PROSERVEIT

5 Strategies To Fortify Your Security Posture

October 2024

Table of Contents

Executive Summary

In today's digital landscape, the rise of sophisticated cyber threats has made it crucial for organizations to strengthen their overall security posture. Cyberattacks have become more frequent, more complex, and more costly.

According to recent studies, the average cost of a data breach in 2023 reached $4.88 million, with businesses of all sizes being vulnerable to attacks. Small and medium-sized enterprises (SMEs) are particularly at risk, with 43% of all cyberattacks targeting them. Despite these alarming statistics, only 14% of SMEs are adequately prepared to defend against these threats.

This whitepaper provides an in-depth exploration of the key pillars of cybersecurity for organizations to focus on to mitigate these growing risks. It highlights five critical areas of protection.

1. Identity Protection
Implement multi-factor authentication (MFA) and Zero Trust models to reduce identity theft risks.

2 . Application Security
Regularly update software and integrate security during development to address vulnerabilities.

3. Data Security
Utilize encryption, Data Loss Prevention (DLP), and role-based access control (RBAC) to protect sensitive data from ransomware attacks.

4. Inbox Protection
Combat phishing, the most common attack vector, through advanced email filtering, user training, and incident response plans.

5. Endpoint Security
Protect remote work devices with specialized security apps and implement Zero Trust models for ongoing monitoring.

By 2025, cybercrime damages could cost $10.5 trillion annually.

To maintain an effective overall security posture, organizations should assess their systems, protect sensitive data through comprehensive security measures, and continuously monitor activities. By adopting a multi-layered security approach that addresses these five key areas, organizations can significantly reduce the risk of a successful cyberattack and protect their critical assets in an increasingly hostile digital environment.

1 Protect Your Identity

Identity protection is a cornerstone of cybersecurity, as compromised identities can lead to severe repercussions for both individuals and organizations.

Key Elements of Identification Risks

Identifying risks is a critical step in maintaining a strong security posture. By understanding and addressing vulnerabilities in systems, applications, and user behavior, organizations can better protect themselves against potential threats and reduce their exposure to cyberattacks.

Weak or Reused Passwords

Passwords serve as the primary defense for identity protection, but weak or reused passwords create security vulnerabilities. Cybercriminals exploit these weaknesses through brute force attacks, credential stuffing, and phishing.

Lack of Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is crucial for preventing unauthorized account access. It enhances security by requiring a second verification method, such as a mobile device or biometrics, in addition to a password. Without MFA, compromised credentials can easily lead to infiltration of sensitive systems, making it easier for cybercriminals to steal identities and compromise accounts, especially during large-scale breaches.

Unsecured Networks

Using unsecured public Wi-Fi exposes users to identity theft risks, as cybercriminals can intercept data through man-in-the-middle attacks. Remote employees accessing corporate resources on these networks heighten the risk of exposing sensitive information.

Mismanagement of Permissions

Poorly managed access controls pose serious risks to personal and corporate identities. Excessive permissions for employees, contractors, or partners can lead to insider threats and unintended data exposure, while attackers may exploit these permissions to access critical systems and sensitive data.

Over 90%

of data breaches stem from human error, highlighting the necessity of ongoing training and awareness initiatives.
(Source: ICO)

Strategies for Identity Protection

Multifactor Authentication (MFA)

Multi-Factor Authentication (MFA) is essential for securing both corporate and personal accounts, requiring two or more verification methods for enhanced protection. These methods include **something you know** (like a password or PIN), **something you have** (such as a mobile device or security token), and **something you are** (like biometric data). MFA effectively **blocks 99.9% of identity attacks** by necessitating additional verification even if a password is compromised.

Use a Password Manager and Strong Passphrases

A password manager is essential for protecting your digital identities by creating, storing, and managing complex, unique passwords for every service. This prevents attackers from accessing multiple accounts if one password is compromised. Additionally, create **strong passphrases** instead of passwords. Combine four unrelated words, like "WhiteWallBigScreen," and aim for 12-16 characters. Avoid using personal information and never reuse passphrases across different sites.

Be Cautious with Permissions and Public Wi-Fi

Always read the permissions you grant when signing up for new apps or services. Review permissions carefully, especially with corporate accounts, to prevent unauthorized access.

