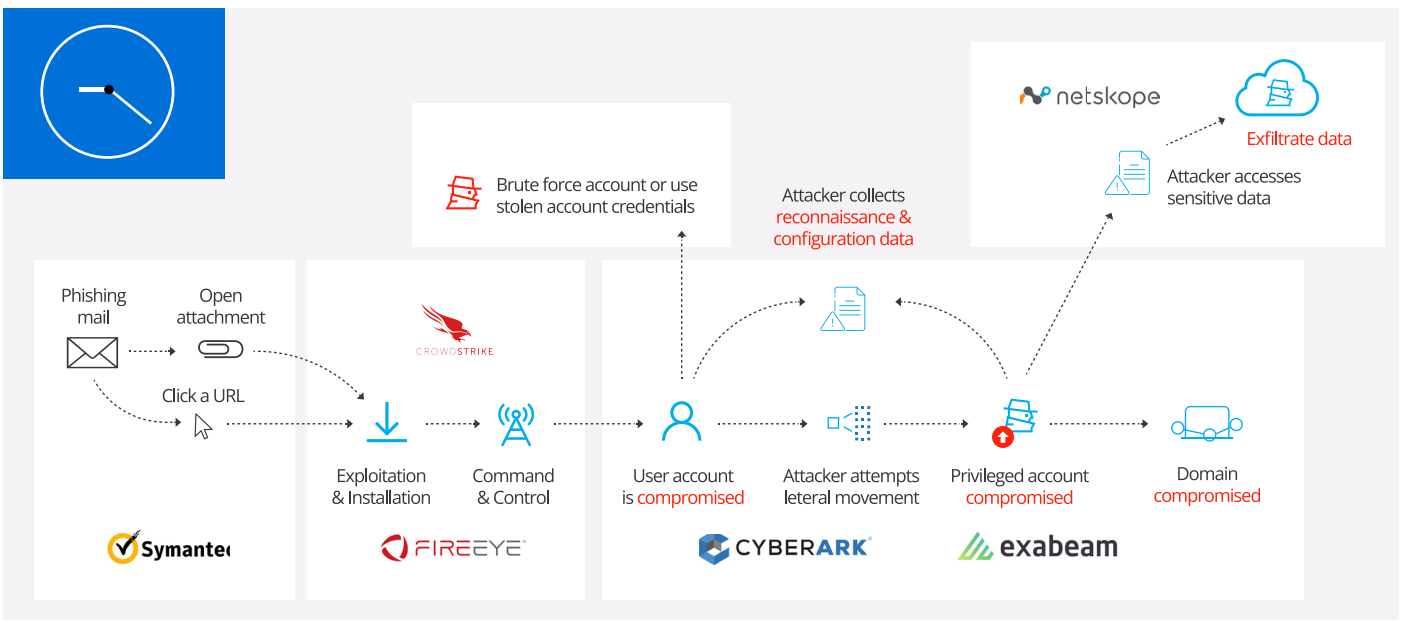
# Consolidating your security framework within your existing Azure infrastructure

The cybersecurity environment for the average organisation has become unmanageable. It is common to have over 40 products from a wide range of vendors operating independently of each other. It's time to simplify and improve visibility across the security estate to ensure full coverage in the face of today's ever more sophisticated threat landscape. A single ecosystem is needed to reduce the overhead of management and increase the operational efficiency and response times of security teams.

Microsoft is leading the way in this space with their extended detection and response (XDR) platform. This encompasses the entire Microsoft security stack, including many services recognised by Gartner as industry-leading solutions. And as an Azure user, the more you consolidate with Microsoft, the more you save.

