanced threat detection

Next-generation firewalls (NGFWs) offer advanced capabilities like application awareness and cloud-delivered threat intelligence, improving detection of sophisticated cyber threats.



Application control

NGFWs enable granular control over application usage within the network, reducing the risk of unauthorized access and data breaches.



Integrated intrusion prevention

NGFWs include built-in intrusion prevention systems (IPS) to proactively block malicious activities and exploits, safeguarding network assets.



Regulatory compliance

Implementing NGFWs helps mid-market businesses meet cybersecurity regulatory requirements, ensuring compliance with industry standards and protecting sensitive data.

Here's how to effectively implement an NGFW:



Assess network requirements and security objectives to select an NGFW tailored to the organization's needs.



Configure NGFW policies based on business requirements, including application control, user identity management, and threat prevention.



Implement advanced security features such as Intrusion Prevention Systems (IPS), SSL decryption, and threat intelligence integration.



Regularly update NGFW firmware and security signatures to ensure protection against emerging threats and vulnerabilities.



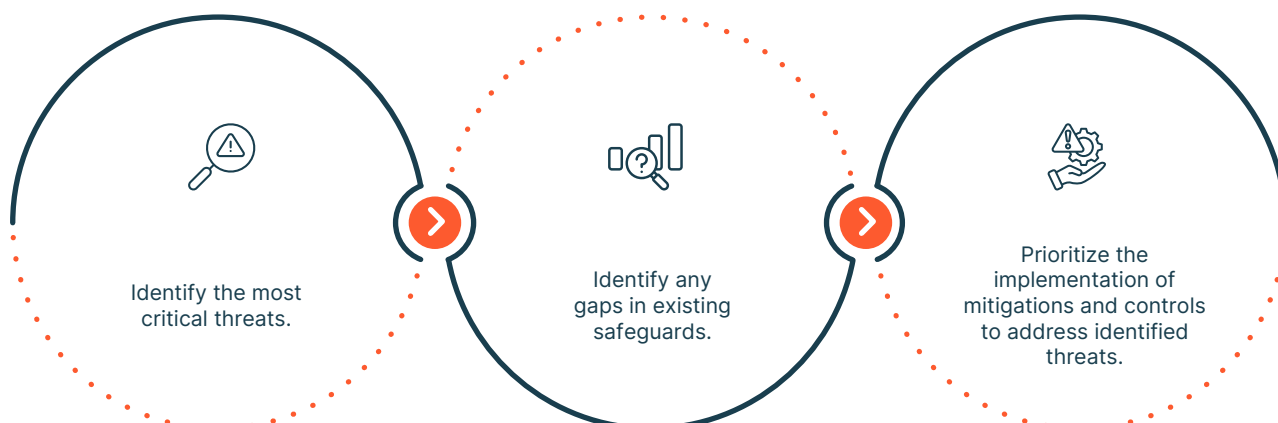
Continuously monitor NGFW logs and alerts to identify and respond to security incidents in real-time



