ACCESS DENIED:

HOW TO STOP CYBER THREAT ACTORS AT THE DOOR

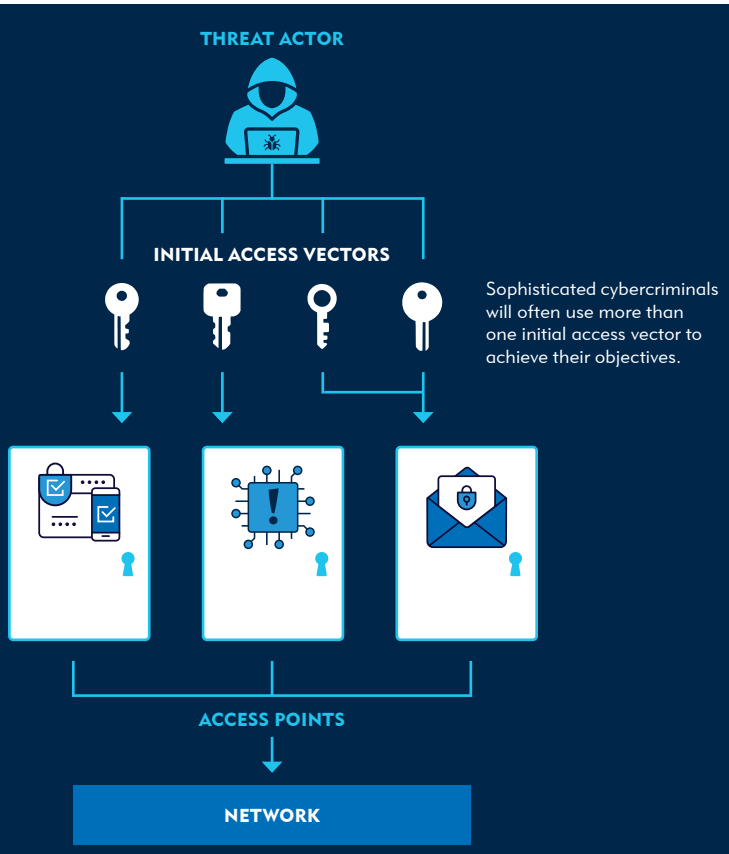
Securing the Front Line Against Initial Access

Every cyber breach has a beginning, and it often starts with a single click. Cybersecurity threats continue to evolve in complexity and scale, with attackers increasingly targeting the weakest links in organizational defenses to gain initial access. These methods of entry, known as initial access vectors, are the means by which threat actors infiltrate networks, systems and data environments.

Understanding initial access vectors is not just a technical necessity, but it's also crucial to building a strong cybersecurity foundation. According to CrowdStrike's 2025 Global Threat Report, "attacks related to initial access boomed, accounting for 52% of vulnerabilities… in 2024." These vulnerabilities are both common and preventable, yet their exploitation may lead to data loss, operational disruption, reputational damage and significant financial costs. Critically, they also are responsible for a significant portion of cyber insurance claims, and thus play a role in underwriting decisions.

By proactively identifying and addressing weaknesses in the access points that are commonly targeted in initial access-related attacks, organizations may not only reduce the likelihood of successful attacks, they may also position themselves for more favorable insurance coverage and fewer claims. For organizations seeking to build a cyber protocol that meets the moment, this is where a successful strategy begins.

WHAT ARE INITIAL ACCESS VECTORS?



Examples of Initial Access Vectors:

- Phishing, or using deceptive emails
- Public-facing applications such as VPNs
- Valid accounts
- Drive-by downloads from malicious websites
- Malicious scripts embedded in digital documents
- Remote access services
- Software vulnerabilities

Understanding initial access vectors is the first step to stopping cybercriminals in their tracks. Initial access vectors are the methods threat actors use to infiltrate an organization's network, steal data or deploy malware. Sophisticated cybercriminals will often use more than one of these modalities to achieve their objectives in any given attack. While initial access vectors are commonly used in targeted attacks seeking to penetrate a digital system, they are not necessarily needed in attacks that rely on external disruption or deception, such as social engineering scams.

Once threat actors successfully gain initial access, they will attempt to "break out," or move laterally within the system to access high-value information or assets. The more quickly an attacker can break out, the faster they can cause significant damage. Notably, breakout times are getting faster. In 2024, "the average breakout time for interactive eCrime intrusions fell to 48 minutes, down from 62 minutes in 2023" according to CrowdStrike.