Avoid using public Wi-Fi networks in places like airports, hotels, and cafes, as they pose significant security risks. If you must use public Wi-Fi, use a virtual private network or VPN, preferably a paid version to protect your data.

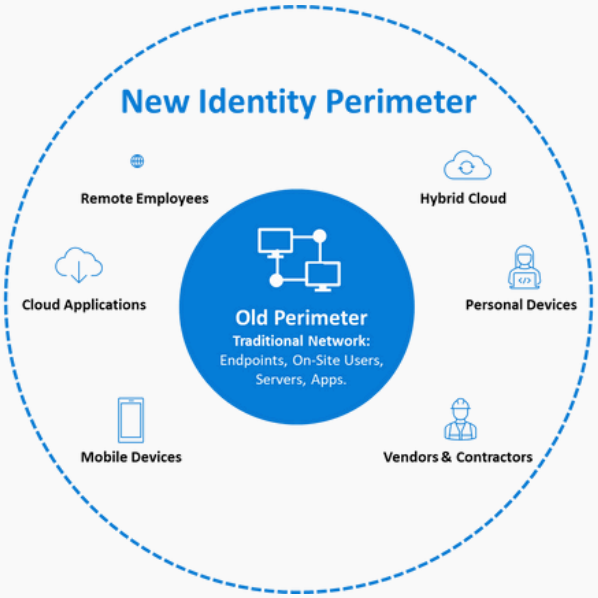
Implement Access Policies

Use Single Sign-On (SSO) platforms for business apps to reduce the risk of weak or stolen credentials. Policies like conditional access can restrict access based on location and device, enhancing security. Implement location-based access policies to block access from countries where you don't conduct business.

81% **of breaches are caused by weak or reused passwords.**
(Source: Verizon, 2023)

Best Practices for Identity Protection:

- **Regularly audit** accounts and access rights to ensure only the right users have access to critical data.
- Implement **strong password** policies that discourage reuse and weak passwords.
- Use **password-less authentication** methods like biometric scans to enhance security.



As organizations shift to hybrid cloud and remote work, security has transitioned from perimeter defenses to prioritizing digital identities.

With employees accessing resources from multiple locations and devices, robust identity management is essential for controlling access to sensitive information, serving as the primary defense against cyber threats.

2 Protect Your Applications

Applications are often targeted by cybercriminals to exploit vulnerabilities. Securing applications is essential to maintaining organizational integrity.

Key Elements of Identification Risks

Shadow IT

Users often employ unapproved applications, known as Shadow IT, making it difficult for organizations to protect against unknown threats.

User Consent

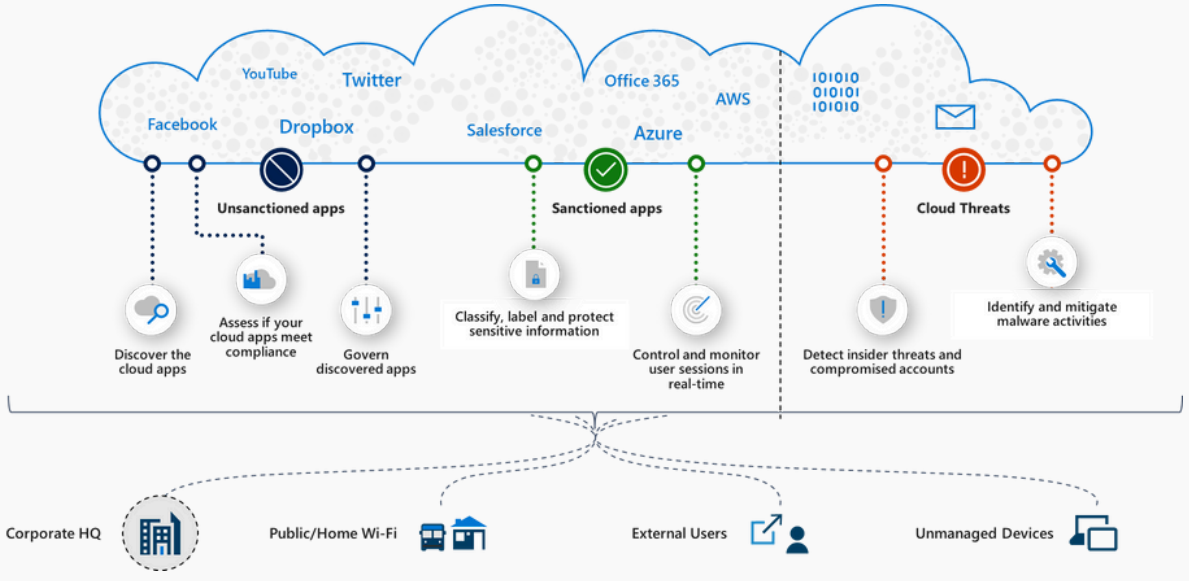
Users frequently grant permissions to applications without understanding the implications, risking exposure of personal and corporate information.

