zix®

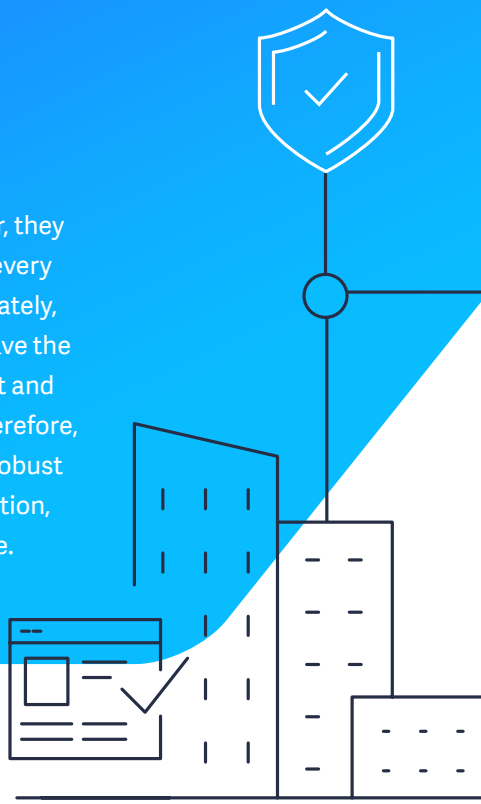
Break the Cyber Threat Cycle with Zix Layered Protection

Achieving robust security does not have to be hard work. However, with the multitude of ways organizations are targeted, coupled with the hundreds of security companies pitching different approaches, choosing and implementing the right security solution can be daunting.

Endpoint security vendors will highlight the many risks of bring your own device (BYOD) and the need to install security directly on the endpoint. Security awareness vendors will tell you that your people are the weakest link. Web or email gateway security vendors will recommend that securing the gateway is your best bet. Finally, a threat hunting expert will tell you it is too late because you've already been compromised!

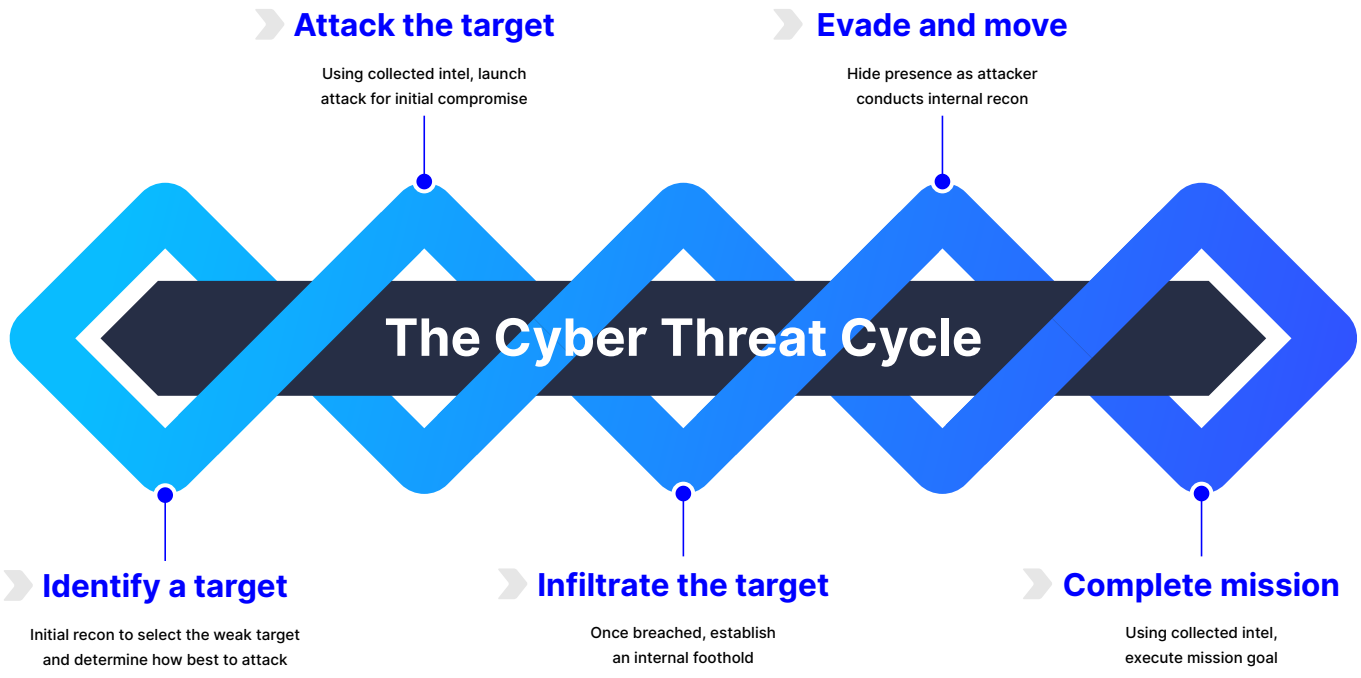
What can you do?