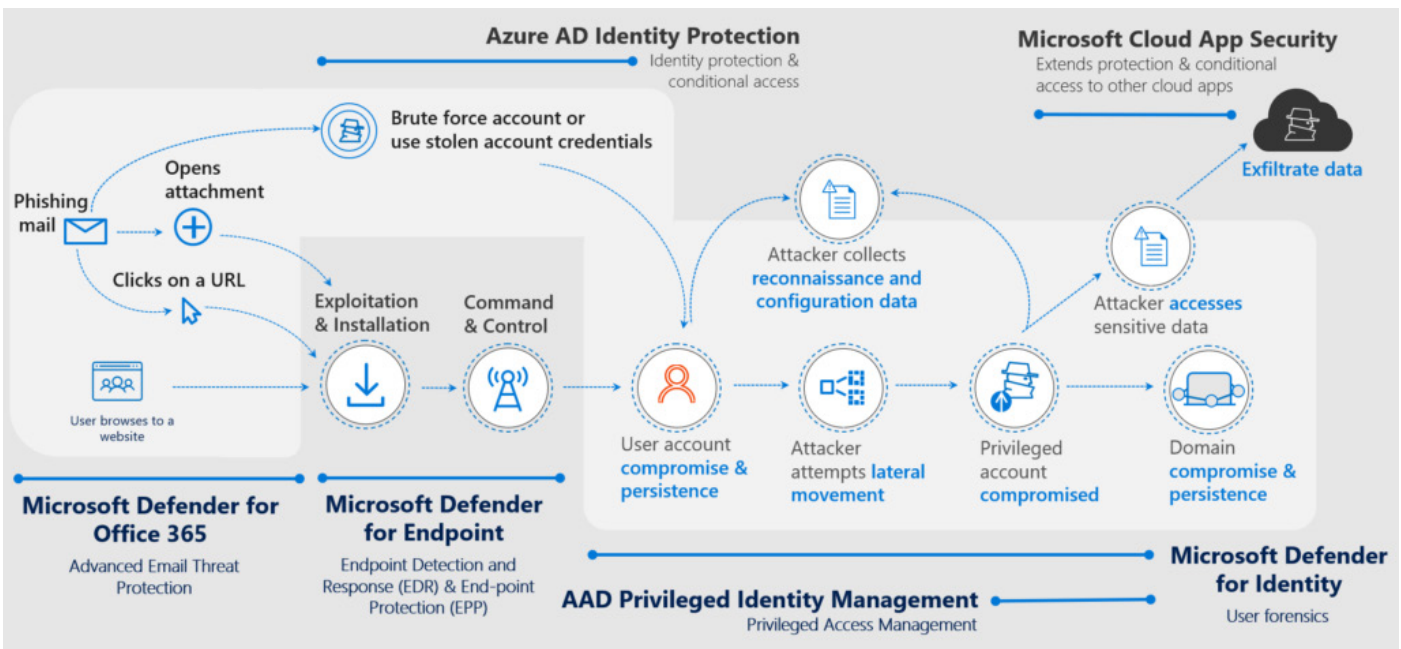
## Attack kill chain with multiple vendors

This chart represents how many businesses are currently set-up to respond to a malware attack delivered by email. While the entire attack chain is covered, it requires seven vendors to provide this coverage. The complexity of this environment leads to delays in detection time and a lack of automated response. Performing digital forensics across the entire attack chain is a laborious, manual, and time-consuming process.




## Attack kill chain with Microsoft XDR

The same attack kill chain can be protected entirely under the Microsoft XDR umbrella, where each product enhances the fidelity of the previous alert. A single incident is created in Microsoft Sentinel that covers the entire attack. Microsoft Sentinel is the SIEM platform that enables the integration of threat intelligence from all sources (be they internal, external, cloud or on-premises) and enables security analysts to detect and respond to all incidents in seconds instead of hours.




## Consolidation delivers cost savings

As part of your Microsoft Azure account, you already have access to the Microsoft XDR suite, though you will likely need some expert support to fully leverage the game-changing capabilities of these solutions and to rapidly reduce your costs. Your expensive log costs, for example, can be reduced to zero for logs from Microsoft Exchange or Azure AD and the first 50GB of server logs are free from all sources. You will continue to pay for logs ingested from external endpoints, for example, so the more effectively and quickly you can consolidate in Azure, the sooner the savings will be realised.

**CyberOne is a Microsoft Gold Partner. We specialize in deploying Microsoft XDR & Sentinel. Contact us for tailored advice on your integration journey.**

Get in touch →

### About CyberOne

CyberOne strives to offer the most trusted cyber experience in the digital world. Founded in 2005 and based in Milton Keynes, our assessment, detection and response services empower you to stay one step ahead of the latest cyber threats. We are trusted by leading UK and global businesses and our people provide a service that is second to none.

www.cyberone.security
+44 (0)3452 757575
enquiries@cyberone.security