With cybercriminals' growing efficiency in exploiting initial access vectors, it's no surprise that selling access to these methodologies has grown into a booming business on the dark web. Increasingly, threat actors are gaining access to an organization's network, and then selling that access to other cybercriminals. CrowdStrike reported that, in 2024, "advertised accesses [increased] by nearly 50% over 2023," further underscoring the necessity for organizations to reexamine their initial access defense strategies.

Common access points in initial access vector attacks include remote access systems lacking properly maintained multifactor authentication (MFA), unpatched software vulnerabilities and email security vulnerabilities. While these attack methods are not new, they are evolving rapidly in sophistication and scale, making them a critical focus for cyber teams seeking to implement up-to-date security controls and process improvements.

ACCESS POINT: IMPROPERLY MAINTAINED MULTIFACTOR AUTHENTICATION

Remote access tools such as virtual private networks (VPNs) and other external gateways such as cloud networks and remote monitoring and management tools (RMM) are common targets for cyber attackers.

When multifactor authentication (MFA) is not properly enforced, these tools become vulnerable to credential-based attacks as threat actors can easily exploit stolen or leaked usernames and passwords to gain access to internal systems. According to a paper by Osterman Research "almost all organizations don't protect every employee and every app with MFA (94.2%), which immediately opens exposure pathways for threat actors to infiltrate…"

Implementing MFA across all remote access points, especially for remote access and email, and regularly auditing its configuration is essential to reducing exposure and strengthening defenses.

> Almost all organizations don't protect every employee and every app with MFA (94.2%), which immediately opens exposure pathways for threat actors to infiltrate…

CASE STUDY:

The Cost of MFA Without Safeguards

In 2021, a nonprofit organization experienced a major cyber breach due to critical gaps in its multi-factor authentication (MFA) infrastructure. These gaps existed primarily due to a lack of auditing and oversight in identity management processes. The attackers gained access through an active account no longer associated with a current user and were able to register their own MFA device without triggering any verification checks. The MFA enrollment process lacked safeguards such as identity revalidation, session integrity checks or administrative approval, allowing unauthorized users to complete MFA setup as if they were legitimate account holders. This failure to audit and secure the enrollment workflow enabled attackers to bypass authentication controls and gain full access to the organization's internal network. The incident highlights that simply having MFA isn't enough to protect from threat actors—as their attacks grow in complexity, so too must organizations' defense strategies. Furthermore, it underscores the importance of enforcing strict verification protocols during MFA enrollment and regularly auditing account activity to prevent unauthorized access.

Auditing MFA systems is particularly challenging for many organizations due to the sheer number of access points that need attention. However, there are tactics that can be implemented to reduce the time and effort needed to manage this critical area of cybersecurity:

TACTIC 1: Enforce

Enforce conditional access policies with an identity management system that requires MFA for all users accessing the network remotely. This is an effective strategy for preventing threat actors from taking advantage of weak or inconsistent MFA implementation. It will also help to ensure that MFA requirements are applied to all employees included in the conditional access policy.

TACTIC 2: Audit

Frequently export users and their authentication methods of various remote access tools to identify any users who are exempt or not registered. As a part of this process, it is also recommended that organizations audit their conditional access policies to identify where exemptions are applied and where users have not registered for MFA and ensure monitoring and follow up with these edge cases to limit exposure.

TACTIC 3: Alert

Create alerts for suspicious or unexpected modifications to your MFA and conditional access policies and have a playbook detailing response protocol in the event of one of these alerts. Playbooks should include information on what steps need to be taken to respond to an alert, who is responsible for carrying out the response and the areas within the organization's cyber infrastructure that require particular attention from respondents.

TACTIC 4: Partner

Partner with vendors who specialize in identity monitoring. Ideally, your cyber insurer will have partnerships with vendors who provide this service as a part of your organization's policy. For example, organizations may partner with an identity vendor that specializes in monitoring identity access and applying adaptive MFA for suspicious activity.

