CONTRAFORCE

Microsoft Security 101: Everything You Need to Know

An overview of Microsoft security tools, licenses, and product gaps to help eliminate blind spots and build a stronger security posture.

INTRODUCTION

Over the past few years, we've embraced major changes to the way we work, from hybrid/remote work environments to the rapid adoption of new technologies. These changes brought a volume and sophistication of cyberattacks unlike anything we've seen before.

Small and mid-sized enterprises are struggling to keep up with this ever-changing landscape. With the adoption of Zero-Trust policies, IT teams are forced to verify every user, endpoint, and application, adding an unprecedented amount of work to their plate.

Fortunately, most of these small and mid-sized enterprises have already invested in Microsoft security tools, most commonly those included in a Business Premium, E3, or E5 license. Each of the Microsoft licenses contains a bundle of security products designed to support companies' cybersecurity initiatives.

Microsoft's security tools are undoubtedly some of the most robust and trusted tools on the market— but they are inherently complex, from procurement to configuration and everyday use.

In this eBook, we'll break down the nuances of Microsoft security, including how to choose the right license, understanding the security tools included, and how to maximize your Microsoft investment.

Microsoft Business Premium

Microsoft Business Premium is a cloud-based subscription offering designed to provide a wide range of business services for small and medium businesses of up to 300 employees. The subscription costs $22 per user per month (when purchased with an annual contract via Microsoft or through a certified reseller).

Business Premium provides access to Microsoft's 365 application suite, a generous amount of storage per user, as well as important collaboration services such as Exchange Online, Skype for Business and Microsoft Teams. Business Premium also provides a powerful set of security features, providing the access to nearly all of the core security infrastructure a small or medium business needs to protect against cyber threats. Below you'll find a summary of the key security features of Business Premium.

BUSINESS PREMIUM AT A GLANCE

- ✓ Provides a strong foundation of security capabilities at an affordable price
- ✓ A SIEM such as Microsoft Sentinel provides the glue needed to bring the overall security solution together, and integrate any 3rd party solutions
- ✓ Buyers should consider augmenting it with Defender for Cloud and Defender for Cloud Apps if they have significant use of cloud infrastructure and SaaS apps
- ✓ Buyers will need to look outside of Microsoft to fill gaps in areas such as backup and recovery, network firewall, and VPN