If you evaluate your security strategy through the lens of the security vendor, they all make valid points and the need for every single solution makes sense. Unfortunately, most growing organizations neither have the money, expertise, or time to implement and integrate such a complex strategy. Therefore, what is the most straight forward yet robust security strategy? To answer this question, let's first review the Cyber Threat Cycle.



The Cyber Threat Cycle

The Cyber Threat Kill Chain or Cyber Threat Cycle was first articulated by Lockheed-Martin. Many security organizations have developed their own interpretation of this kill chain but, at its simplest form cyber threat actors commence in 5 major activities:



Activity 1: Identify a target

Threat actors will use a variety of methods for reconnaissance based on their mission goals to identify a target. Tactics can range from company and user profiling via LinkedIn or other social media platforms, through to conducting internet-wide vulnerability scans or snooping communication traffic via man-in-the-middle attacks. Yet, the most widely and easily accessible method has always been email. By sending a seemingly innocent email, threat actors can collect a lot of information, from the type of security gateway in place to whether the user actually exists and willing to engage.

Activity 2: Attack the target

Once a target has been identified, the threat actors will launch their initial attack. The attack can spawn multiple steps but the end goal is the same – gain access to an endpoint or internal server. From analysis of hundreds of thousands of breaches over recent years, email has been the easiest way to gain initial entry in the majority of instances.

Activity 3: Infiltrate the target

Gaining access to a single system does not automatically result in a completed mission. Often the compromised system doesn't have the right access to move within the organization. Threat actors will attempt to establish a foothold through a number of steps including:

- creation of a back door
- set-up a connection to a command and control (C&C) server
- download an exploit
- launch phishing attacks internally
- infiltrate communication channels to establish their reconnaissance.

It's often increasing or elevating the credentials they already have that helps establish a foothold.

Activity 4: Evade and move

Once a threat actor has infiltrated their target, they can act methodically to gain more information and evade detection. At this point, it is important to remember that the breaches that make headlines are often years in the making. The threat actor often laid dormant, closely researching their victim, and waiting for the perfect time to execute the mission goal. Compromising a user's inbox is a common technique to gaining more information about the business processes and personnel within an organization. Yet, threat actors are cunning enough to augment mailbox rules so that their presence is never detected.

Activity 5: Complete mission

The last activity is execution of the mission goal. Is the goal to exfiltrate sensitive data? Is it to force the victim to execute a wire transfer due to ransomware or carefully crafted Business Email Compromise (BEC) attack? Is the goal to wreak havoc by corrupting or making the victim's data inaccessible? At this point, it is a matter of mitigating or containing the execution before the breach makes headlines.

Alignment with industry-known security frameworks ultimately should be the right approach, but to reach that point takes a heavy investment of money, personnel, and time. Further, the deeper the organization finds itself within the cycle the more business interruption will occur. With that in mind, we can begin to formulate a tactical, simple layered protection strategy that initiates a move towards a security-mature goal.

Comparing with a recent breach

Reflecting on the recent SolarWinds breach and exploitation of the Microsoft Exchange 0-day, the associated threat actors started from the beginning of the Cyber Threat Cycle. They needed to run reconnaissance to identify the right target and instigate the initial attack.