ACCESS POINT: UNPATCHED SOFTWARE VULNERABILITIES

Unpatched software vulnerabilities are a common point of entry for threat actors, especially when patches are delayed. These vulnerabilities are typically flaws in a software application or system that allow cybercriminals to more easily break in to organizations' networks, and they often affect internet-facing services such as VPNs and third-party software. When a new software vulnerability is publicly disclosed, it can pose a serious risk to organizations, especially if a demonstration or proof-of-concept shows how the flaw can be exploited. These public examples make it easier for attackers to replicate the exploit, increasing the likelihood of cyberattacks if the vulnerability isn't patched quickly. According to IBM, "30% of the incidents… in 2024 involved the exploitation of public-facing applications. For many organizations, this is magnified by vulnerability patch management challenges."

Once an attacker gains entry via this access point, they will typically use the following strategies:

Remote Code Execution (RCE): This type of attack allows cyber criminals to execute arbitrary code on a system from a remote location. When criminals execute these codes, they can gain access to a device and run commands, install software or steal data.

Authentication Bypass: This type of attack enables attackers to circumvent login credentials and MFA entirely, allowing them to easily access an organization's internal systems.

CASE STUDY:

Unpatched and Exposed

In 2024, a U.S. Federal Civilian Executive Branch (FCEB) agency experienced a break-in stemming from a critical RCE vulnerability in GeoServer, an open source information platform. This vulnerability was present in GeoServer's default installation, which had not been patched. According to CISA, "vulnerabilities were not promptly remediated, the agency did not test or exercise their incident response plan (IRP), and EDR alerts were not continuously reviewed." The impact included unauthorized control over core infrastructure and the potential for data exfiltration and lateral movement.

CASE STUDY:

Lessons in Securing Automation and Access Control

Multiple organizations were impacted by an unpatched vulnerability affecting Cleo Managed File Transfer. The breach involved a critical authentication bypass vulnerability that allowed attackers to gain unauthorized access to sensitive files without valid credentials. Exploiting a misconfigured autorun directory, threat actors uploaded malicious files that executed automatically, effectively bypassing login requirements and triggering RCE. The incident highlights the importance of securing automation features and ensuring authentication controls are enforced consistently across all access points.

Timely identification and remediation of vulnerabilities are critical to maintaining a secure network perimeter. Attackers are becoming quicker at developing exploits for publicly disclosed vulnerabilities.

The IBM X-Force 2025 Threat Intelligence Index identified the top 10 common vulnerabilities being discussed on dark web forums. They found that, of those 10, 60% had publicly available exploits less than two weeks after their discovery and disclosure. For organizations seeking to strengthen their cybersecurity posture, rapid vulnerability patching is as crucial as ever.

For high-risk vulnerabilities such as those that could enable authentication bypass or remote code execution on internet-facing assets, organizations should aim to implement vendor-recommended patches as soon as feasible and ideally within 72 hours. To support this level of responsiveness, organizations are encouraged to establish internal processes that promote continuous vulnerability awareness and rapid response.

These processes can be strengthened by incorporating the following components:

COMPONENT 1

Auditing

Routinely assess all network-connected assets to ensure newly introduced systems and software are promptly evaluated for known vulnerabilities. Consider deploying a software solution that frequently and regularly scans your systems.

COMPONENT 2

Analysis

Not all identified vulnerabilities pose an immediate threat. It is recommended to review scan results carefully and conduct research to determine whether a vulnerability is exploitable within the organization's environment and what its potential impact may be. Conducting thorough analyses can help ensure your organization is appropriately remediating vulnerabilities with the highest potential impact.

COMPONENT 3

Prioritization

Establish clear criteria for prioritizing remediation efforts, with particular focus on internet-facing systems, third-party software and any devices that are considered "end of life." Organizations should define service-level agreements (SLAs) for patching vulnerabilities based on severity ratings and maintain an out-of-band process for addressing critical issues that require immediate attention.