6. Threat modeling

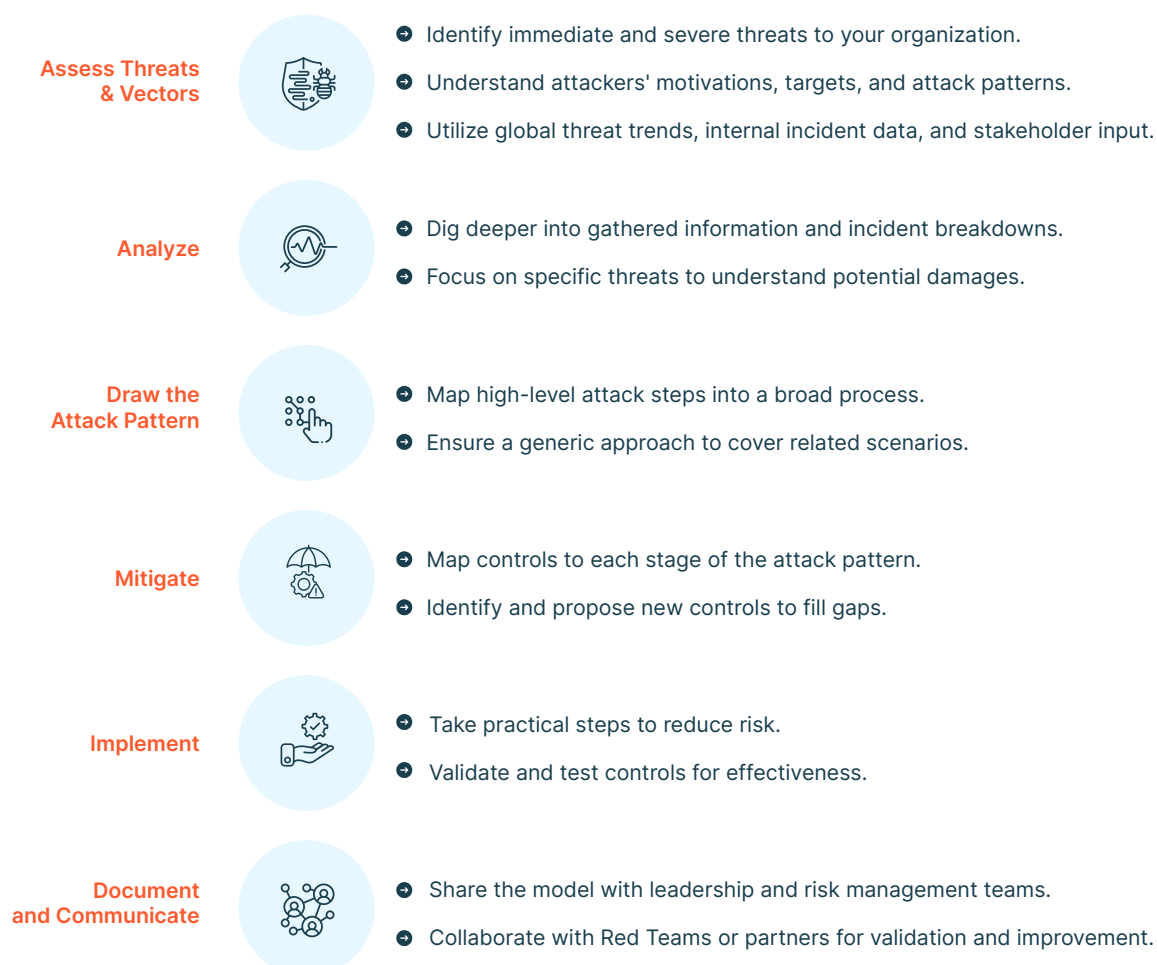
Threat Modeling offers a valuable approach to prioritizing controls against external security threats. Initially developed for military purposes to assess defensive strategies, this method is now widely employed to achieve the following objectives:

Threat modeling can help:



By adopting simple steps for basic threat modeling, businesses can prioritize risks and allocate resources efficiently to mitigate potential threats.

Simple steps for basic threat modelling:



Why is threat modeling crucial?



Proactive risk management

Threat modeling enables mid-market companies to identify and assess potential threats before they manifest, allowing for proactive risk mitigation.



Resource allocation

By prioritizing risks based on likelihood and impact, threat modeling helps allocate resources efficiently to address the most critical security vulnerabilities.



Tailored security measures

Threat modeling facilitates the development of tailored security measures specific to the organization's unique threat landscape, enhancing overall cybersecurity posture.



Cost-effective security

Implementing threat modeling minimizes the likelihood of costly security incidents by addressing vulnerabilities early in the development process, saving resources in the long run.



Compliance readiness

Incorporating threat modeling practices assists mid-market companies in meeting regulatory requirements by demonstrating a systematic approach to identifying and mitigating security risks.