This is key to the first part of Zix Layered Protection. Preventing the initial attack takes the least amount of resources and can save the organization the biggest headache. Further, many fail to realize that the majority of successful attacks are rooted in well-established techniques. Similar to the principles of their security counterparts, threat actors balance sophisticated techniques with ease of use. If there is an easy way to infiltrate a target, they will always go that route. The SolarWinds breach was years in the making, as sophisticated as the technique was to drop malware into the SolarWinds Orion system, the breach was almost certainly started with an email. We can make this assumption given the evidence that has been discovered.

Inside the SolarWinds breach

Reconnaissance and attacking the target

There are numerous ways to collect reconnaissance from a target to determine the right attack, and in the SolarWinds case it would appear that email was a primary research tool and ultimately the attack vector.

Points of evidence:

- According to the SEC filing, email was a primary attack vector during the initial SolarWinds attack and APT29 are known to launch phishing attack campaigns as a tactical strategy.
- During the Malwarebytes breach, their investigation uncovered that the, "attackers leveraged a dormant email protection product within their own O365 tenant."
- Microsoft reported to Crowdstrike that a reseller account was being used to read emails that were linked to Crowdstrike.

Infiltrating the target and evading detection

With a spear phishing attack the technique most likely to have been used to initially compromise SolarWinds, there was still no guarantee that the threat actors would be able to move within the environment without the right privileges and ensuring that their activities were going undetected.

Yet according to published details:

- Hackers gained privileged access to restricted systems
- Hackers were communicating via Command and Control infrastructure
- Hackers were altering file systems to prevent detection

Considering these key points, an effective advanced email threat prevention and encryption solution must be part of the layered security framework.

Queue: Zix Layered Protection

Prevent the initial reconnaissance and attack (Activity 1 & 2) with an effective advanced threat protection and email encryption solution coupled with enforcing multi-factor authentication for user logins.

97% of users are still not able to detect a sophisticated phishing attack[1]. SolarWinds is just another reminder that email continues to be core to the Cyber Threat Cycle. It is the most difficult to secure and the easiest to exploit. While security organizations validly discuss new attack techniques and the potential of these being used, there is a never-ending list of evidence that:

- Email is a treasure trove of reconnaissance information
- Email attacks are very cheap for the threat actor to execute
- Employees are no more effective at detecting a phishing attack intended to steal their credentials or malware intended to compromise their endpoint today than they were years ago.

Detect the presence of a threat actor (Activity 3 & 4) with a security audit or monitoring solution

Highly-effective email defense with a better than 99.9% effectiveness rating against phishing and malware will close 95% of your prevention gap. We are aware that threat actors will figure out other ways to get into your network, so developing approaches to protect other vectors will be necessary. However, you can quickly close this gap while evaluating other tools by leveraging a security auditing service. Particularly a solution that focuses on:

- Identifying weaknesses in user login and authentication
- Identifying suspicious behavior related to mailbox rules and email communication

As the SolarWinds breach proved, the threat actors needed to gain access to secured development environments. In that context, monitoring for weaknesses in simple policies like regularly changing passwords, or where a user may be logging into a system from a remote location, can be a clear indication that someone not employed by the organization has made it into your network.

Furthermore, we know in every case of a major breach, when the threat actor has infiltrated the business, they must communicate to something on the outside to retrieve further instructions, files, or exfiltrate internal intelligence. Monitoring for email forwarding rules or activity such as immediately deleting sent messages on an automated basis should set off a red alert.

Therefore a security audit or monitoring tool to detect internal suspicious behavior is a must for the layered protection strategy.

1 https://securityboulevard.com/2021/01/how-to-avoid-the-phishing-bait-in-2021/

Zix Layered Protection

Act on any suspicious behavior through containment and remediation to prevent attacker success (Activity 5).