Threat Detection Risks

Identifying malware and suspicious activities in cloud apps is challenging without proper monitoring tools.

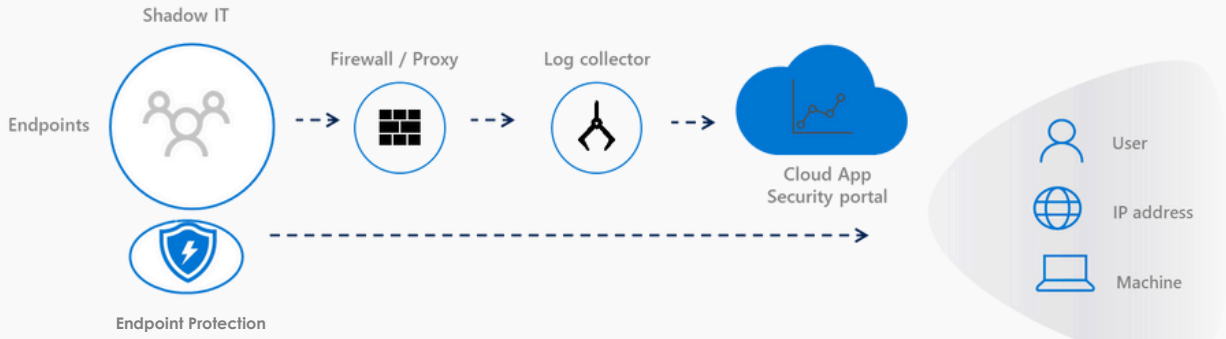
Sensitive Data Exposure

Sensitive data may be exposed to risks if users access your data and applications from non-secure devices or from public networks.



In today's world, users often choose various SaaS applications without considering security, complicating organizations' monitoring and controlling access.

Cloud App Discovery Architecture



To identify cloud app usage, organizations can use two main methods:

1.Capture Office Network Traffic: Configure firewalls to log all network traffic and analyze them to identify and manage applications accessed from within the corporate network.

2. Use Endpoint protection tool: Monitor traffic from any location, including remote work and public Wi-Fi, using an endpoint protection tool. This ensures comprehensive visibility and security for cloud app usage, regardless of user location.

Strategies for Application Security

Managing User Consent

To protect applications, organizations should restrict users from being able to consent to unmanaged apps, allowing only admin approval. Many apps request extensive permissions that users may not fully understand. Organizations can manage user consent by allowing default consent, requiring admin approval, or disabling user consent altogether.

Conditional Access App Control

Secure applications by enforcing location and device-based policies, blocking sign-ins from outside specified areas, like national boundaries. Create and enforce policies to restrict document downloads on unmanaged devices, ensuring only secure, compliant access.

Monitoring and Governance

Use specialized security apps to track risky behaviors, such as clicking on unsecured links and unauthorized file sharing. When alerts are triggered, automatic governance actions, like removing external users or setting expiration dates on shared links, can enhance security.

Best Practices for Application Security

- Implement a **development security operations** model to integrate security in all stages of application development.
- Use **automated tools** for continuous application monitoring to detect and respond to potential threats.
- Ensure **third-party applications** and plugins are regularly assessed for vulnerabilities.

74% **of organizations report being moderately to extremely vulnerable to insider threats, often due to unpatched applications.**
(Source: Secureframe)

3 Protect Your Data

Data protection is crucial as it often contains sensitive information that can be exploited if compromised.

