DATAPRISE

Maximizing Microsoft 365 E5's Security & Compliance Capabilities

Microsoft 365 E5 is an upgrade from the M365 and E3 license, prompting business leaders across the country to ask whether the additional benefits are worth the investment. In a recent webinar from Dataprise, Maximizing Microsoft 365 E5's Security and Compliance Capabilities, the team discussed E5's security enhancements and how they impacted both the compliance and operational efficiency of a company.

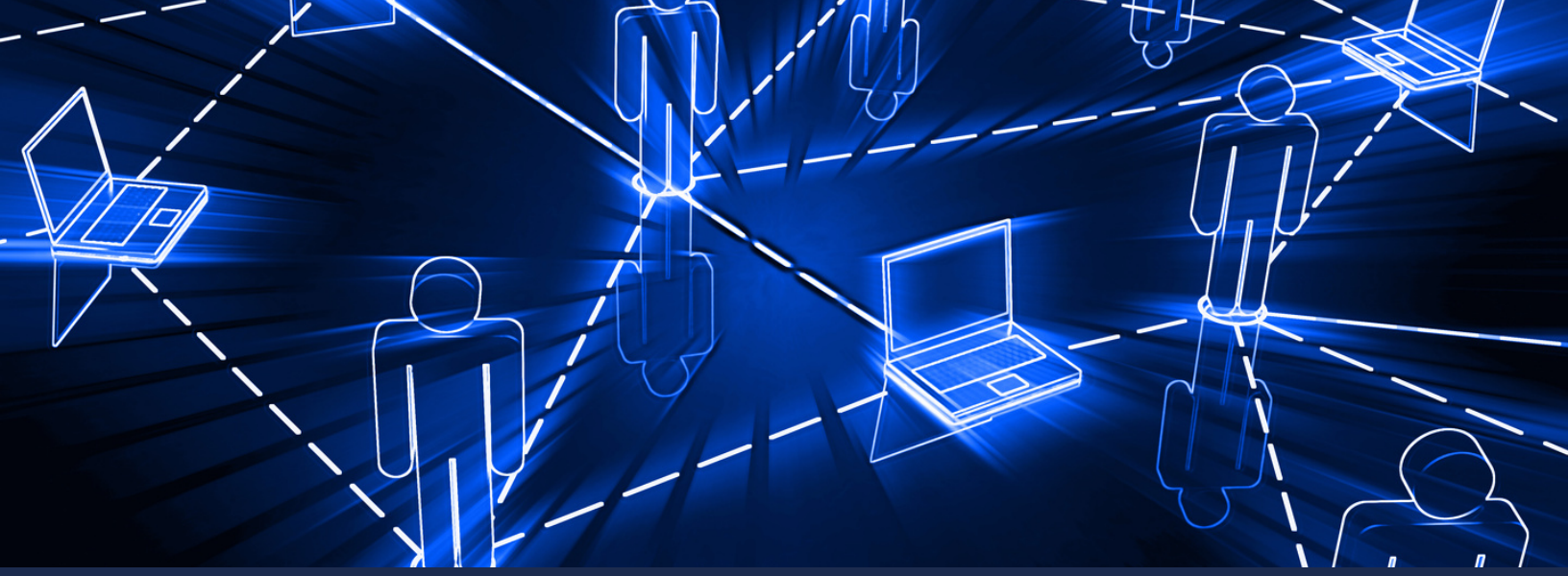
Integrated Security Features

When companies are liable to distribute their resources across platforms, Microsoft has responded by integrating security into the cloud. Companies that are busy trying to manage AWS, Azure, and Google compliance can trust Defender for Cloud to reach all of their data.
Whether a company has data stored on internal or external servers, E5 makes the tech stack more robust. Given the sometimes vague protection regulations, you can trust this license to meet or exceed the standards of multiple agencies and organizations. Plus, these security features eliminate the need for platform-specific security, potentially saving companies up to 30%.

Microsoft Security Portfolio

The Security Portfolio may not be groundbreaking in terms of the promises it makes, but it does introduce multiple features that work together as one to drastically reduce the odds of a breach.

Access Management
The person behind the screen is more likely to be the cause of a breach than the gaps in your network are. With identity management and protection, companies get more security layers than just multifactor authentication. Leadership can ensure that only authorized users have access to various assets and resources.



Information Protection

E5 has both Microsoft Information Protection and Azure Information Protection, giving you an all-around defense for your most important details. By leveraging machine learning, Microsoft can go a step further by identifying sensitive information before it has the chance of exposure.

Device Management

All devices within an organization are protected under E5's Endpoint Manager, making it an excellent choice for companies having trouble keeping up with both internal and external machinery. This is a compliance lifesaver when you can never be sure who's keeping up with what updates.

Compliance Standards

Microsoft Cloud App Security and Azure Security Center work to streamline compliance standards across internal and external environments. This helps companies keep up with changing policies and protocols, automating security so that audits can go smoother and employees can breathe easier when emerging threats trigger new rules.

Stronger Security Posture

Microsoft Secure Score can both manage and monitor an organization's posture, and provide custom recommendations to strengthen your proverbial castle. Defender for Endpoint and Sentinel can also go a long way to staving off even the most committed hackers in the business.

In addition, Microsoft Defender Advanced Threat Protection (ATP) has been upgraded from Microsoft's original ATP. The features extend to desktops, services, mobile devices, and servers. Dataprise engineers have seen how real-time threat detection has helped companies identify openings in their systems that could lead to a breach.

Compliance Today

When technology seemingly changes at every turn, it's no wonder regulatory bodies have been known to issue hundreds of updates per day. With every law change and security recommendation, companies are expected to do their part. E5 was created with these often unwieldy laws in mind.

The license allows companies to not just track their data it also gives the CTO and CEO (and every other decision-maker in between) full visibility into how the activity is happening and whether it meets the company's compliance standards.

So, if an internal actor decided to slowly steal financial information by loading documents onto an external device, E5's data governance solution would be able to show who was behind the theft.
As the world struggles to balance its security with AI threats, there's more reason than ever for companies to take precautions. The more an organization invests in proactive security, the less likely it is to be caught in a data security incident (or slapped with regulatory fines for failing to meet compliance standards).

E5 was built using the best automation tools available today, and when a company has them all working together, they're more likely to spot the often well-disguised threats that can derail their staff, revenue, and reputation. Features like the Security Co-Pilot through E5 utilize machine learning to answer questions about which digital assets are most likely to be attacked. With this license, employees can ask in everyday language what they can do to mitigate emergencies, complete standard tasks, and safeguard their assets against would-be criminals.

Making the Switch

Upgrading to Microsoft E5 might not be easy for everyone to agree to, but organizations concerned with security may not have much choice. When the goalposts keep changing, Microsoft's security tools have proven that they can keep pace with the ever-evolving expectations. Setting up all the tools in a way that works for your security needs (not to mention the staff's needs) may mean reaching out to an experienced vendor. A Managed Service Provider (MSP) like Dataprise can be essential to the transition, particularly if you want the E5 license to pay for itself over time. **Interested in making the switch to E5? Dataprise can help. Contact us at 1-888-519-8111.**