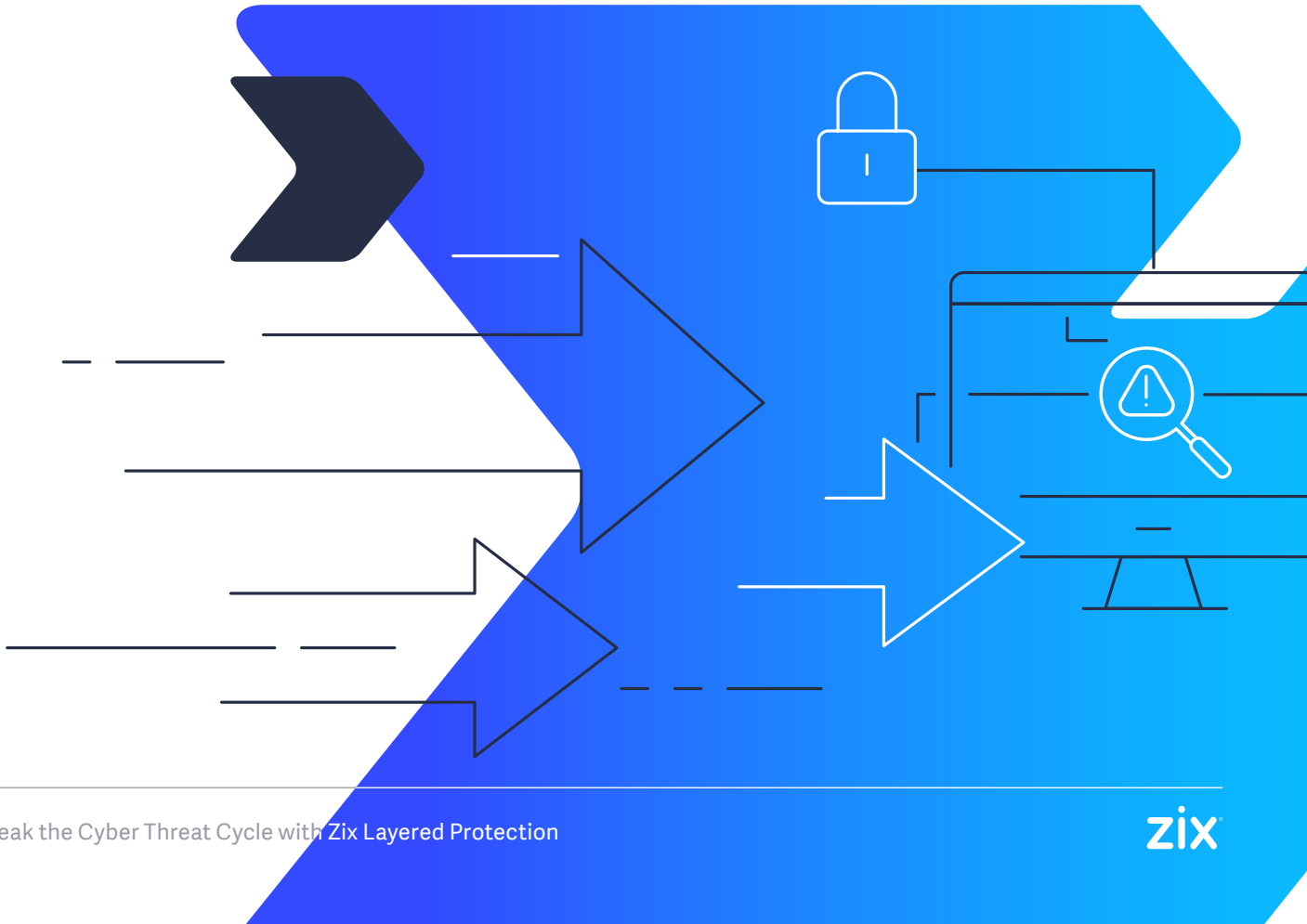
As you put in place the two main components to prevent and detect malicious behavior, the third motion must be in response to what may have failed. As we've indicated, businesses can implement every security solution pitched to them by the hundreds of security vendors available, but Zix Layered Protection is intended to keeping your security as simple as possible while maximizing your time and investment. To complete this goal, the response to the potential breach must be immediate. The goal should be to maintain business productivity even in the face of an attack. Most growing businesses may not have the time or expertise to immediately triage the incident, but they can begin their response and remediation process at no risk. Those tasks at minimum should be:

Immediately remove any malicious email that may have landed within the targeted employee's inbox.