Challenges with Data Security

Data security presents ongoing challenges as organizations deal with increasing volumes of sensitive information. Protecting this data from breaches, unauthorized access, and misuse requires robust strategies that address both internal and external threats.

Mobile Workforce and Data Growth

With the increase of mobile workforces, safeguarding information has become more complex. Data volume is growing by 50% annually, requiring organizations to protect sensitive data like employee details, customer credit card information, intellectual property, and personal identifiable information. Identifying and securing this data is essential.

Cloud Storage Risks

While storing sensitive information in the cloud is not inherently risky, failing to protect it is. Over 6 billion records were exposed last year due to unprotected data, with an average of six months between infiltration and detection. Organizations often remain unaware of data breaches until significant damage has occurred.

Accidental Data Exposure

Users frequently send sensitive information to the wrong recipients by mistake. A Microsoft survey found that 58% of users have done this. Such errors can lead to identity theft and fraud, as sensitive data like Social Insurance Numbers can be misused. Even non-malicious mistakes can have severe consequences.

Backup and Disaster Recovery

Backups are essential due to increasing cybercrime, but they are not enough on their own. Organizations must implement a solid disaster recovery plan to maintain business continuity. Regular testing of this plan, including full IT system shutdowns, is crucial for meeting business needs and ensuring rapid recovery after incidents.

71% **of ransomware attacks target sensitive data.**
(Source: Sophos, 2023)

Strategies for Data Security

Organizations need to implement robust data security strategies to protect sensitive information. These strategies integrate technology, policies, and employee training, forming a comprehensive defense against unauthorized access and data breaches. This section highlights essential strategies that can enhance organizational security and resilience against evolving threats.

Data Loss Prevention

Utilize DLP solutions to monitor and control data transfers across the network. These tools help identify potential data breaches by preventing unauthorized sharing or transmission of sensitive information.

Data Encryption

Protect sensitive information by encrypting it both at rest and in transit. This ensures that even if data is intercepted or accessed without authorization, it remains unreadable without the proper decryption keys.

Regular Audits and Compliance Checks

Conduct frequent security audits and compliance assessments to identify vulnerabilities and ensure adherence to relevant regulations and industry standards.

User Training and Awareness Programs

Educate employees about data security best practices and the importance of safeguarding sensitive information. Regular training can help reduce the likelihood of human error, which is often a significant factor in data breaches.

Conditional Access & App Control

Establish strict access controls to limit who can view or manipulate sensitive data. Implementing role-based access ensures that employees have the minimum level of access required to perform their job functions.

16 days

is the average downtime due to ransomware, leading to significant operational and financial losses.
(Source: Coveware, 2023)

Best Practices for Data Security

- Regularly **audit permissions** to ensure data is accessible only by authorized personnel.
- Conduct regular **backups of critical data** and store backups in secure, offsite locations.
- Implement **endpoint encryption** for devices handling sensitive data.

4 Protect Your Inbox

Phishing attacks continue to be one of the most common methods used by cybercriminals to gain access to sensitive information.

Phishing attacks are a common and dangerous form of cybercrime that exploit human error. Recognizing the key signs of these attacks is crucial for protecting sensitive information and preventing unauthorized access to systems.

Key Signs of Phishing Attacks

Urgent Action

Be wary of emails that urge immediate action, like clicking links or opening attachments. These messages often create a false sense of urgency, typical of phishing attacks, to discourage critical thinking or seeking advice.

Suspicious Senders and Domains

Emails from unfamiliar senders or those marked [External], especially with strange email domains, can be phishing attempts.

Errors and Generic Greetings

Poor grammar or generic openings like "Dear Customer" are red flags, as professional organizations avoid such mistakes.

Fake Orders

Fake order scams exploit people's excitement over purchases by sending fraudulent emails that look like legitimate order confirmations or invoices. These messages encourage recipients to click links or open attachments to review order details, often leading to phishing sites aimed at stealing personal and financial information.

Suspicious Link or Attachments

If you suspect an email might be a phishing attempt, do not click on any links or open attachments. Instead, hover your mouse over the link (without clicking) to reveal the real web address. If the link looks unfamiliar or doesn't match what was typed in the message, it's probably a scam.