ACCESS POINT: EMAIL SECURITY VULNERABILITIES

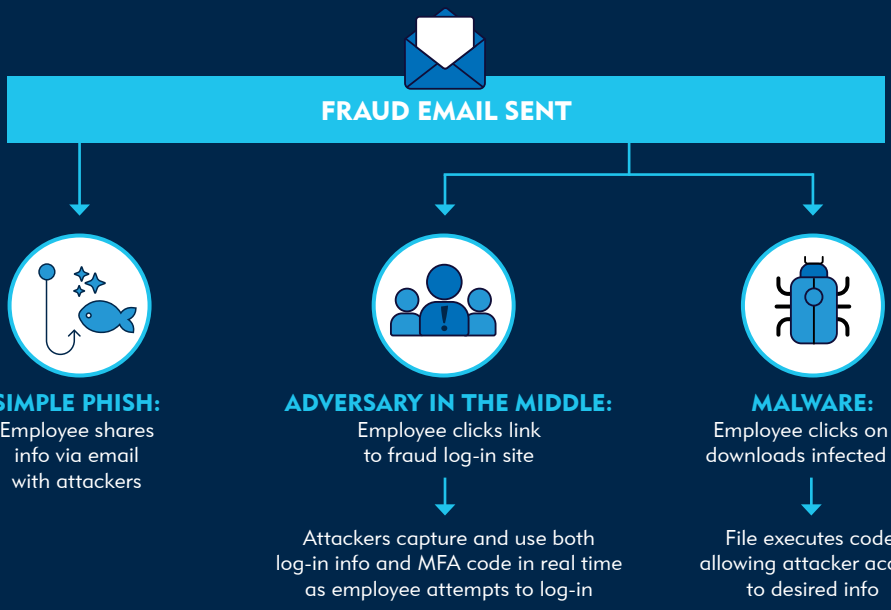
Email remains one of the most common and effective initial access vectors. Furthermore, it can serve as an effective springboard for additional malicious activity. Understanding the methods by which attackers attempt to use email to gain access to an organization's digital network is the first step in preventing such attacks.

Historically, attackers relied on simple phishing techniques that trick users into revealing sensitive information, most commonly login credentials, by impersonating trusted entities. A simple phishing attack involves directing a user to a fake login page designed to capture their username and password. These phishing campaigns typically rely on volume, targeting large numbers of users in the hope someone without MFA enters their credentials. While these simple phishing attacks still occur, they are becoming less common as attackers develop more sophisticated methodologies that employ phishing as the first step.

Artificial Intelligence (AI) tools have played a role in the increasing sophistication. According to Checkpoint, "An AI-driven phishing attack uses artificial intelligence to craft more convincing and tailored phishing messages. These phishing messages may include familiar details, such as references to recent purchases, interests or online interactions, making them appear more credible and harder to ignore." This growing sophistication reflects a broader trend. Rather than relying on volume and simplicity as they have in the past, attackers are interacting, adapting and anticipating.

> "An AI-driven phishing attack uses artificial intelligence to craft more convincing and tailored phishing messages. These phishing messages may include familiar details, such as references to recent purchases, interests or online interactions, making them appear more credible and harder to ignore."

COMMON PHISHING ATTACKS



ADVERSARY IN THE MIDDLE ATTACK:

To bypass multifactor authentication (MFA), attackers increasingly use techniques that mimic legitimate login portals. These fraudulent websites are designed to closely resemble trusted platforms — such as Microsoft 365 or corporate VPN portals — and trick users into entering their credentials. Unlike traditional phishing, man in the middle attacks intercept login sessions in real time. When the legitimate system prompts for an MFA code, the attacker relays that prompt to the victim via the fake portal. Once the victim enters their MFA code, the attacker immediately uses it to access the real system before the session key expires. This tactic is especially effective against organizations that rely solely on time-based one-time passwords or SMS-based MFA, without additional layers of contextual or behavioral verification. Furthermore, AI has made these attacks increasingly sophisticated and impactful. For example, machine learning models can help attackers modify their malicious content into intercepted communications more convincingly and in real time.

MALICIOUS ATTACHMENTS ENABLING DEVICE ACCESS:

Another technique threat actors use to obtain persistent network access is attachments designed to create a false sense of urgency, prompting recipients to open them without verifying the source. In 2024, IBM reported an 84% increase in "infostealer" malware, which is often delivered via fraudulent emails. This increase is aided by machine learning, which helps attackers avoid detection by more closely mimicking actual user behavior. Common file types used in these attacks include PDFs, Word documents, Excel spreadsheets and URLs, making them high-risk attachments susceptible to malicious downloads. Once opened, these attachments may execute malicious code, installing malware that enables unauthorized access, data exfiltration, or further compromise of the endpoint.

Integrating the following defense strategies can help to combat some of these cyber attacks carried out through email:

STRATEGY 1: **Enhanced Monitoring of Suspicious Email Content**

Organizations may employ tools capable of identifying and flagging emails that prompt software installations, contain high-risk attachments, are from a suspicious sender or contain language that elicits an action. These tools are designed to supplement existing email security solutions by providing deeper analysis of message content and attachment behavior. Effective monitoring requires technology that can distinguish truly suspicious emails from benign noise, reducing false positives and improving response efficiency.