Microsoft Business Premium Key Security Features

SECURITY PILLAR	SECURITY CAPABILITIES INCLUDED	SUGGESTED SECURITY ADD-ONS
Security Foundations	**Device Management** and **Patch Management** capabilities in Business Premium provide the foundation to manage and control your security footprint. **Vulnerability Scanning** is another foundational piece of security infrastructure, helping administrators to identify and prioritize missing patches and insecure configurations. *Delivered via: Microsoft Intune, Defender for Business*	While Microsoft's cloud data services provide built-in redundancy and high-availability, most organizations will benefit from deploying a robust third-party **Backup and Recovery** solution to provide a failsafe should ransomware or other threats make data unavailable. *Requires third-party solution*
Endpoint Protection	Business Premium provides a wide set of protection features, including next-generation **anti-malware protection** for laptops, desktops, and mobile devices. Business Premium also delivers **attack surface reduction**, a critical set of features that proactively identifies and blocks known exploit techniques and disables potentially harmful features. *Delivered via: Defender for Business*	
Network Protection	Business Premium includes a variety of capabilities to help protect against **email-based threats** such as spam and phishing, as well as threats that might present through collaboration tools such as SharePoint or OneDrive. Business Premium also brings **cloud application discovery**, to provide visibility and risk assessments against more than 31,000 common SaaS applications. *Delivered via: Defender for Office 365 Plan 1, Azure Active Directory Plan 1*	Organizations with on-premises applications will continue to benefit from investing in a third-party **network firewall** to defend the corporate environment against network-based threats, as well as a **VPN** to provide secure remote access. In addition, as many organizations have moved toward broader deployment of cloud-based SaaS services, a **Cloud Access Security Broker (CASB)** solution gives defenders enhanced control over these distributed cloud applications. *CASB delivered via: Defender for Cloud Apps* *Third-party solutions required for firewall and VPN*
Cloud Protection		Enterprise applications running within cloud infrastructure such as Microsoft Azure, Amazon Web Services, and Google cloud require tailored protection, both to protect against threats at runtime, as well as to ensure that containers and cloud workloads are securely configured and deployed. Many organizations find it worthwhile to invest in **Cloud Workload Protection (CWP)** as well as **Cloud Security Posture Management (CSPM)** capabilities to fill these crucial gaps. *Delivered via: Defender for Cloud*
Identity Protection	In order to ensure that users' identities are protected from abuse and misuse, secure **user provisioning**, **single sign-on**, and **multi-factor authentication** are critical tools for any organization. *Delivered via: Azure Active Directory Premium Plan 1*	Organizations who deploy Active Directory on-premises will benefit from enhanced protection to secure local user accounts. *Delivered via: Defender for Identity*
Data Protection	Business Premium includes a solid set of basic data protection features, to help organizations protect against loss or theft of sensitive data. Bitlocker and Bitlocker-to-Go provide **encryption for laptops and USB devices** to protect data should a device become lost or get stolen. Encryption provides protection for data-at-rest, but additional measures are required to protect data as it moves around the organization. For starters, Business Premium gives organizations the ability to apply **sensitivity labeling** as well as **basic message encryption** to track and protect data-in-motion. *Delivered via: Bitlocker, Bitlocker-to-Go, Azure Information Protection Plan 1*	
Security Operations	With today's sophisticated attackers, it's critical that security teams focus not only on preventing threats, but detecting and responding to threats that slip past automated defenses. Business Premium includes Microsoft's powerful **Endpoint Detection and Response (EDR)**, to provide deep context and analysis of an emerging threat. *Delivered via: Defender for Business*	With the diverse range of threats, from endpoint to network to data and cloud, security teams can be faced with a daunting number of consoles and interfaces needed to get the full picture of an attack. **Security Information and Event Management (SIEM)** solutions pull it all together and overlay additional analysis to dramatically cut down on the time needed to investigate, understand, and respond to attacks while Security Orchestration and Automation and Response (SOAR) helps security teams automate tedious and repetitive tasks, coordinate their workflows, and respond to security incidents quickly and effectively. *Delivered via: Microsoft Sentinel*

Microsoft 365 E3

Microsoft E3 is the first level of Microsoft 365 enterprise licenses and costs $36 per user. While initially designed for organizations with over 300 employees, many companies with a heavy tech focus or high data storage requirements have skipped past Business Premium in order to gain the benefits of the additional capabilities included in E3.

When it comes to security functionality, E3 includes most of the same features as Microsoft Business Premium, with a couple of exceptions, notably email protection as well as endpoint detection and response. Organizations with E3 licenses should consider investing in standalone licenses for these important capabilities.

MICROSOFT E3 AT A GLANCE

- ✓ E3 lacks EDR and email protection capabilities. To fill these gaps, organizations often consider augmenting their E3 license with Defender for Office 365 Plan 1 as well as Defender for Endpoint Plan 2
- ✓ A SIEM such as Microsoft Sentinel provides the glue needed to bring the overall security solution together, and integrate any 3rd party solutions
- ✓ Buyers often consider augmenting this license with Defender for Cloud and Defender for Cloud Apps if they have significant use of cloud infrastructure and SaaS apps
- ✓ Buyers will need to look outside of Microsoft to fill gaps in areas such as backup and recovery, network firewall, and VPN