Scan the targeted employee's login activity and require any vulnerable passwords to be changed immediately (enforce MFA if disabled).

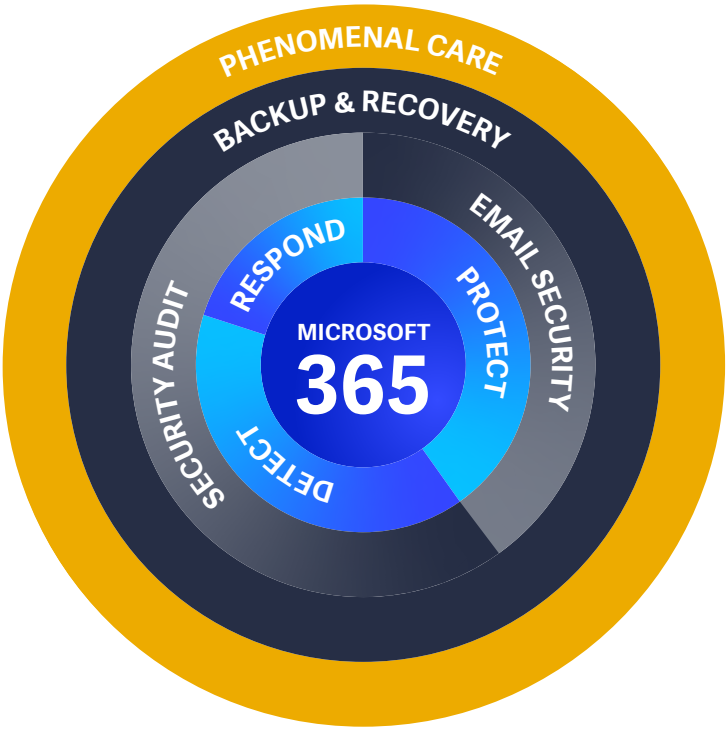
Immediately clear their file systems and provide the targeted employee with a clean working copy of their data.

Zix Layered Protection enables organizations to maintain productivity through Zix Backup and Recovery services. Coupled with message retraction and account lock-down, latent threats can be rapidly eliminated.



How does Zix Layered Protection break the Cyber Threat Cycle?

Zix Secure Cloud turns a complex plan into a simple operational model.



Protect

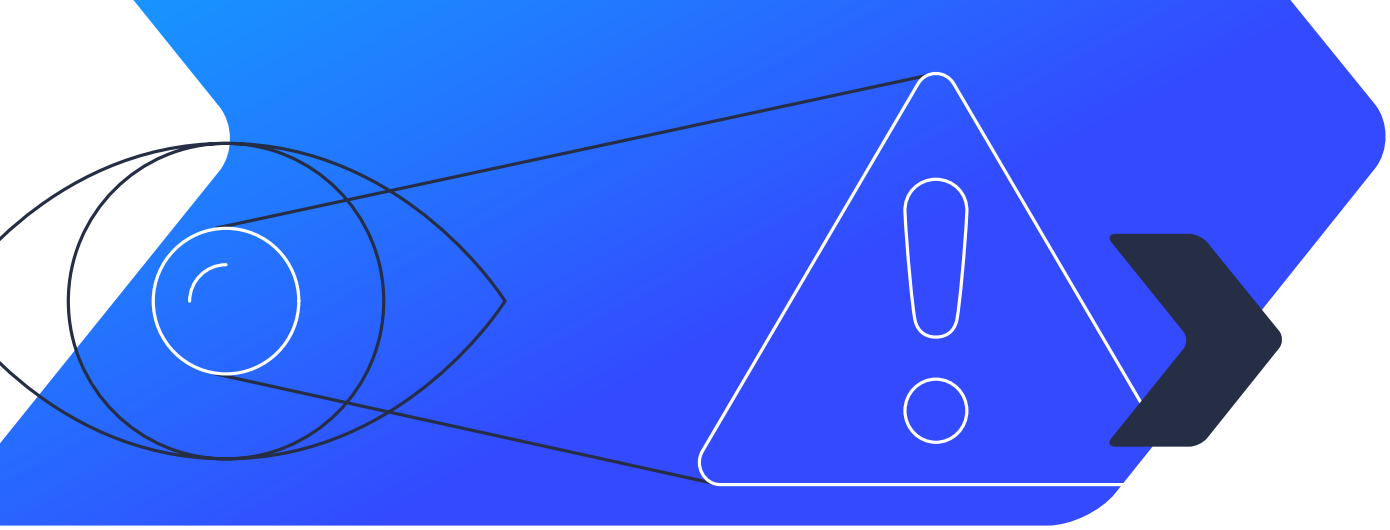
Advanced Email Encryption: The gold standard of encryption secures the email channel so that threat actors cannot hijack the SMTP conversation via a man-in-the-middle attack. With Zix's Best Method of Delivery regardless of who the organization communicates with, business insights are fully protected from inbox to inbox.