STRATEGY 2: **Deploy strong Endpoint Detection and Response (EDR) Solutions**

Implement robust EDR tools to detect and respond to malicious activity at the device level. Ensure these solutions are properly configured to the organization's digital environment, as default settings may not provide adequate protection. Common misconfigurations include incomplete coverage such as missing endpoints for new hires and failure to enable anti-tampering features. Collaboration with vendors during deployment can help tailor the solution to specific organizational needs.

STRATEGY 3: **Restrict Local Administrator Rights**

Limit local administrative privileges to reduce the risk of unauthorized software installation and execution. These privileges allow a user to install software and run administrator commands on their devices. Restricting these rights lowers the attack surface of malicious file downloads, helping to prevent malware from gaining a foothold on user devices. Organizations should regularly audit user permissions and enforce least privilege principles across all systems.

EDR

EDR is "software that uses real-time analytics and AI-driven automation to protect an organization's end users, endpoint devices and IT assets against cyberthreats that get past antivirus software and other traditional endpoint security tools."

CONCLUSION

Initial access vectors are where cybersecurity strategy meets insurance readiness. They're among the most exploited vulnerabilities in today's threat landscape. From remote access gaps to unpatched systems and phishing emails, these entry points are responsible for a significant share of cyber incidents, many of which result in insurance claims.

For insurers, these vectors are more than technical risks — they're underwriting signals. The frequency and severity of claims tied to initial access can make them a focal point in coverage decisions. Organizations that proactively address these vulnerabilities not only reduce their exposure but also demonstrate insurability.

For organizations seeking to build the foundation for a cybersecurity protocol that meets the moment, initial access vectors are the place to start. By strengthening defenses at the point of entry, organizations position themselves for more favorable terms and better outcomes in the event of a breach.

Cyber insurance is evolving alongside the threat landscape, and initial access vulnerabilities are playing a growing role in both.

Reach out to our underwriting experts to learn insights on current trends, common claim drivers, and practical steps that can support a stronger cybersecurity posture.

Reach out to the Arch Cyber team to learn more about what we do and how we can help.

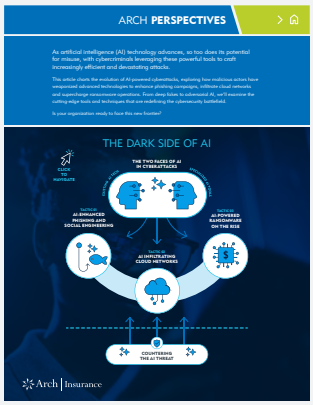
Jamie Schibuk
Executive Vice President,
Professional Liability and Cyber
jschibuk@archinsurance.com

Kyle Lutterman
Vice President,
Cybersecurity Risk Engineer,
Cyber Product Leader
klutterman@archgroup.com

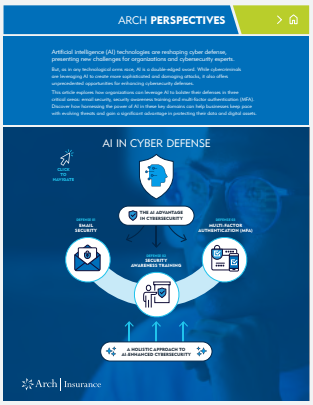
Arch | Insurance

Further Reading:

8 Critical Controls for Cybersecurity and Insurance Coverage



The Dark Side of AI



AI In Cyber Defense

Arch CyPro

Arch Insurance has long been a force and a recognized global leader in the cyber insurance industry, protecting the critical operations of digital businesses. Now, with its new cyber insurance offering, CyPro, Arch is taking a proactive approach to protect its insureds from the ever-evolving threat of cybercrime.

Arch Insurance

Arch Insurance is a market-leading insurer, providing a wide range of property, casualty and specialty insurance options for corporations, professional firms and financial institutions across the U.S. Our approach to doing business is based on collaboration, responsiveness and commitment. Together with our business partners, we pursue better ways of doing things and designing more effective solutions to respond to the needs of our customers.

Scan or click the code. Discover more.

Pursuing Better Together®

archinsurance.com/cypro