Microsoft E3 Key Security Features

SECURITY PILLAR	SECURITY CAPABILITIES INCLUDED	SUGGESTED SECURITY ADD-ONS
Security Foundations	**Device Management** and **Patch Management** capabilities in E3 provide the foundation to manage and control your security footprint. **Vulnerability Scanning** is another foundational piece of security infrastructure, helping administrators to identify and prioritize missing patches and insecure configurations. *Delivered via: Microsoft Intune, Microsoft Defender for Endpoint Plan 1*	While Microsoft's cloud data services provide built-in redundancy and high-availability, most organizations will benefit from deploying a robust third-party **Backup and Recovery** solution to provide a failsafe should ransomware or other threats make data unavailable. *Requires third-party solution*
Endpoint Protection	E3 provides a wide set of protection features, including next-generation **anti-malware protection** for laptops, desktops, and mobile devices. E3 also delivers **attack surface reduction**, a critical set of features that proactively identifies and blocks known exploit techniques and disables potentially harmful features. *Delivered via: Defender for Business*	
Network Protection	E3 brings **cloud application discovery**, to provide visibility and risk assessments against more than 31,000 common SaaS applications. *Delivered via: Azure Active Directory Plan 1*	E3 lacks features to **protect against email-based threats** such as spam and phishing. Email is one of the most common vectors for attacks, and it's worth investing in a solution here to reduce risk. Organizations with on-premises applications will continue to benefit from investing in a third-party **network firewall** to defend the corporate environment against network-based threats, as well as a **VPN** to provide secure remote access. In addition, as many organizations have moved toward broader deployment of cloud-based SaaS services, a **Cloud Access Security Broker (CASB)** solution gives defenders enhanced control over these distributed cloud applications. *Email protection delivered via: Defender for Office 365 Plan1. CASB delivered via: Defender for Cloud Apps. Third-party solutions required for firewall and VPN*
Cloud Protection		Enterprise applications running within cloud infrastructure such as Microsoft Azure, Amazon Web Services, and Google cloud require tailored protection, both to protect against threats at runtime, as well as to ensure that containers and cloud workloads are securely configured and deployed. Many organizations find it worthwhile to invest in **Cloud Workload Protection (CWP)** as well as **Cloud Security Posture Management (CSPM)** capabilities to fill these crucial gaps. *Delivered via: Defender for Cloud*
Identity Protection	In order to ensure that users' identities are protected from abuse and misuse, secure **user provisioning**, **single sign-on**, and **multi-factor authentication** are critical tools for any organization. *Delivered via: Azure Active Directory Premium Plan 1*	Organizations who deploy Active Directory on-premises will benefit from enhanced protection to **secure local user accounts**. *Delivered via: Defender for Identity*
Data Protection	E3 includes a solid set of basic data protection features, to help organizations protect against loss or theft of sensitive data. Bitlocker and Bitlocker-to-Go provide **encryption for laptops and USB devices** to protect data should a device become lost or get stolen. Encryption provides protection for data-at-rest, but additional measures are required to protect data as it moves around the organization. For starters, E3 gives organizations the ability to apply **sensitivity labeling** as well as **basic message encryption** and **Data Loss Prevention (DLP)** for email and files to track and protect data-in-motion. *Delivered via: Bitlocker, Bitlocker-to-Go, Azure Information*	
Security Operations		With today's sophisticated attackers, it's critical that security teams focus not only on preventing threats, but detecting and responding to threats that slip past automated defenses. **Endpoint Detection and Response (EDR)** technology provides deep context and analysis of emerging threats. To get EDR functionality, organizations will need to upgrade from Microsoft Defender for Endpoint Plan 1 (included in E3) to Plan 2 With the diverse range of threats, from endpoint to network to data and cloud, security teams can be faced with a daunting number of consoles and interfaces needed to get the full picture of an attack. **Security Information and Event Management (SIEM)** solutions pull it all together and overlay additional analysis to dramatically cut down on the time needed to investigate, understand, and respond to attacks while Security Orchestration and Automation and Response (SOAR) helps security teams automate tedious and repetitive tasks, coordinate their workflows, and respond to security incidents quickly and effectively. *EDR (and additional capabilities) Delivered via: Microsoft Defender for Endpoint Plan 2* *SIEM and SOAR Delivered via: Microsoft Sentinel*

Microsoft 365 E5

Microsoft 365 E5 is Microsoft's most comprehensive enterprise bundle, and costs $57 per user. E5 includes the full set of capabilities in the E3 package, along with additional capabilities to provide enhanced business analytics, telephony and audio conferencing, and support for compliance, among others.

Some of the most significant additions in E5 come in the form of enhanced security features, including more comprehensive protection for identities, cloud applications, and data, as well as advanced capabilities to assist security analysts in investigating and responding to threats.