76% **of businesses have experienced phishing attacks, making it the most common type of cyberattack.**
(Source: Verizon, 2023)

Phishing attacks are increasing, with **96% delivered via email.** It's crucial to remain calm and know how to respond to suspicious emails. Important steps exist to protect personal information, whether you identify the email as phishing beforehand or afterward. Here's how to handle phishing emails before and after opening them.

Actions to take Before You Open a Phishing Email

Do not click on any links or open attachments

Hover over any links without clicking to reveal the web address. This can help you identify whether the link leads to a malicious site before you risk interacting with it.

Do not respond or provide personal information

Even if the email looks legitimate, avoid responding or sharing sensitive details like passwords or financial information. Cybercriminals often create emails designed to provoke an urgent response.

Report the email as phishing

Most email providers allow users to report suspicious emails. Reporting helps strengthen spam filters and reduces the chances of similar attacks targeting others.

Actions to take After You Open a Phishing Email

Avoid clicking on any links or attachments

If you accidentally open a phishing email, resist clicking on any links. Instead, go directly to the company's official website by typing the URL in your browser or using a saved bookmark.

Contact the organization through official channels

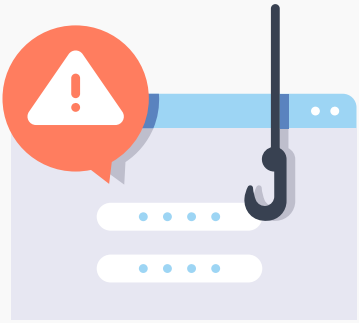
If you think the email might be legitimate, contact the organization using verified phone numbers or emails from their official website, not the contact information provided in the email.

Verify if the sender is someone you know

If the suspicious email comes from someone in your contact list, contact that person through another communication method to verify its authenticity.

Delete the email

Once you've ensured that the email is a phishing attempt, delete it immediately to avoid accidentally interacting with it later.



Actions to Take When You Have Been Phished!

Document the Details

While it's fresh, **write down all details** you remember sharing, including usernames, account numbers, passwords, and the platform of the attack.

Change Passwords

Change passwords on affected accounts and any using the same password. Use unique, strong passwords for each account and consider a password manager for secure storage.

Enable MFA

Turn on **MFA (multi-factor authentication or two-step verification)** for all your accounts. This adds an extra layer of security.

Notify Relevant Parties

If the attack involves your work or school accounts, inform your IT support team.

Report to Authorities

If you've lost money or been a victim of identity theft, report the incident to local law enforcement.

Best Practices for Inbox Protection

- Encourage employees to report suspicious emails and provide an easy reporting system.
- Implement robust spam filters to prevent phishing emails from entering the inbox.
- Regularly update employees on the latest phishing tactics.

22% **of all breaches involve phishing, and phishing-related attacks cost businesses an average of $1.5 million per incident.**
(Source: Proofpoint, 2023)

5 Protect Your Endpoints

Endpoints, devices that connect to and exchange information with your network including laptops, mobile devices, and desktops, represent potential entry points for cyberattacks.

Challenges with Data Security

Data security is a critical concern for organizations, especially as the volume of sensitive information being handled increases. Protecting data from breaches, leaks, and unauthorized access presents ongoing challenges that require robust strategies and solutions. This section explores the common challenges organizations face in maintaining data security.

Ransomware

Encrypts data until a ransom is paid, potentially crippling operations and causing financial loss.