Here's how mid-market companies can implement threat modeling effectively:

🕒 Identify potential threats

Consider both internal and external factors that may jeopardize data security and business continuity. Analyze potential threats such as hackers, malware, employee errors, and malicious insiders. Assess vulnerabilities in systems, processes, and assets, including outdated software, weak passwords, and lack of **cybersecurity awareness among employees**.

🕒 Assess risk

Utilize quantitative or heatmap-based analysis to prioritize risks based on probability and potential impact. Understand the susceptibility of systems, processes, and assets to various threats and their potential impact on the organization. Identify important assets, systems, services, and data that may cause severe losses and business disruptions if lost—not to forget your database servers and your network directory infrastructure (like Active Directory).

🕒 Understand and prioritize assets

Recognize tangible and digital assets like customer data, intellectual property, and financial records as critical components of threat assessment. Prioritize assets based on their importance to the organization's operations, revenue, reputation, and regulatory compliance.

✓ Allocate resources efficiently

Address high-priority risks first by allocating resources to implement preventive measures, controls, and mitigation strategies.

✓ Leverage existing tools and frameworks

Threat modeling frameworks, such as STRIDE, PASTA, and OCTAVE can be beneficial, but medium-sized enterprises may lack the resources for extensive threat modeling. Instead, they may extract key concepts from these frameworks, applying them to address specific issues, and refining their approach over time. Utilize tools like [Mozilla's Rapid Risk Assessment \(RRA\)](#) to establish a foundation for threat modeling.

✓ Continuous monitoring and review

Regularly monitor and review the threat landscape to stay updated on emerging risks and evolving threats. Update threat models and risk assessments regularly to adapt to changing circumstances.

✓ Develop and update response plans

Create response plans for significant risks, including preventive strategies like regular software updates and employee training. Establish response protocols for different types of security incidents to ensure timely and effective responses.



Although threat modeling can turn highly sophisticated, even a brief evaluation can pinpoint 20% of the issues responsible for 80% of your risk.

7. Partner with the right MSSP

Lean teams often lack adequate support, prompting them to seek third-party solutions. However, relying on multiple third-party tools can strain the budget significantly, imposing financial constraints on the organization. This restraint may hinder investments in essential areas like talent acquisition, training, and technology upgrades.

So it is only right that SMEs prioritize investing in cybersecurity measures **tailored to their size and industry**, encompassing both technological defenses and comprehensive staff training to enhance threat awareness and prevention efforts.

Partnering with the appropriate Managed Security Service Provider (MSSP) is ideal; however, medium-sized enterprises must take care to select an MSSP that offers comprehensive services within the budgetary framework.



Partnering with an MSSP (Managed Security Service Provider) provides mid-market businesses with expert guidance and resources to navigate cybersecurity challenges.



MSSPs offer specialized knowledge and 24/7 monitoring, enhancing proactive threat detection and rapid incident response, which is particularly valuable for companies with limited internal resources.



MSSPs deliver scalable solutions customized to the unique needs and budget limitations of mid-market businesses, granting access to advanced security technologies and strategies that may otherwise be inaccessible.

By entrusting their cybersecurity needs to the right MSSP, mid-market companies can focus on their core operations with peace of mind, knowing that their digital assets are in capable hands.

Scrut's tailored solutions for your needs

For mid-market companies and lean teams seeking comprehensive security solutions and struggling with GRC processes, Scrut's smartGRC™ platform offers a tailored solution. With its suite of tools and features designed to support governance, risk management, and compliance efforts, smartGRC™ empowers organizations to navigate the complexities of cybersecurity with confidence.

As you embark on your journey to strengthen your organization's security posture, [we invite you to explore the possibilities with Scrut's smartGRC™ platform](#). Together, we can safeguard your business against emerging threats and build a resilient security foundation for the future.