MICROSOFT E5 AT A GLANCE

- ✓ Provides the most comprehensive set of security capabilities
- ✓ A SIEM such as Microsoft Sentinel provides the glue needed to bring the overall security solution together, and integrate any 3rd party solutions
- ✓ Buyers often consider augmenting it with Defender for Cloud if they have significant use of cloud infrastructure
- ✓ Buyers will need to look outside of Microsoft to fill gaps in areas such as backup and recovery, network firewall, and VPN

Microsoft E5 Key Security Features

SECURITY PILLAR	SECURITY CAPABILITIES INCLUDED	SUGGESTED SECURITY ADD-ONS
Security Foundations	E5 provides the same **Device Management**, **Patch Management**, and **Vulnerability Scanning** capabilities as E3. *Delivered via: Microsoft Intune, Microsoft Defender for Endpoint Plan 2*	While Microsoft's cloud data services provide built-in redundancy and high-availability, most organizations will benefit from deploying a robust third-party **Backup and Recovery** solution to provide a failsafe should ransomware or other threats make data unavailable. *Requires third-party solution*
Endpoint Protection	In addition to next generation **anti-malware protection** and **attack surface reduction** in E3, E5 incorporates **document containment** technology that isolates untrusted documents to prevent access to trusted corporate resources, as well as Microsoft's **Safe Documents** feature that automatically scans documents when they are opened for malicious content such as macros, malicious URLs or embedded objects. *Delivered via: Microsoft Defender for Endpoint Plan 2, Application Guard for Office 365, Microsoft Defender for Office 365 Plan 2*	
Network Protection	E5 provides comprehensive **protection against email-based threats** such as spam and phishing, as well as c**loud application discovery** and **Cloud Access Security Broker (CASB)** to provide visibility and enhanced control over more than 31,000 common SaaS applications. *Delivered via: Microsoft Defender for Office 365 Plan 2, Microsoft Defender for Cloud Apps*	Organizations with on-premises applications will continue to benefit from investing in a third-party **network firewall** to defend the corporate environment against network-based threats, as well as a **VPN** to provide secure remote access. *Third-party solutions required for firewall and VPN*
Cloud Protection		Enterprise applications running within cloud infrastructure such as Microsoft Azure, Amazon Web Services, and Google cloud require tailored protection, both to protect against threats at runtime, as well as to ensure that containers and cloud workloads are securely configured and deployed. Many organizations find it worthwhile to invest in **Cloud Workload Protection (CWP)** as well as **Cloud Security Posture Management (CSPM)** capabilities to fill these crucial gaps. *Delivered via: Defender for Cloud*
Identity Protection	E5 delivers the same **user provisioning**, **single sign-on**, and **multi-factor authentication** capabilities of E3, and brings additional advanced capabilities to better manage privileged identities and entitlements, as well as to **detect identity vulnerabilities and risky accounts**. For organizations who deploy Active Directory on-premises, E5 also provides enhanced protection to **secure local user accounts**. *Delivered via: Azure Active Directory Premium Plan 2, Defender for Identity*	
Data Protection	E3 provided a baseline for protecting data at rest with **encryption for laptops and USB devices** to protect data should a device become lost or get stolen, and this is also included in E5. E5 provides greatly enhanced protection for data-in-motion by providing automatic sensitivity labeling as well as more comprehensive **data loss prevention (DLP)**, including **DLP for Teams Chat** and **DLP for endpoints** in addition to **DLP for email and files.** *Delivered via: Bitlocker, Bitlocker-to-Go, Azure Information Protection Plan 2, Microsoft Purview*	
Security Operations	E5 provides Microsoft's most advanced tools to assist SOC analysts in quickly identifying and responding to threats that slip past automated defenses, starting with **Endpoint Detection and Response (EDR)** technology to provide deep context and analysis of emerging threats. In addition to endpoints, E5 provides capabilities to help defenders with **Identity Risk Detection and Investigation**, as well as **Email Threat Detection and Response.** To help further accelerate threat response, E5 includes access to Microsoft's own **Threat Experts** to provide deep assistance in understanding emerging threats. *Delivered via: Microsoft Defender for Endpoint Plan 2, Microsoft Defender for Identity, Microsoft Defender for Office 365 Plan 2*	With the diverse range of threats, from endpoint to network to data and cloud, security teams can be faced with a daunting number of consoles and interfaces needed to get the full picture of an attack. **Security Information and Event Management (SIEM)** solutions pull it all together and overlay additional analysis to dramatically cut down on the time needed to investigate, understand, and respond to attacks while **Security Orchestration and Automation and Response (SOAR)** helps security teams automate tedious and repetitive tasks, coordinate their workflows, and respond to security incidents quickly and effectively. *SIEM and SOAR Delivered via: Microsoft Sentinel*

What's not included in these licenses?

