



Microsoft E5 Licensing: A Comprehensive Guide



Microsoft E5 Licensing: A Comprehensive Guide

From security to compliance to analytics, the functionality of Microsoft 365 E5 can help companies consolidate resources, improve operations, and conserve their budget. Beyond standard SharePoint and email capabilities, we explore how E5 provides advanced identity and threat protection for users, devices, and apps.

The Value of E5 Over M365 License

There are millions of people using M365 today due to its comprehensive suite of tools and built-in security. The scalability and accessibility of the platform have made it particularly useful for remote teams and SMBs looking to trim costs. Upgrading to E5 extends the benefits, allowing Microsoft users to improve protections and operational efficiency while reducing their tech budget.

Security Enhancements and Operational Efficiency

With Advanced Threat Protection (ATP), Cloud App Security, and Microsoft Defender Advanced Threat Protection (ATP), E5 introduces a slew of additional hurdles for threat actors to jump through to reach their goal. What's more, these protections can stretch across environments.

When many companies have footprints across Google, AWS, and Azure in addition to their on-premises servers, E5 takes an integrated approach to cloud security. Defender for Cloud includes data under a company's umbrella. It adds more structure to your tech stack, particularly as it pertains to compliance and security policy standardizations. Securing different cloud environments has been a headache for companies when they have to string different protocols together. By eliminating the need for additional tools, this feature can translate to up to 30% savings.

Microsoft Sentinel has also introduced some incredible advantages to companies that want to improve their operational efficiency. For enterprises with complex needs, tools like Splunk have been notoriously difficult to set up, especially for companies that have to configure multiple types of storage. Because Sentinel is in the cloud, it can take just 20 minutes to get up and running.

On average, Dataprise found that it takes 67% less time to deploy and, when combined with Azure network security, 73% improved efficiency for network-related IT work. Tools like single sign-on make it possible for users to reset their own passwords, leading to a 75% reduction in password requests to the Help Desk. This reduction in busy work opens up their time to focus on more pressing matters.



Evergreen Service

Swapping out several standalone services for E5 ensures that companies have an evergreen service. While the change will disrupt operations in the short term, the long-term outlook is smoother than companies that stick with their current system. Instead of being at the mercy of updates from multiple vendors, companies can expect a constant stream of improved capabilities and features. Tools like Advanced Analytics with Power BI Pro can improve compliance, while Cloud PBX and PSTN Conferencing help teams collaborate from wherever they are.

When vendors have a tendency to roll out changes in erratic patterns, this shift can make a marked difference in a company’s operations. Employees can be more productive, improving output in addition to the cost savings. Plus, now you only have one service contract to deal with instead of several.



Understanding Microsoft E5 vs Microsoft E3 Licensing

When comparing the two licensing options. The core takeaway is that E5 offers enhanced features to users. Companies can expect better security, stronger compliance oversight, and more communication options. From a cost perspective, the average difference per user is around \$25.50 a month (\$32 for E3 vs. \$57.50 for E5).

These features can be customized and scaled to fit the needs of each client, and the licensing add-ons are proven to augment the securities already found in the E3 package. This is particularly true for larger corporations that may be at higher risk of a breach, though it’s fair to say that even smaller-scale operations may find the upgrade worth it.

What Layers Are Included in the Microsoft Security Portfolio?

- Identity and access management: MFA, identity management, and identity protection allow only authorized individuals to access key resources.
- Threat protection: Tools like Defender for Endpoint and Sentinel ward off even the most well-planned attacks, including malware and phishing.
- Information Protection: This layer, which includes Azure Information Protection and Microsoft Information Protection, shields documents and emails and ensures that they’re properly labeled and classified.