Advanced Email Threat Protection: Today's top attack technique continues to be advanced phishing and malware-based attacks. Zix Advanced Email Threat Protection is rated one of the most effective solution in 3rd party testing:

- Phishing Detection Rate: 99.9%
- Threat (Malware, ransomware, etc.) Detection Rate: 100%
- Accuracy Rate: 99.994%

With Zix acting as the first layer of defense the initial compromise is mitigated exponentially.

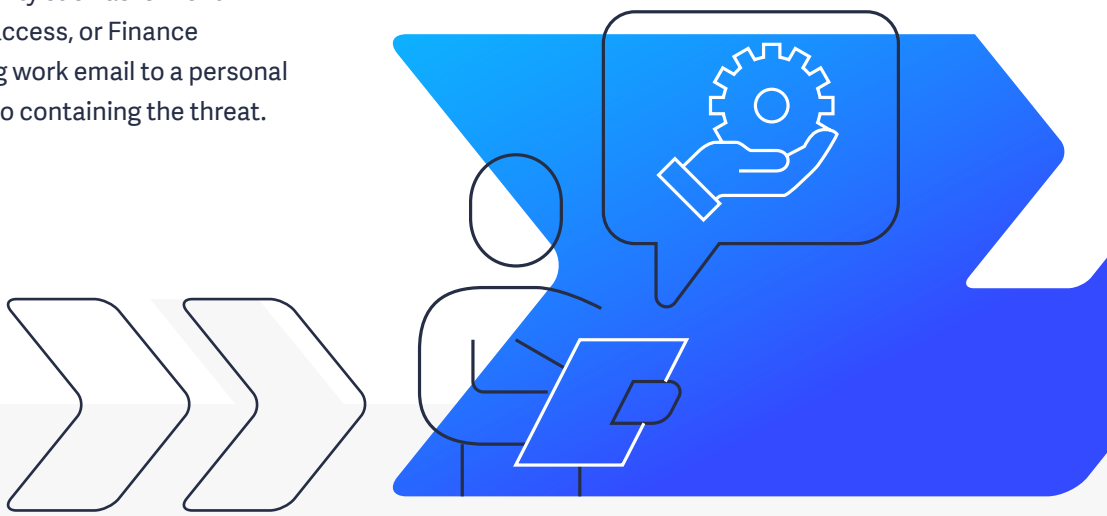
Azure AD Multi-factor Authentication: Relying on users to detect a phishing URL is a recipe for allowing a cybercriminal access to their endpoint. By enforcing multi-factor authentication that is built into every M365 bundle, security teams can close this gap and solve the protection need.



Detect

Security Audit (Detect & Alert): While the protection components exponentially reduce the attack surface, the risk for internal negligence does exist. Continuous monitoring and detection within Zix Security Audit adds a layer of scanning that quickly identifies suspicious activity that bypassed the security gateway. With compromised credentials being the key to establishing a foothold, being able to detect suspicious user activity such as low-end employees having administrative access, or Finance employees suspiciously forwarding work email to a personal email address becomes essential to containing the threat.

Advanced Email Threat Protection Threat Analyst Support: Combined with insights from the Zix Security Audit, customers can work directly with Zix Phenomenal Care and Threat Analyst to immediately develop and implement a mitigation strategy to stop subsequent attacks. This is a unique value-add that is essential to making Zix Layered Protection effective.