Malvertising / Adware

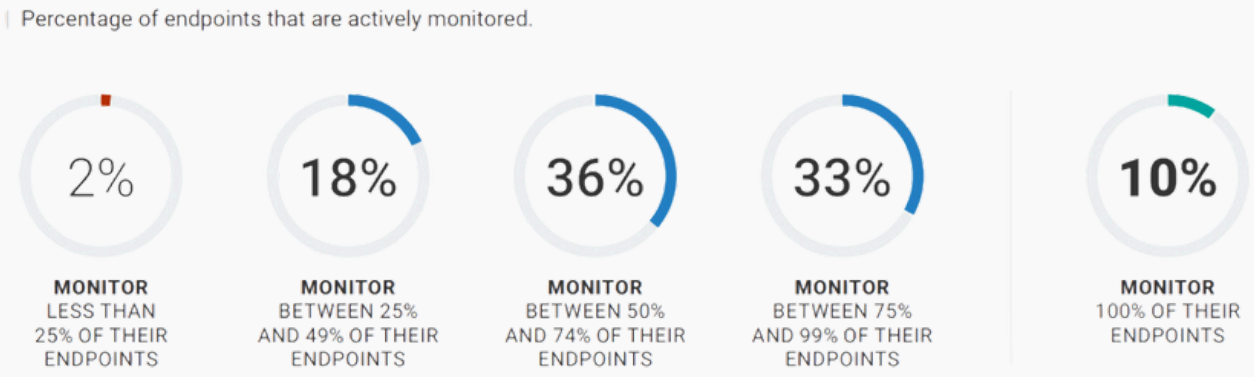
Malicious ads redirect users to scam sites or deploy harmful malware, compromising user data.

Advanced Persistent Threats

Groups gain long-term network access, conducting reconnaissance and stealing data over extended periods.

Data Loss and Theft

Involves stealing critical data such as financial information, client data, and intellectual property, causing significant damage.



A survey by TechTarget's ESG found that **only 10% of organizations monitor all their endpoints**, leading to over 70% experiencing cyberattacks due to unmanaged devices, with those having more than 20% unmanaged devices being nearly 11 times more likely to suffer multiple attacks.

Key Points to Consider for Your Endpoint Protection

Protecting your organization's endpoints is essential for maintaining overall security. By implementing key strategies and practices, you can significantly reduce vulnerabilities and safeguard your network from potential threats. Here are key points to consider for effective endpoint protection.

Legacy vs. Modern Solutions

Evaluate if you're relying on traditional antivirus (AV) or utilizing modern endpoint protection with response capabilities. Legacy AV may stop at signature-based detection, while sophisticated endpoint protection offers real-time monitoring and response to advanced threats.

Coverage Across Endpoints

Ensure that all endpoints—both corporate and remote devices—are protected. Unprotected endpoints create significant vulnerabilities in your security framework.

Cost vs. Value

While modern solutions may seem more expensive upfront, their ability to prevent costly security breaches can offer long-term savings and reduce overall risks.

Proactive Threat Detection

Modern endpoint detection and response (EDR) solutions provide advanced threat intelligence and proactive detection beyond known malware, helping to secure endpoints from zero-day vulnerabilities and emerging threats.

Key Strategies for Endpoint Protection

In the digital age, protecting endpoints is crucial for network security due to the rise of remote work and mobile devices. Key strategies involve securing all devices, applications, and user access points to mitigate risks and defend against cybercriminal activity.

Endpoint Detection and Response

Endpoint Detection and Response (EDR) solutions are critical for real-time monitoring and defense, enabling organizations to detect and mitigate threats as soon as they emerge. These solutions use advanced algorithms to analyze activity on devices, helping identify suspicious behaviors and respond quickly to mitigate risk.

Mobile Device Management

Mobile Device Management (MDM) is essential in securing the growing number of mobile endpoints in today's remote work environment. By enforcing security protocols across all devices, MDM ensures that only authorized and secure devices can access corporate data, safeguarding against data breaches on personal and company-owned devices.

Zero Trust Security Model

The Zero Trust Security Model is a modern approach that requires continuous verification of users and devices before granting access to resources. It operates on the principle of "never trust, always verify," significantly reducing the chances of unauthorized access and protecting sensitive organizational data from internal and external threats.

Encryption of Endpoint Data

Data encryption is a foundational security measure that ensures information is protected, whether stored locally on devices or transmitted across networks. Encrypting endpoint data minimizes the risk of exposure, ensuring that sensitive information remains secure even in the event of a breach or device theft.

Strict BYOD (Bring Your Own Device) Policies

Bring Your Own Device (BYOD) policies are essential for managing the security risks associated with personal devices accessing corporate networks. A well-defined policy helps ensure that only secure, compliant devices are granted access to sensitive data, reducing the risk of breaches.