- **Security management:** Solutions such as Microsoft Secure Score will both manage and monitor the security posture of an organization and make recommendations for improvement.
- **Device management:** E5 offers solutions like Endpoint Manager for all devices and applications across the organization. This is a must for companies that struggle with implementing security policies equally across the board.
- **Cloud Security:** Azure Security Center and Microsoft Cloud App Security can set and manage compliance standards across all environments. This includes all regulations and policies, regardless of whether they're internal or external.

Making the Business Case for E5 to Leadership

A CFO isn't going to view E5 features in the same way a CTO will. For them, it comes down to understanding how the organization will run more efficiently for the additional costs.

Full Visibility Into the Network

There's been something of a trend for companies these days to opt for the so-called best-of-breed tech available. They may leverage different security tools from companies with incredible track records, giving them full access to the technology without putting all of their eggs in one basket. This somewhat understandable approach fails to account for the complexity of the threat actors.

Emails, apps, data, endpoints, and the cloud are all just possible in-roads for criminals and mischief-makers. E5 secures across these highly distributed environments with the help of Advanced Threat Protection, Cloud App Security, and Microsoft Defender ATP. It's consistently proven to be best-in-class because it protects across the entire digital landscape.

It would be easy for a CFO to focus purely on identity compromise protections (because they account for 95% of the breaches), but identity compromises can originate from nearly anywhere in your network. With Intune, Priva, Purview, Entra, Sentinel, and the Defender Stack, companies can manage devices, improve identity management, and ensure privacy across the board.

Compliance and Governance

Regulatory bodies can issue more than 250 updates per day based on everything from changing laws to recommended security practices. The influx of rules has led to full-time positions being carved out to simply keep up with official expectations. With E5, you can label, store, and protect data, and you can track both internal and external movements of that data based on a 360° understanding of the activity. So if an employee gets a poor review from HR and then begins siphoning data onto a USB drive, Purview would be able to show that connection so staff could intervene.

These are situations where a company like Dataprise can really prove its value to clients. More than 50% of organizations surveyed say that IT and cybersecurity are their number one risks and that identifying and assessing risks is the most time-consuming activity in risk management. With expertise across multiple environments and endless rollouts, their background with these tools is an invaluable asset for clients who can't afford to waste time.

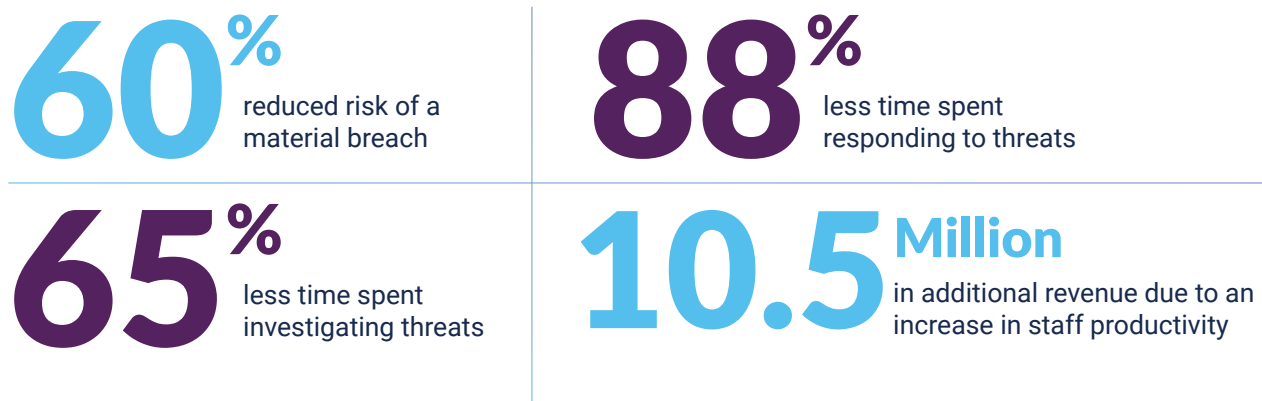
New threats, particularly as AI capabilities are ramped up for threat actors, will always stir apprehension for companies that want to protect their revenue and clients. A CFO may need to be reminded that security is not a one-time solution but rather an evolving entity that's worth the investment. From permissions to governance, E5 is a proactive security tool that can satisfy even the most rigorous compliance regulations.