Respond

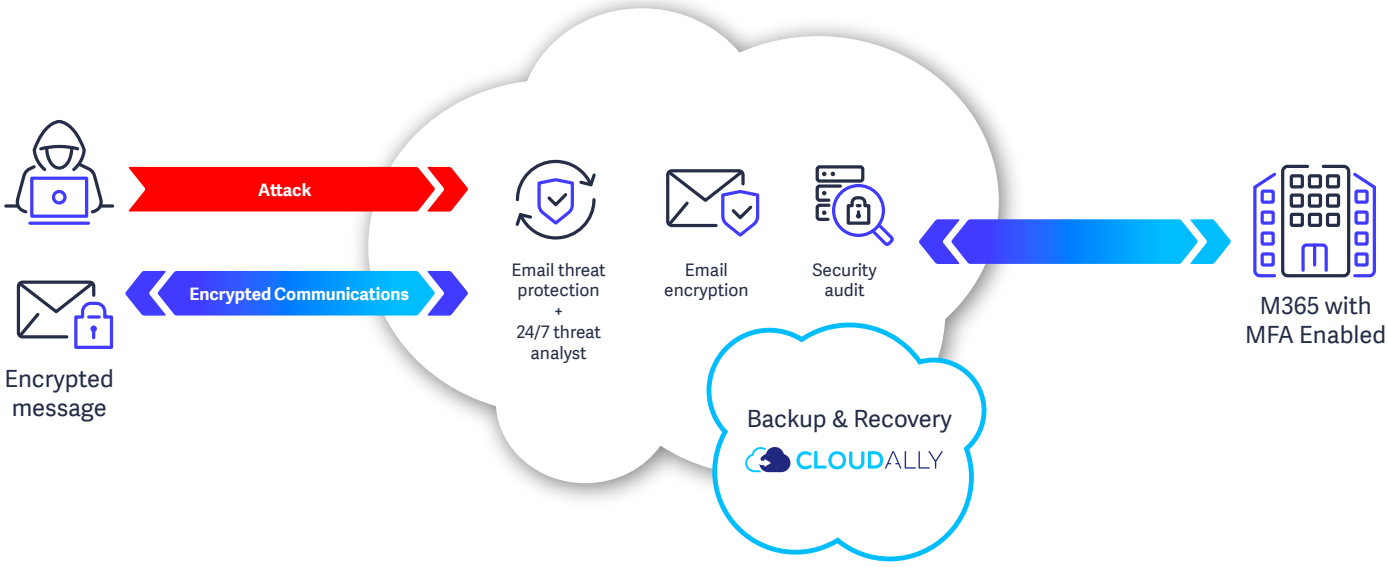
Security Audit (Detect & Alert): Integrated within the Security Audit are actionable response steps to stop threat actors in their tracks such as locking the user out of the environment.

Advanced Email Threat Protection (Message Retraction): An additional response step to take once a threat is discovered is to remove any existence of malicious email that may have been launched internally from the compromised account. Message retraction provides the ability to immediately reduce the risk to anyone else that may have been targeted.

Backup & Recovery: Any response goal must keep employee productivity in mind. With Zix Backup and Recovery services, even if the attacker goal was to corrupt corporate data or hold the data for ransom, the business has peace-of-mind knowing that they have a clean copy of their data to keep their business going.

Advanced Email Encryption (DLP): Insight into what the attacker may have been after can provide an advantage to keeping this data secure. With Data Loss Prevention policies within Zix Advanced Email Encryption, security personnel are notified if key information is attempted to be extracted via email.

Enabled by Zix Secure Cloud



Zix Secure Cloud plus Azure AD Multi-factor Authentication encompasses the layered protection. With these foundational pieces in place, growing businesses can focus on their productivity without being exposed to significant gaps. We recognize that the threat landscape is constantly changing and no growing business should stand still, as their business matures so will the threats targeting them. With assistance from our security partners, we can help guide you through your maturity path while keeping the strategy simple and straightforward.

For further information on Zix Layered Protection or to request a Security Review contact: 800-729-3496 or visit: zix.com