Continuous Monitoring and Incident Response

Bring Your Own Device (BYOD) policies are essential for managing the security risks associated with personal devices accessing corporate networks. A well-defined policy helps ensure that only secure, compliant devices are granted access to sensitive data, reducing the risk of breaches.

Fortify Your Security Posture

An organization's security posture refers to its ability to assess, protect, and monitor implemented security measures.

3-Step Approach to Simplifying Security

A 3-Step Approach to Simplifying Security involves these phases: Assess, Protect, and Monitor. This method helps organizations manage modern security challenges, prioritize efforts, and maintain vigilance over their digital infrastructure.

1 Assess

The first step is identifying vulnerabilities, weaknesses, and risks in your environment. A thorough assessment allows you to map out potential entry points, misconfigurations, and areas lacking proper defense mechanisms. This stage involves not only identifying existing risks but also anticipating future ones, ensuring that your security strategy is dynamic and forward-thinking.

Key elements of assessment include:

- Vulnerability scanning and risk assessments.
- Identifying high-priority assets and sensitive data.
- Understanding regulatory compliance requirements relevant to your industry.

ProServeIT offers a free threat landscape review that visualizes global login attempts to your environment, highlighting successful (🟡 yellow dots) and unsuccessful (🔴 red dots) attempts. The detailed report includes a dark web scan, privileged role exposure, and secure score. This service helps identify ongoing attacks, their locations, and necessary actions to take.

Password attacks in cyberspace have surged 20-fold in three years, with cybercrime now being the world's third-largest economy, growing at 15% annually. ProServeIT aims to empower organizations by implementing essential security measures to protect against these risks.

2 Protect

Once the assessment is complete, it's crucial to implement strategies and tools that provide robust defense mechanisms for your digital estate. Protecting involves both preventive measures and active threat mitigation techniques to ensure security layers are in place to prevent unauthorized access, data breaches, and malware attacks.

Key protection strategies include:

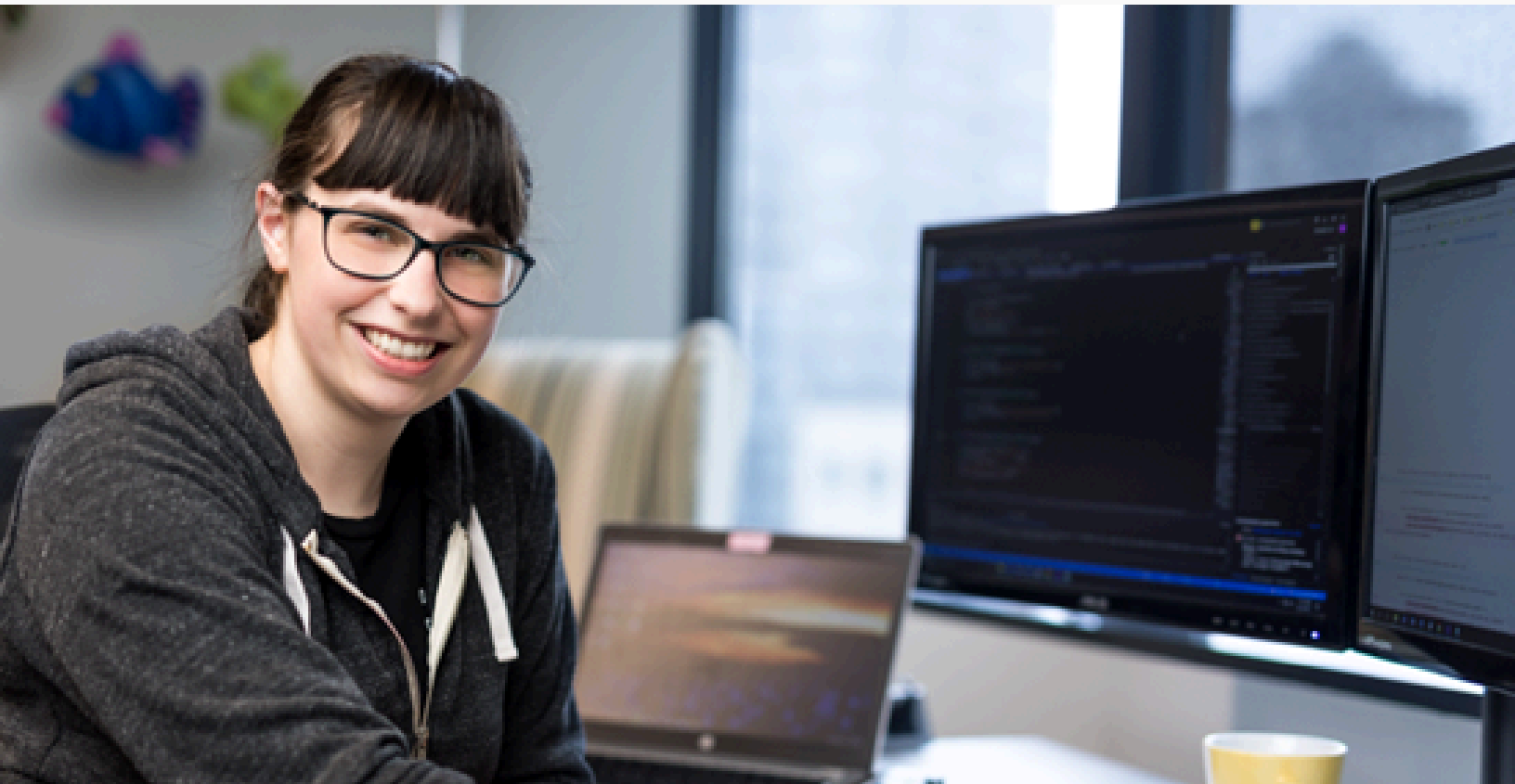
- Establishing strong access controls and identity management.
- Securing endpoints and devices through encryption, patching, and regular updates.
- Implementing network security tools such as firewalls and intrusion prevention systems.
- Ensuring data security through encryption and secure storage practices.