Cost Efficiency Through Simplified Vendor Management

Simplifying to one vendor can save more money in the long run. Dataprise used publicly available pricing for Cloud PBX, Advanced BI, Identity and Access Management, and Compliance Management vendors to determine the average amount spent on these services and arrived at around \$118 per user. Because E5 provides these services in one convenient package, it can bring the overall cost down to \$97 per user on average. (Please note that E5 cannot replace every vendor, but it's common for Dataprise to find several subscriptions that can be eliminated after upgrading.)

Case Studies

There are numerous case studies that highlight the real-world benefits of Microsoft E5. Dataprise has quantified the results to help CFOs understand the potential ROI:



While the actual statistics and revenue increases will vary across companies, Microsoft Sentinel, Microsoft 365 Defender, and Microsoft Defender for Cloud have shown tremendous potential to offset the limitations of any security team and free up more time to focus on enhancing the business.

In addition, collaboration tools like PSTN Conferencing and Cloud PBX can foster a more collaborative environment, giving team members simple ways to get in touch with one another, even if they're experiencing internet issues or their laptop has unexpectedly malfunctioned. Tools like Power BI improve data analytics and can be merged with teams to help everyone on a project properly contextualize the information as they move forward to completion. For companies that want to move forward with a more comprehensive digital transformation, the analytics and agility offered across all tools can streamline the process.

The Transition

A good CFO isn't just going to weigh the direct costs of the E5 licensing. They're also going to factor in everything from staff resistance to the C-suite's objections. These are situations where a company like Dataprise can prove its value to clients. More than 50% of organizations surveyed say that IT and cybersecurity are their number one risks and that identifying and assessing risks is the most time-consuming activity in risk management. With expertise across multiple environments and endless rollouts, Dataprise's background and expertise are an invaluable asset for clients who can't afford to waste time.

An MSP like Dataprise may first start with an assessment of a company's current infrastructure. This is often where teams learn that they're still paying for certain services and vendors that they thought they had canceled. The goal is then to evaluate where E5 would fit in, how many vendors it could replace, and what it would mean to disrupt the organization as everyone adapted the new tools.

How do AI and Automation Contribute to the M365 E5 License?

The enhanced security of E5 is strongly linked to its AI and automation features. These tools are built as a stack to reveal threats in context, allowing companies to see how threat actors move across environments. Threat actors are increasingly using AI and automation for their own goals, making it more critical than ever to understand how they gather the necessary intel to execute a successful breach. E5 can quickly reveal that red thread, giving a company more time to react and putting the company at less risk for a compliance violation.

Tying it together is an AI assistant currently being integrated into Microsoft's capabilities. Dubbed the Security Co-Pilot, the tool allows for natural-language questions about which programs or accounts are at most risk for certain attacks. Even as new threats emerge, Microsoft is positioning this tool as one that can be used for both emergencies and general inquiries.

Once asked, it will answer back in the same natural language, giving security teams more time to respond to the ever-evolving list of threats. Robotic Process Automation, Power BI Pro, and Cloud App Security can streamline business processes, provide better insights, and migrate threats in the cloud environment. It all boils down to less manual intervention. The security team gets real-time threat protection, so they can respond immediately to any threats that can't be automatically mitigated.



Interested in Learning More? Dataprise Can Help.

Upgrading from E3 to E5 has the power to streamline both the budget and business processes. As a vendor, Microsoft's portfolio has consistently found ways to satisfy even the most cut-throat evaluations. Dataprise provides managed services to companies that recognize the potential to lower costs while freeing up their employees' time.

Call us at [1.888.519.8111](tel:1-888-519-8111) to talk about your E5 Licensing needs.