The biggest missing piece from Microsoft's Business Premium and Enterprise licensing is Sentinel—Microsoft's cloud-native SIEM (Security Information and Event Management). Sentinel ingests security data from across your Microsoft ecosystem, hybrid-cloud environment, and varying security tools to allow threat detection and response capabilities. An organization's data is stored within an Azure Monitor Log Analytics workspace (which is also purchased separately from BP/E3/E5 licensing). Sentinel then brings the data from the Logs Analytics workspace into its own console, where it analyzes the security data.

An added benefit of Sentinel is that is also includes SOAR (security orchestration, automation, and response) capabilities in order for you to automate SecOps (Security Operations) incident response workflows.

Your Azure subscription is billed by the volume of data stored processed through Sentinel and stored in the Log Analytics workspaces. Microsoft provides a pricing calculator to estimate hourly or monthly costs.

While Sentinel brings the Microsoft security suite together, it's an incredibly robust tool that is often too heavy for smaller-sized organizations. Not only is it expensive, but users find it to be challenging to implement and configure properly, leading to missed security alerts. Sentinel requires sophisticated security expertise, like understanding how to run KQL queries to perform log searches and the ability to create, tune, and manage detection rules. Additionally, users must also understand how to write using Juypter notebooks for threat hunting, and have expertise in Logic Apps to create automated incident response workflows. Users also mention the counterintuitive UI that adds to its complexity.

Challenges with managing Microsoft security tools

Microsoft security tools, though some of the most robust and advanced tools on the market, come with their fair share of challenges.

Managing too many consoles and tools

We listed many individual tools and capabilities in the above table, and that just scratches the surface of all the tools (both security and non-security) included in the Microsoft ecosystem. When working with these tools, users are required to log into each individual console, app, or product to manage and maintain the information. Not only does this monopolize the time of IT teams, but it creates blind spots and lack of visibility which then increases cyber risk.

Data Overload

In addition to managing a vast array of products, there's a massive amount of data stored in each tool—sensitive user information, permission settings, governance data, threat alerts, detection verification, behavior anomalies, and much more. On top of that, IT teams are required to watch data from many places: applications, logs, infrastructure, network devices, clouds and users.

Signal-to-noise ratios quickly become unbalanced, requiring teams to sift though huge pools to data (which becomes increasingly expensive to store).

Take Defender for Cloud Apps for example. Defender for Cloud Apps is known for generating noise due to challenges with tuning and its default policy alert (which is configured to generate an alert every time the system identifies a met policy criteria). While there are many modifications that can be made to alerts (like grouping together repeated activities into one incident alert), this takes time and an intimate understanding of detection tuning.

Reducing False Positives and False Negatives

With the increase in data and noise, teams are forced to verify threats at a larger scale. As Sentinel helps bring in all the ingested data, it requires the user to put specific automation rules in place to modify existing analytics rules. The problem, however, is the amount of knowledge and time required to be able to put these rules in place and often, these configurations must happen at the product-level.

Further, for many Microsoft tools (like Defender for Endpoint and other endpoint solutions), a user must submit an entity to Microsoft for analysis when a false positive or negative is detected. At this point, Microsoft's team of security analysts will dig into the case to analyze the case for further tuning. Not only is this a time consuming process, but Microsoft notes that "authenticated customers, especially enterprise customers with valid Software Assurance IDs (SAIDs) are given a higher priority."

HOW TO SIMPLIFY YOUR MICROSOFT SECURITY STACK

For most small and mid-sized enterprises, IT professionals care about two things: simplicity and security. While Microsoft creates incredibly robust tools, ContraForce makes them efficient and simple.

ContraForce condenses your Microsoft security stack into one, easy-to-use platform (with no need to deploy or use Sentinel). It eliminates blind spots, automates threat detection, provides one-click incident response, and offers actionable insights that stakeholders will understand.

For a demo of the platform or to speak with a security expert, click here.

CONTRAFORCE

ContraForce
7540 121 SH Suite 200,
McKinney, TX 75070

For more information visit
contraforce.com