3 Monitor

Continuous monitoring ensures that your security measures are working effectively and that any potential threats are identified and addressed promptly. This involves real-time detection of suspicious activities, detailed analytics, and the ability to respond to incidents quickly. Monitoring allows for proactive security management and the ability to detect evolving threats before they can cause significant damage.

Key monitoring strategies include:

- Real-time monitoring of network traffic and endpoint activity.
- Implementing automated alerts and incident response workflows.
- Using analytics to spot patterns of suspicious behavior or anomalies.
- Leveraging threat intelligence to stay updated on emerging security risks.



Conclusion

Securing your organization's digital assets requires a disciplined, layered defense. From protecting identities and applications to safeguarding data, inboxes, and endpoints, each component strengthens your overall security posture.

Identity protection ensures credential safety, while application security defends vital platforms. Data security demands robust encryption and vigilant monitoring to prevent breaches, and email security protects against phishing and social engineering, often the entry point for larger attacks.

Endpoint security enforces policies across all devices, maintaining strict standards. The strategy outlined—covering identity, applications, data, inboxes, endpoints, and overall security—provides a comprehensive roadmap for building a proactive, adaptable defense against evolving cyber threats.

At ProServeIT, we provide comprehensive managed cybersecurity services designed to protect your organization from ever-evolving threats. Engage with us to leverage our expertise in managed cybersecurity services, helping your business stay secure, resilient, and prepared for today's complex threat landscape.

Contact ProServeIT

Get started with ProServeIT today - contact us to get complimentary landscape review and learn how we can enhance your security posture with our expertise.

Get Started

PROSERVEIT

About ProServeIT

ProServeIT is a distinguished Microsoft Cloud Solutions Partner, with over twenty years of experience in digital transformation and IT services. With a strong emphasis on cybersecurity, ProServeIT empowers organizations to enhance their digital security through advanced cloud migration and managed IT services.

As a Certified B Corporation, ProServeIT commits to leveraging technology as a powerful catalyst for positive change. ProServeIT employs a strategic, security-first approach that strengthens defenses against continuously evolving threats. This empowers businesses to enhance operational efficiency while effectively managing IT risks.

For more information, visit www.proserveit.com
Email us at cloud@proserveit.com

Member of
Microsoft Intelligent Security Association

Microsoft Security

Microsoft Solutions Partner
Security

Specialist
Cloud Security
Identity and Access Management
Threat Protection